Guide de configuration d'Oracle® Solaris Trusted Extensions

Référence : E22294
Août 2011

ORACLE®

111013@25097

Table des matières

Préface 13

1 Planification de la sécurité pour Trusted Extensions 19
Planification de la sécurité dans Trusted Extensions 19
Prise de connaissance de Trusted Extensions 20
Prise de connaissance de votre stratégie de sécurité du site 20
Conception d'une stratégie d'administration de Trusted Extensions 21
Élaboration d'une stratégie d'étiquetage 22
Planification du matériel et de la capacité du système pour Trusted Extensions 23
Planification de votre réseau de confiance 23
Planification de zones dans Trusted Extensions 24
Planification pour l'accès multiniveau 26
Planification pour le service de nommage LDAP dans Trusted Extensions 27
Planification du contrôle dans Trusted Extensions 27
Planification de la sécurité de l'utilisateur dans Trusted Extensions 28
Élaboration d'une stratégie de configuration pour Trusted Extensions 29
Résolution d'autres problèmes avant d'activer Trusted Extensions 31
Sauvegarde du système avant l'activation de Trusted Extensions 31
Résultats de l'activation de Trusted Extensions du point de vue de l'administrateur 32

2 Déroulement de la configuration de Trusted Extensions 35
Liste des tâches : préparation d'un système Solaris pour Trusted Extensions 35
Liste des tâches : préparation et activation de Trusted Extensions 35
Liste des tâches : configuration de Trusted Extensions 37

3 Ajout du logiciel Trusted Extensions au SE Solaris (tâches) 41
Responsabilités de l'équipe chargée de la configuration initiale 41

Installation ou mise à niveau du SE Solaris pour Trusted Extensions 42
▼ Installation d'un système Solaris pour prendre en charge Trusted Extensions 42
▼ Préparation d'un système Solaris installé pour Trusted Extensions 43
Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions 46
▼ Collecte d'informations système avant l'activation de Trusted Extensions 46
▼ Prise de décisions relatives au système et à la sécurité avant l'activation de Trusted Extensions 47
Activation du service Trusted Extensions 49
▼ Activation de Trusted Extensions 49

4 Configuration de Trusted Extensions (tâches) 51
Configuration de la zone globale dans Trusted Extensions 51
▼ Vérification et installation du fichier de votre fichier label_encodings 52
▼ Activation du réseau IPv6 dans Trusted Extensions 56
▼ Configuration du domaine d'interprétation 57
▼ Création d'un pool ZFS pour le clonage des zones 58
▼ Redémarrage et connexion à Trusted Extensions 59
▼ Initialisation du serveur Console de gestion Solaris dans Trusted Extensions 61
▼ Établissement de la zone globale en tant que client LDAP dans Trusted Extensions 64
Création de zones étiquetées 68
▼ Exécution du script `txzonemgr` 69
▼ Configuration des interfaces réseau dans Trusted Extensions 70
▼ Attribution de nom et étiquetage de la zone 74
▼ Installation de la zone étiquetée 77
▼ Démarrage de la zone étiquetée 78
▼ Vérification de l'état de la zone 79
▼ Personnalisation de la zone étiquetée 81
▼ Copie ou clonage d'une zone dans Trusted Extensions 82
Ajout d'interfaces réseau et acheminement vers les zones étiquetées 84
▼ Ajout d'une interface réseau pour acheminer une zone étiquetée existante 85
▼ Ajout d'une interface réseau qui n'utilise pas la zone globale pour acheminer une zone étiquetée existante 87
▼ Configuration d'un cache de service de noms dans chaque zone étiquetée 91
Création de rôles et d'utilisateurs dans Trusted Extensions 92
▼ Création de profils de droits permettant d'appliquer la séparation des tâches 93
▼ Création du rôle d'administrateur de sécurité dans Trusted Extensions 96

▼ Création d'un rôle d'administrateur système limité 99
▼ Création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions 99
▼ Vérification du fonctionnement des rôles Trusted Extensions 102
▼ Autorisation des utilisateurs à se connecter à une zone étiquetée 104
Création de répertoires personnels dans Trusted Extensions 104
▼ Création du serveur d'annuaires personnel dans Trusted Extensions 105
▼ Activation de l'accès des utilisateurs à leurs répertoires personnels dans Trusted Extensions 106
Ajout d'utilisateurs et d'hôtes à un réseau Trusted Network existant 107
▼ Ajout d'un utilisateur NIS au serveur LDAP 107
Dépannage de votre configuration Trusted Extensions 110
La commande `netservices limited` a été exécutée après l'activation de Trusted Extensions 110
Impossible d'ouvrir la fenêtre de console dans une zone étiquetée 110
La zone étiquetée ne peut accéder au serveur X 111
Tâches de configuration supplémentaires de Trusted Extensions 113
▼ Copie de fichiers sur un support amovible dans Trusted Extensions 113
▼ Copie de fichiers dans Trusted Extensions à partir d'un support amovible 115
▼ Suppression de Trusted Extensions du système 116

5 Configuration de LDAP pour Trusted Extensions (tâches) 119
Configuration d'un serveur LDAP sur un hôte Trusted Extensions (liste des tâches) 119
Configuration d'un serveur proxy LDAP sur un hôte Trusted Extensions (liste des tâches) ... 120
Configuration du Sun Java System Directory Server sur un système Trusted Extensions 121
▼ Collecte d'informations pour le serveur d'annuaire pour LDAP 121
▼ Installation du Sun Java System Directory Server 122
▼ Création d'un client LDAP pour le serveur d'annuaire 125
▼ Configuration des journaux pour le Sun Java System Directory Server 127
▼ Configuration d'un port multiniveau pour le Sun Java System Directory Server 128
▼ Remplissage du Sun Java System Directory Server 129
Création d'un proxy Trusted Extensions pour un Sun Java System Directory Server existant 131
▼ Création d'un serveur proxy LDAP 132
Configuration de la Console de gestion Solaris pour LDAP (liste des tâches) 132
▼ Enregistrement des informations d'identification et de connexion LDAP avec la Console de gestion Solaris 133
▼ Activation de la Console de gestion Solaris afin qu'elle accepte les communications

réseau 134
▼ Modification de la boîte à outils LDAP dans la Console de gestion Solaris 135
▼ Vérification des informations Trusted Extensions contenues dans la Console de gestion Solaris 136

6 Configuration d'un écouteur avec Trusted Extensions (tâches) 139
Configuration de l'écouteur dans Trusted Extensions (liste des tâches) 139
▼ Activation de la connexion à distance par l'utilisateur `root` dans Trusted Extensions 141
▼ Activation de la connexion à distance par un rôle dans Trusted Extensions 141
▼ Activation de la connexion à distance à partir d'un système sans étiquette 143
▼ Utilisation d'une Console de gestion Solaris à distance pour administrer dans l'étendue fichiers 144
▼ Activation de l'affichage à distance des interfaces graphiques d'administration 145
▼ Utilisation de la commande `rlogin` ou `ssh` pour se connecter à un écouteur dans Trusted Extensions et l'administrer 145

A Stratégie de sécurité du site 149
Création et gestion d'une stratégie de sécurité 149
Stratégie de sécurité du site et Trusted Extensions 150
Recommandations relatives à la sécurité informatique 151
Recommandations relatives à la sécurité physique 152
Recommandations relatives à la sécurité du personnel 153
Violations de sécurité courantes 153
Références de sécurité supplémentaires 154
U.S. Government Publications 154
Publications relatives à la sécurité UNIX 155
Publications relatives à la sécurité générale du système informatique 155
Publications UNIX générales 155

B Utilisation d'actions CDE pour installer des zones dans Trusted Extensions 157
Association d'interfaces réseau avec des zones à l'aide d'actions CDE (liste des tâches) 157
▼ Spécification de deux adresses IP pour le système à l'aide d'une action CDE 158
▼ Spécification d'une adresse IP pour le système à l'aide d'une action CDE 159
Préparation de la création de zones à l'aide d'actions CDE (liste des tâches) 160
▼ Spécification des noms et étiquettes de zone à l'aide d'une action CDE 161

Création de zones étiquetées à l'aide d'actions CDE (liste des tâches) 163
▼ Installation, initialisation et démarrage d'une zone étiquetée à l'aide d'actions CDE 164
▼ Résolution de l'acheminement zone locale-zone globale dans Trusted CDE 167
▼ Personnalisation d'une zone initialisée dans Trusted Extensions 168
▼ Utilisation de la méthode de copie de zone dans Trusted Extensions 170
▼ Utilisation de la méthode de clonage de zone dans Trusted Extensions 171

C Liste de contrôle de configuration pour Trusted Extensions 173
Liste de contrôle de configuration Trusted Extensions 173

Glossaire 177

Index 185

Liste des figures

FIGURE 1–1 Administration d'un système Trusted Extensions : séparation des tâches en fonction du rôle de l'utilisateur 31

FIGURE 4–1 Fenêtre initiale de la Console de gestion Solaris 62

FIGURE 4–2 Outils Trusted Extensions dans la Console de gestion Solaris 63

Liste des tableaux

TABLEAU 1–1 Modèles d'hôtes par défaut dans Trusted Extensions 24
TABLEAU 1–2 Paramètres de sécurité par défaut Trusted Extensions pour les comptes utilisateur 28

Préface

Le guide *Guide de configuration d'Oracle Solaris Trusted Extensions* décrit les procédures de configuration de Trusted Extensions sur le système d'exploitation Solaris (SE Solaris). Ce guide décrit également la préparation du système Solaris pour la prise en charge d'une installation sécurisée de Trusted Extensions.

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

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

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

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

Utilisateurs de ce guide

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

Mise en œuvre de la sécurité du site

Pour configurer Trusted Extensions sur un système de manière compatible avec la sécurité de votre site, vous devez avoir une bonne maîtrise des fonctionnalités de sécurité de Trusted Extensions et de la stratégie de sécurité de votre site. Avant de commencer, lisez le Chapitre 1, "Planification de la sécurité pour Trusted Extensions" pour savoir comment garantir la sécurité de votre site lors de la configuration du logiciel.

Trusted Extensions et le système d'exploitation Solaris

Trusted Extensions s'exécute sur le SE Solaris. Étant donné que Trusted Extensions peut modifier le SE Solaris, Trusted Extensions peut nécessiter un paramétrage particulier des options d'installation de Solaris. Pour plus d'informations, reportez-vous au Chapitre 3, “Ajout du logiciel Trusted Extensions au SE Solaris (tâches)”. En outre, les guides Trusted Extensions complètent les guides Solaris. En tant qu'administrateurs, vous devez avoir accès aux guides Solaris et Trusted Extensions.

Organisation de ce document

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 Solaris.

Le Chapitre 2, “Déroulement de la configuration de Trusted Extensions” contient des listes de tâches concernant l'ajout du logiciel Trusted Extensions aux systèmes Solaris.

Le Chapitre 3, “Ajout du logiciel Trusted Extensions au SE Solaris (tâches)” fournit des instructions sur la préparation d'un système Solaris pour le logiciel Trusted Extensions. Il contient également des instructions sur l'activation de Trusted Extensions.

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 de LDAP pour Trusted Extensions.

Le Chapitre 6, “Configuration d'un écouteur avec Trusted Extensions (tâches)” décrit la configuration et l'administration du logiciel Trusted Extensions sur un écouteur.

L'Annexe A, “Stratégie de sécurité du site” traite de la stratégie de sécurité du site et place Trusted Extensions dans le contexte de la sécurité du site et de l'entreprise de manière plus générale.

L'Annexe B, “Utilisation d'actions CDE pour installer des zones dans Trusted Extensions” décrit la configuration des zones étiquetées à l'aide d'actions Trusted CDE.

L'Annexe C, “Liste de contrôle de configuration pour Trusted Extensions” fournit une liste de contrôle de configuration destinée à l'équipe chargée de la configuration initiale.

Le Glossaire définit des termes et expressions utilisés dans ce guide.

Organisation des guides Trusted Extensions

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

Titre du guide	Sujets	Public visé
Solaris Trusted Extensions Transition Guide	Obsolète. Fournit un aperçu des différences entre les logiciels Trusted Solaris 8, Solaris10 et Trusted Extensions. Pour cette version, le document *What's New* pour le SE Solaris fournit un aperçu des modifications apportées à Trusted Extensions.	Tous
Solaris Trusted Extensions Reference Manual	Obsolète. Fournit les pages de manuel Trusted Extensions pour les versions Solaris 10 11/06 et Solaris 10 8/07 de Trusted Extensions. Pour cette version, les pages de manuel Trusted Extensions sont incluses avec les pages de manuel Solaris.	Tous
Guide de l'utilisateur Oracle Solaris Trusted Extensions	Décrit les fonctions de base de Trusted Extensions. Ce guide contient un glossaire.	Utilisateurs, administrateurs, développeurs
Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases	Obsolète. Décrit la planification, l'installation et la configuration de Trusted Extensions pour les versions Solaris 10 11/06 et Solaris 10 8/07 de Trusted Extensions.	Administrateurs, développeurs
Guide de configuration d'Oracle Solaris Trusted Extensions	À partir de la version Solaris 10 5/08, décrit l'activation et la configuration initiale de Trusted Extensions. Remplace *Solaris Trusted Extensions Installation and Configuration*.	Administrateurs, développeurs
Procédures de l'administrateur Oracle Solaris Trusted Extensions	Indique comment effectuer des tâches d'administration spécifiques.	Administrateurs, développeurs
Oracle Solaris Trusted Extensions Developer's Guide	Décrit le développement d'applications avec Trusted Extensions.	Développeurs, administrateurs
Oracle Solaris Trusted Extensions Label Administration	Fournit des informations sur la manière de spécifier les composants d'étiquette dans le fichier label_encodings.	Administrateurs
Compartmented Mode Workstation Labeling: Encodings Format	Décrit la syntaxe utilisée dans le fichier label_encodings. La syntaxe applique les différentes règles permettant de créer des étiquettes bien formées pour un système.	Administrateurs

Guides d'installation connexes

Les guides suivants contiennent des informations utiles lors de la préparation du logiciel Trusted Extensions.

Oracle Solaris 10 8/11 Installation Guide: Basic Installations : fournit des conseils sur les options d'installation du SE Solaris.

Oracle Solaris 10 8/11 Installation Guide: Custom JumpStart and Advanced Installations : fournit des conseils sur les méthodes d'installation et les options de configuration.

Oracle Solaris 10 8/11 Installation Guide: Planning for Installation and Upgrade : fournit des conseils sur l'installation d'une mise à niveau du SE Solaris.

Références connexes

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

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

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

Références connexes aux sites Web de logiciels tiers

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

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

Documentation, support et formation

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

- Documentation (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)
- Assistance (`http://www.oracle.com/us/support/systems/index.html`)
- Training (`http://www.oracle.com/global/us/education/sun_select_country.html`) : choisissez le pays pour lequel vous voulez des informations de formation pour d'anciens produits Sun.

Ressources logicielles Oracle

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

- Discutez de problèmes techniques et trouvez des solutions sur les forums de discussion (`http://forums.oracle.com`).
- Découvrez des tutoriels pratiques avec Oracle par l'exemple (`http://www.oracle.com/technetwork/tutorials/index.html`).
- Téléchargez un échantillon de code (`http://www.oracle.com/technology/sample_code/index.html`).

Conventions typographiques

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

TABLEAU P–1 Conventions typographiques

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

TABLEAU P–1 Conventions typographiques *(Suite)*

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

Invites de shell dans les exemples de commandes

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

TABLEAU P–2 Invites de shell

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

◆ ◆ ◆ CHAPITRE 1

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" à la page 19
- "Résultats de l'activation de Trusted Extensions du point de vue de l'administrateur" à la page 32

Planification de la sécurité dans Trusted Extensions

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

- "Prise de connaissance de Trusted Extensions" à la page 20
- "Prise de connaissance de votre stratégie de sécurité du site" à la page 20
- "Conception d'une stratégie d'administration de Trusted Extensions" à la page 21
- "Élaboration d'une stratégie d'étiquetage" à la page 22
- "Planification du matériel et de la capacité du système pour Trusted Extensions" à la page 23
- "Planification de votre réseau de confiance" à la page 23
- "Planification de zones dans Trusted Extensions" à la page 24
- "Planification pour l'accès multiniveau" à la page 26
- "Planification pour le service de nommage LDAP dans Trusted Extensions" à la page 27
- "Planification du contrôle dans Trusted Extensions" à la page 27
- "Planification de la sécurité de l'utilisateur dans Trusted Extensions" à la page 28
- "Élaboration d'une stratégie de configuration pour Trusted Extensions" à la page 29
- "Résolution d'autres problèmes avant d'activer Trusted Extensions " à la page 31
- "Sauvegarde du système avant l'activation de Trusted Extensions" à la page 31

Pour une liste de contrôle des tâches de configuration de Trusted Extensions, reportez-vous à l'Annexe C, "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 22. 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 20.

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 fonctionnalités 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 configurables suivants :
  - `/usr/openwin/server/etc/*`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/SelectionManager`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolsession`
  - `/usr/dt/bin/Xtsolusersession`
  - `/usr/dt/config/sel_config`
  - `/usr/X11/lib/X11/xserver/TrustedExtensionsPolicy`

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 d'utilisateur `root` ou 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.
- L'administrateur principal est responsable de la création d'un profil de droits pour l'administrateur sécurité et de la résolution des problèmes lorsque les administrateurs de sécurité et système ne disposent pas de privilèges suffisants.
- 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 version définitive du fichier doit être prête avant que le système ne vérifie les étiquettes. Le fichier doit se trouver sur un support amovible. Les étiquettes sont vérifiées au cours du premier démarrage après l'activation du service Trusted Extensions.

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 *Oracle Solaris 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`.

Trusted Extensions prend en charge moins de paramètres régionaux que le SE Oracle Solaris. Lorsque vous travaillez dans un environnement linguistique que Trusted Extensions ne prend pas en charge, le texte spécifique à Trusted Extensions, tels que les messages d'erreur relatifs aux étiquettes, n'est pas traduit dans votre langue. Oracle Solaris reste traduit dans votre langue.

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 à la section "System Requirements and Recommendations" du *Solaris 10 5/09 Installation Guide: Basic Installations*.
- 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 exécutant la Console de gestion Solaris, une interface graphique d'administration requise
    - 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 pour planifier votre matériel réseau, reportez-vous au Chapitre 2, "Planning Your TCP/IP Network (Tasks)" du *System Administration Guide: IP Services*.

Comme pour tout réseau client-serveur, vous devez identifier les hôtes par leur fonction, c'est-à-dire serveur ou client, et configurer le logiciel de manière appropriée. Pour obtenir de l'aide pour la planification, reportez-vous au *Solaris 10 5/09 Installation Guide: Custom JumpStart and Advanced Installations*.

Le logiciel Trusted Extensions reconnaît deux types d'hôtes, étiquetés 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.

La page de manuel `smtnrhtp(1M)` contient une description complète de chaque type d'hôte avec plusieurs exemples.

Planification de zones dans Trusted Extensions

Le logiciel Trusted Extensions est ajouté au SE 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`.

La configuration de zones implique la configuration du réseau. Par défaut, les zones étiquetées sont configurées pour communiquer avec la zone globale. En outre, vous pouvez configurer les zones sur le système pour communiquer avec d'autres zones du réseau.

- Le serveur X qui exécute l'affichage de l'ordinateur de bureau n'est disponible qu'à partir de la zone globale. À partir de la version Solaris 10 10/08, l'interface de loopback, `lo0`, peut être utilisée pour communiquer avec la zone globale. Par conséquent, l'affichage de l'ordinateur de bureau est disponible pour les zones non globales via `lo0`.
- Par défaut, les zones non globales ne peuvent pas communiquer avec des hôtes non approuvés. À partir de la version Solaris 10 10/08, vous pouvez configurer chaque zone non globale avec une route par défaut unique qui n'utilise pas la zone globale.

Zones Trusted Extensions et zones Oracle Solaris

Les zones étiquetées diffèrent des zones Oracle Solaris standard. 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. La seule interface interactive vers une zone étiquetée est la console de la zone. Seul l'utilisateur root peut accéder à la console de la zone.

Création d'une zone dans Trusted Extensions

La création d'une zone étiquetée implique la copie de l'intégralité du SE Oracle Solaris, puis le démarrage des services pour le SE Oracle Solaris dans chaque zone. Ce processus peut prendre beaucoup de temps. Un processus plus rapide consiste à créer une zone, puis la copier ou cloner son contenu. Le tableau suivant décrit les options disponibles pour créer une zone dans Trusted Extensions.

Méthode de création de zone	Efforts requis	Caractéristiques de cette méthode
Création de chaque zone étiquetée à partir de zéro.	Configuration, initialisation, installation, personnalisation et amorçage de chaque zone étiquetée.	■ Cette méthode est prise en charge et s'avère très utile pour la création d'une ou de deux zones supplémentaires. Les zones peuvent être mises à niveau. ■ Cette méthode nécessite beaucoup de temps.
Création des zones étiquetées supplémentaires à partir d'une copie de la première zone étiquetée.	Configuration, initialisation, installation et personnalisation d'une zone. Cette zone est ensuite utilisée comme modèle pour d'autres zones étiquetées.	■ Cette méthode est prise en charge et est plus rapide que la création de zones à partir de zéro. Les zones peuvent être mises à niveau. Utilisez la méthode de copie de zone si vous voulez que l'assistance Oracle vous aide en cas de difficulté liée aux zones. ■ Cette méthode utilise UFS. UFS n'offre pas l'isolement supplémentaire pour les zones offert par Oracle Solaris ZFS.

Méthode de création de zone	Efforts requis	Caractéristiques de cette méthode
Création de zones étiquetées supplémentaires à partir d'un instantané ZFS de la première zone étiquetée.	Configuration d'un pool ZFS à partir d'une partition que vous avez mise de côté pendant l'installation d'Oracle Solaris. Configuration, initialisation, installation et personnalisation d'une zone. Cette zone est ensuite utilisée comme instantané ZFS pour d'autres zones étiquetées.	■ Cette méthode utilise Oracle Solaris ZFS et est la méthode la plus rapide. Elle fait de chaque zone un système de fichiers, et offre ainsi une isolation supérieure à celle offerte par UFS. ZFS utilise beaucoup moins d'espace disque. ■ Si vous testez Trusted Extensions et pouvez réinstaller les zones plutôt que de les mettre à niveau, cette méthode peut constituer un bon choix. Cette méthode peut s'avérer utile sur les systèmes dont le contenu n'est pas volatil, car le système peut rapidement être réinstallé afin d'être utilisable. ■ Cette méthode n'est *pas* prise en charge. Les zones créées à l'aide de cette méthode *ne peuvent pas être mises à niveau* lors de la publication d'une nouvelle version du SE.

Les zones Oracle Solaris ont une incidence sur l'installation de package et l'application de patchs. Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 25, "About Packages and Patches on a Solaris System With Zones Installed (Overview)" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- FAQ relatives aux zones et conteneurs Solaris (`http://hub.opensolaris.org/bin/view/Community+Group+zones/faq`)

Planification pour l'accès multiniveau

En règle générale, l'impression et le NFS sont configurés en tant que services multiniveau. Pour accéder aux services multiniveau, un système correctement configuré nécessite que chaque zone puisse accéder à une ou plusieurs adresses réseau. Les configurations suivantes fournissent des services multiniveau :

- **Pile IP exclusive** : comme dans le SE Oracle Solaris, une adresse IP est affectée à chaque zone, y compris la zone globale. Par défaut, une carte d'informations de réseau virtuel (VNIC) est créée pour chaque zone étiquetée.

  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.

- **Pile IP partagée** : une adresse `all-zones` est affectée. Dans cette configuration, le système ne peut pas être un serveur NFS multiniveau. Une ou plusieurs zones peuvent avoir des adresses spécifiques à la zone.

Un système qui répond aux deux conditions suivantes ne peut pas fournir de services multiniveau :

- Une adresse IP partagée par la zone globale et les zones étiquetées est affectée.
- Aucune adresse spécifique à une zone n'est affectée.

Astuce – Si les utilisateurs des zones étiquetées ne sont pas supposés avoir accès à une imprimante multiniveau locale et si vous avez besoin d'exports NFS des répertoires personnels, vous pouvez affecter une adresse IP à un système que vous configurez avec Trusted Extensions. Sur un tel système, l'impression multiniveau n'est pas prise en charge et les répertoires personnels ne peuvent pas être partagés. L'utilisation typique de cette configuration est sur un ordinateur portable.

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 prévoyez d'exécuter Trusted Extensions sur un réseau de systèmes, utilisez LDAP en tant que service de nommage. Pour Trusted Extensions, un Sun Java System Directory Server (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, le contrôle est activé lors de l'installation de Trusted Extensions. C'est pourquoi, par défaut, la connexion `root`, le verrouillage d'écran et la déconnexion font l'objet d'un contrôle. Pour contrôler 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 de contrôle 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 92.

La planification du contrôle dans Trusted Extensions est identique à la planification dans le SE Oracle Solaris. Pour en savoir plus, reportez-vous à la Partie VII, “Oracle Solaris Auditing” du *System Administration Guide: Security Services*. Bien que Trusted Extensions ajoute des classes, des événements et des jetons de contrôle, le logiciel ne modifie pas le mode d'administration du contrôle. Pour en savoir plus sur les ajouts de Trusted Extensions au contrôle, reportez-vous au Chapitre 18, “Audit de Trusted Extensions (présentation) ” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Planification de la sécurité de l'utilisateur dans Trusted Extensions

Le logiciel Trusted Extensions fournit des paramètres de sécurité par défaut raisonnables aux 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`	`_unix_`
	`LOCK_AFTER_RETRIES`	`no | yes`
	`PRIV_DEFAULT`	`basic`
	`PRIV_LIMIT`	`all`
	`AUTHS_GRANTED`	`solaris.device.cdrw`
	`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, par défaut, le shell initial de tous les utilisateurs est un shell Bourne. L'administrateur système peut configurer un modèle qui donne à chaque utilisateur un shell C. Pour plus d'informations, reportez-vous à l'aide en ligne de la Console de gestion Solaris relative aux comptes utilisateurs.

Élaboration d'une stratégie de configuration pour Trusted Extensions

Autoriser l'utilisateur `root` à configurer le logiciel Trusted Extensions ne constitue pas une stratégie sécurisée. 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 et décide des utilisateurs locaux qui peuvent les assumer. L'équipe configure également un contrôle en vue de contrôler les événements exécutés par les rôles. Une fois les rôles affectés à des utilisateurs et l'ordinateur redémarré, le logiciel applique la séparation des tâches en fonction des rôles. 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.

  Remarque – Si la sécurité du site requiert une séparation des tâches, un administrateur de confiance doit exécuter la tâche "Création de profils de droits permettant d'appliquer la séparation des tâches" à la page 93 avant de créer des utilisateurs ou des rôles. Dans cette configuration personnalisée, un rôle gère la sécurité, y compris les attributs de sécurité des utilisateurs. L'autre rôle gère les attributs autres que la sécurité des systèmes et utilisateurs.

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

  Très tôt dans le processus de configuration, l'utilisateur `root` crée un utilisateur local et des rôles. Cet utilisateur configure également le contrôle visant à contrôler les événements exécutés par les rôles. Une fois les rôles attribués à l'utilisateur local et l'ordinateur redémarré, le logiciel applique la séparation en fonction des rôles. La piste d'audit fournit un enregistrement de la procédure de configuration.

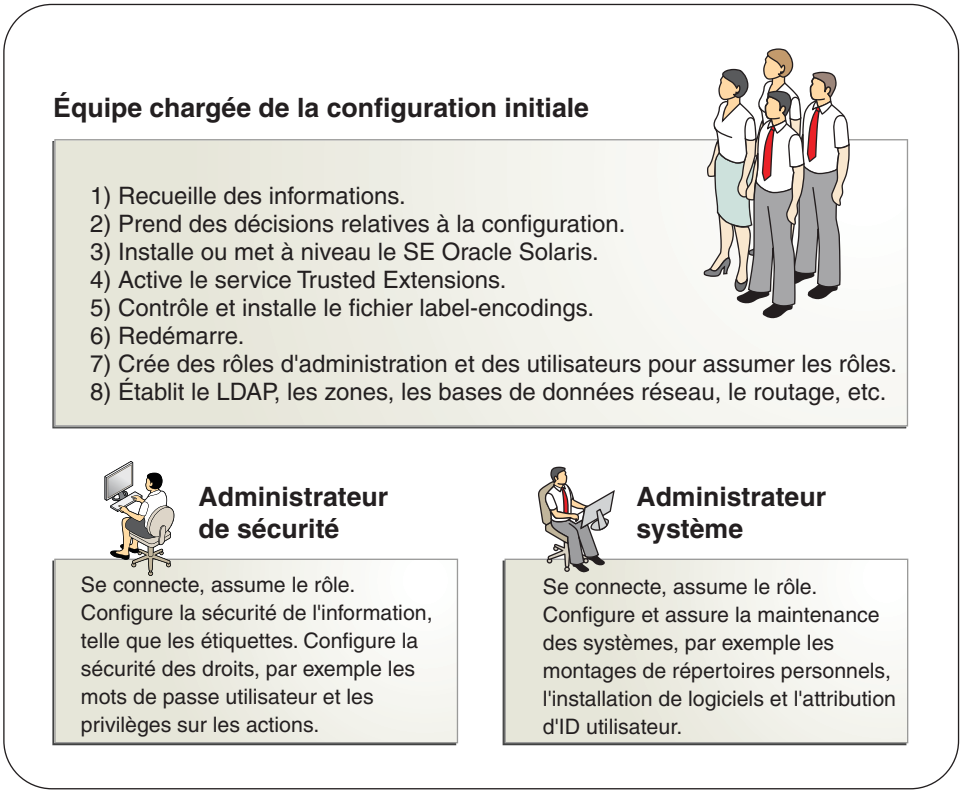
- Une seule personne active et configure le logiciel en assumant le rôle approprié. Le processus de configuration ne fait pas l'objet d'un contrôle.

  En utilisant cette stratégie, aucun enregistrement relatif au processus de configuration n'est conservé.
- L'utilisateur `root` active et configure le logiciel. Le processus de configuration fait l'objet d'un contrôle.

  L'équipe définit le contrôle de tous les événements de contrôle que l'utilisateur `root` effectue lors de la configuration. Avec cette stratégie, l'équipe doit déterminer les événements à contrôler. La piste d'audit n'inclut pas le nom de l'utilisateur `root`.
- L'utilisateur `root` active et configure le logiciel.

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 joindre aux zones et résoudre d'autres problèmes de sécurité. Pour connaître les procédures, reportez-vous à la section "Collecte d'informations et prise de décisions 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 redémarré, les fonctions de sécurité suivantes sont en place. De nombreuses fonctions peuvent être configurées par l'administrateur de sécurité.

- Le contrôle est activé.
- Un fichier label_encodings Oracle est installé et configuré.
- Deux ordinateurs de bureau de confiance sont ajoutés. Solaris Trusted Extensions (CDE) est la version sécurisée de CDE. Solaris Trusted Extensions (JDS) est la version sécurisée de Sun Java Desktop System. Chaque environnement multifenêtre crée des espaces de travail chemin de confiance dans la zone globale.
- Comme dans le SE Oracle Solaris, des profils de droits pour les rôles sont définis. Comme dans le SE Oracle Solaris, les rôles ne sont pas définis.

  Pour utiliser des rôles pour administrer Trusted Extensions, vous devez créer des 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. Les bases de données sont administrées à l'aide des outils Security Template et Trusted Network Zones de la Console de gestion Solaris.
- Trusted Extensions fournit des interfaces graphiques pour administrer le système. Certaines interfaces graphiques sont des extensions d'une interface graphique du Oracle Solaris.
  - Dans Trusted CDE, les actions d'administration sont fournies dans le dossier Trusted_Extensions. Certaines de ces actions sont utilisées lors de la configuration initiale de Trusted Extensions. Les outils sont présentés au Chapitre 2, “Outils d’administration de Trusted Extensions” du *Procédures de l’administrateur Oracle Solaris 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)`.
  - Un éditeur de confiance permet aux administrateurs de modifier les fichiers d'administration locaux. Dans Trusted CDE, l'action Admin Editor appelle un éditeur de confiance.
  - Le gestionnaire d'allocation de périphériques (Device Allocation Manager) gère les périphériques connectés.

- La Console de gestion Solaris fournit des outils Java destinés à la gestion des bases de données d'administration locales et réseau. L'utilisation de ces outils est nécessaire pour la gestion du réseau sécurisé, des zones et des utilisateurs.

◆ ◆ ◆ CHAPITRE 2

Déroulement de la configuration de Trusted Extensions

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

Liste des tâches : préparation d'un système Solaris pour Trusted Extensions

Assurez-vous que le SE Solaris sur lequel vous allez exécuter Trusted Extensions prend en charge les fonctions de Trusted Extensions que vous prévoyez d'utiliser. Procédez à l'une des deux tâches décrites dans la liste des tâches ci-dessous.

Tâche	Voir
Préparation d'une installation Solaris existante ou mise à niveau pour Trusted Extensions.	"Préparation d'un système Solaris installé pour Trusted Extensions" à la page 43
Installation du SE Solaris en prenant en compte les fonctionnalités de Trusted Extensions.	"Installation d'un système Solaris pour prendre en charge Trusted Extensions" à la page 42

Liste des tâches : préparation et activation de Trusted Extensions

Pour préparer un système Trusted Extensions avant de le configurer, effectuez les tâches décrites dans la liste des tâches ci-dessous.

Tâche	Voir
Préparation complète du système Solaris.	"Liste des tâches : préparation d'un système Solaris pour Trusted Extensions" à la page 35

Tâche	Voir
Sauvegarde du système.	Pour un système Trusted Solaris 8, sauvegardez le système comme décrit dans la documentation de votre version. Une sauvegarde étiquetée peut être restaurée sur chaque zone étiquetée de manière similaire.
	Pour un système Solaris, reportez-vous au *System Administration Guide: Basic Administration* .
Collecte d'informations et prise de décisions concernant votre système et votre réseau Trusted Extensions.	"Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions" à la page 46
Activation de Trusted Extensions.	"Activation de Trusted Extensions" à la page 49
Configuration du système.	Dans le cas d'un système comportant un moniteur, reportez-vous à la section "Liste des tâches : configuration de Trusted Extensions" à la page 37.
	Pour un écouteur, reportez-vous à la section "Configuration de l'écouteur dans Trusted Extensions (liste des tâches)" à la page 139.
	Pour un système Sun Ray, reportez-vous à la section *Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System* . Pour le système Sun Ray version 5, reportez-vous au site Web de documentation relative à Sun Ray Server 4.2 et Sun Ray Connector 2.2 (`http://wikis.sun.com/display/SRS/Home`). Ensemble, ce serveur et ce client constituent le package *Sun Ray 5*. Pour configurer la communication initiale client-serveur, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
	Pour un ordinateur portable, rendez-vous sur la page Web relative à la sécurité de la communauté OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`). Cliquez sur Trusted Extensions. Sur la page Trusted Extensions, sous Laptop Configurations (Configurations ordinateurs portables), cliquez sur `Laptop instructions` (Instructions pour les ordinateurs portables).
	Pour éviter que les réseaux ne communiquent avec la zone globale, configurez l'interface `vni0`. Pour obtenir un exemple, reportez-vous à la section `Laptop instructions`. À partir de la version Solaris 10 10/08, il n'est plus nécessaire de configurer l'interface `vni0`. Par défaut, l'interface `lo0` est une interface `all-zones`. Pour que le protocole DHCP fonctionne avec Trusted Extensions, d'autres instructions relatives aux ordinateurs portables s'appliquent toujours.

Liste des tâches : configuration de Trusted Extensions

Pour une configuration sécurisée, créez des rôles tôt dans le processus. L'ordre des tâches lorsque les rôles configurent le système est affiché dans la liste des tâches ci-dessous.

1. Configuration de la zone globale.

Tâches	Voir
Établissez une protection matérielle des machines en exigeant un mot de passe pour modifier les paramètres matériels.	"Controlling Access to System Hardware" du *System Administration Guide: Security Services*
Configurez les étiquettes. Les étiquettes *doivent* être configurées pour votre site. Si vous envisagez d'utiliser le fichier `label_encodings` par défaut, vous pouvez ignorer cette tâche.	"Vérification et installation du fichier de votre fichier label_encodings" à la page 52
Si vous exécutez un réseau IPv6, vous pouvez modifier le fichier `/etc/system` afin que l'IP reconnaisse les paquets étiquetés.	"Activation du réseau IPv6 dans Trusted Extensions" à la page 56
Si le domaine d'interprétation CIPSO de vos nœuds réseau est différent de `1`, spécifiez-le dans le fichier `/etc/system`.	"Configuration du domaine d'interprétation" à la page 57
Si vous prévoyez d'utiliser un instantané ZFS Solaris pour cloner des zones, créez le pool ZFS.	"Création d'un pool ZFS pour le clonage des zones" à la page 58
Initialisez pour activer un environnement étiqueté. Une fois connecté, vous êtes dans la zone globale. Le fichier `label_encodings` du système applique le contrôle d'accès obligatoire.	"Redémarrage et connexion à Trusted Extensions" à la page 59
Initialisez la Console de gestion Solaris. Cette interface graphique permet d'étiqueter les zones, entre autres tâches.	"Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61
Créez le rôle d'administrateur de sécurité et d'autres rôles que vous prévoyez d'utiliser localement. Ces rôles sont créés de la même manière que dans le SE Solaris. Vous pouvez reporter cette tâche jusqu'à la fin. Pour en connaître les conséquences, reportez-vous à la section "Élaboration d'une stratégie de configuration pour Trusted Extensions" à la page 29.	"Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92 "Vérification du fonctionnement des rôles Trusted Extensions" à la page 102

Ignorez les tâches suivantes si vous utilisez des fichiers locaux pour administrer le système.

2. Configuration d'un service de nommage.

Tâches	Voir
Si vous envisagez d'utiliser les fichiers pour administrer Trusted Extensions, vous pouvez ignorer les tâches suivantes.	Aucune configuration n'est nécessaire pour le service de nommage de fichiers.
Si vous disposez déjà d'un Sun Java System Directory Server (serveur LDAP), ajoutez des bases de données au serveur Trusted Extensions. Faites ensuite de votre premier système Trusted Extensions un proxy du serveur LDAP. Si vous ne disposez pas de serveur LDAP, configurez votre premier système en tant que serveur.	Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)"
Configurez manuellement une boîte à outils LDAP pour la Console de gestion Solaris. La boîte à outils peut être utilisée pour modifier les attributs Trusted Extensions des objets du réseau.	"Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132
Pour les systèmes qui ne sont pas le serveur LDAP ou un serveur proxy, faites-en un client LDAP.	"Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 64
Dans l'étendue LDAP, créez le rôle d'administrateur de sécurité et d'autres rôles que vous prévoyez d'utiliser. Vous pouvez reporter cette tâche jusqu'à la fin. Pour en connaître les conséquences, reportez-vous à la section "Élaboration d'une stratégie de configuration pour Trusted Extensions" à la page 29.	"Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92 "Vérification du fonctionnement des rôles Trusted Extensions" à la page 102

3. Création de zones étiquetées.

Tâches	Voir
Exécutez la commande `txzonemgr`. Suivez les menus pour configurer les interfaces réseau, puis créez et personnalisez la première zone étiquetée. Ensuite, copiez ou clonez le reste des zones.	"Création de zones étiquetées" à la page 68
Vous pouvez également utiliser des actions Trusted CDE.	Annexe B, "Utilisation d'actions CDE pour installer des zones dans Trusted Extensions"
(Facultatif) Une fois toutes les zones correctement personnalisées, ajoutez des adresses réseau spécifiques aux zones et un routage par défaut vers les zones étiquetées.	"Ajout d'interfaces réseau et acheminement vers les zones étiquetées" à la page 84

Les tâches suivantes peuvent être nécessaires dans votre environnement.

4. Configuration complète du système.

	Tâches	Voir
	Identifiez les autres hôtes distants qui nécessitent une étiquette, un ou plusieurs ports multiniveau ou une autre stratégie de message de contrôle.	"Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*
	Créez un serveur d'annuaires personnel multiniveau, puis exécutez un montage automatique des zones installées.	"Création de répertoires personnels dans Trusted Extensions" à la page 104
	Configurez le contrôle, montez les systèmes de fichiers et effectuez d'autres tâches avant de permettre aux utilisateurs de se connecter au système.	*Procédures de l'administrateur Oracle Solaris Trusted Extensions*
	Ajoutez des utilisateurs à votre serveur LDAP à partir d'un environnement NIS.	"Ajout d'un utilisateur NIS au serveur LDAP" à la page 107
	Ajoutez un hôte et ses zones étiquetées au serveur LDAP.	"Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

◆ ◆ ◆ CHAPITRE 3

Ajout du logiciel Trusted Extensions au SE Solaris (tâches)

Ce chapitre décrit la préparation du SE Solaris pour le logiciel Trusted Extensions. Ce chapitre décrit également toutes les informations nécessaires avant d'activer Trusted Extensions. Vous y trouverez aussi des instructions sur l'activation de Trusted Extensions.

- "Responsabilités de l'équipe chargée de la configuration initiale" à la page 41
- "Installation ou mise à niveau du SE Solaris pour Trusted Extensions" à la page 42
- "Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions" à la page 46
- "Activation du service Trusted Extensions" à la page 49

Responsabilités de l'équipe chargée de la configuration initiale

Le logiciel Trusted Extensions est conçu pour être activé et configuré par deux personnes possédant des responsabilités distinctes. Cependant, le programme d'installation de Solaris n'applique pas cette séparation des tâches entre deux rôles. Au contraire, la séparation des tâches est effectuée par les rôles. Les rôles·et les utilisateurs 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.

Installation ou mise à niveau du SE Solaris pour Trusted Extensions

Le choix des options d'installation de 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 correctement installer le SE Solaris sous-jacent. Pour connaître les choix d'installation de Solaris qui affectent Trusted Extensions, reportez-vous à la section "Installation d'un système Solaris pour prendre en charge Trusted Extensions" à la page 42.
- Si vous utilisiez le SE Solaris, vérifiez votre configuration actuelle par rapport à la configuration requise de Trusted Extensions. Pour connaître les choix de configuration qui affectent Trusted Extensions, reportez-vous à la section "Préparation d'un système Solaris installé pour Trusted Extensions" à la page 43.

▼ Installation d'un système Solaris pour prendre en charge Trusted Extensions

Cette tâche s'applique aux nouvelles installations du SE Solaris. Si vous procédez à une mise à niveau, reportez-vous à la section "Préparation d'un système Solaris installé pour Trusted Extensions" à la page 43.

- **Lors de l'installation du SE Solaris, appliquez l'action recommandée parmi les choix d'installation suivants.**

  Les choix suivent l'ordre des questions relatives à l'installation de Solaris. Les questions relatives à l'installation qui ne sont pas mentionnées dans ce tableau n'affectent pas Trusted Extensions.

Options Solaris	Comportement de Trusted Extensions	Action recommandée
Service de nommage NIS Service de nommage NIS+	Trusted Extensions prend en charge les fichiers et LDAP comme service de nommage. Pour la résolution de noms d'hôte, DNS peut être utilisé.	Ne choisissez pas NIS ou NIS+. Vous pouvez sélectionner l'option None (Aucun), ce qui est équivalent aux fichiers. Vous pouvez configurer LDAP ultérieurement avec Trusted Extensions.
Mise à niveau	Trusted Extensions installe des zones étiquetées avec des caractéristiques de sécurité particulières.	Si vous procédez à une mise à niveau, reportez-vous à la section "Préparation d'un système Solaris installé pour Trusted Extensions" à la page 43.

Options Solaris	Comportement de Trusted Extensions	Action recommandée
Mot de passe `root`	Les outils d'administration dans Trusted Extensions requièrent des mots de passe. Si l'utilisateur `root` ne dispose pas de mot de passe, `root` ne peut pas configurer le système.	Fournissez un mot de passe `root`. Ne modifiez pas la méthode de chiffrement par mot de passe `crypt_unix` par défaut. Pour plus d'informations, reportez-vous à la section "Managing Password Information" du *System Administration Guide: Security Services*.
Groupe Développeur	Trusted Extensions utilise la Console de gestion Solaris pour administrer le réseau. Le groupe Utilisateur final et des groupes plus petits n'installent pas les packages pour la Console de gestion Solaris.	Sur n'importe quel système que vous envisagez d'utiliser pour administrer d'autres systèmes, n'installez pas de groupe Utilisateur final, Core ou Réseau réduit.
Installation personnalisée	Trusted Extensions installe des zones, de sorte qu'il vous faudra peut-être plus d'espace disque dans les partitions que l'installation par défaut ne fournit.	Choisissez Custom Install (Installation personnalisée) et configurez les partitions. Envisagez d'ajouter l'espace de swap supplémentaire pour les rôles. Si vous prévoyez de cloner des zones, créez une partition de 2 000 Mo pour le pool ZFS. Pour le contrôle des fichiers, il est préférable de créer une partition dédiée.

▼ Préparation d'un système Solaris installé pour Trusted Extensions

Cette tâche s'applique aux systèmes Solaris existants et sur lesquels vous prévoyez d'exécuter Trusted Extensions. Effectuez également cette procédure pour exécuter Trusted Extensions sur un système Solaris mis à niveau. D'autres tâches susceptibles de modifier un système Solaris installé peuvent être effectuées lors de la configuration de Trusted Extensions.

Avant de commencer

Trusted Extensions ne peut pas être activé dans certains environnements Solaris :

- Si votre système fait partie d'un cluster, Trusted Extensions ne peut pas être activé sur le système.
- L'activation de Trusted Extensions dans un environnement d'initialisation alternatif n'est pas prise en charge. Trusted Extensions ne peut être activé que dans l'environnement d'initialisation actif.

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

Vous pouvez également réinstaller le SE Solaris. Si vous réinstallez le SE Solaris, suivez les instructions de la section "Installation d'un système Solaris pour prendre en charge Trusted Extensions" à la page 42.

Trusted Extensions utilise des zones marquées.

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

Les outils d'administration dans Trusted Extensions requièrent des mots de passe. Si l'utilisateur `root` ne dispose pas de mot de passe, `root` ne peut pas configurer le système.

Utilisez la méthode de chiffrement par mot de passe `crypt_unix` par défaut pour l'utilisateur `root`. Pour plus d'informations, reportez-vous à la section "Managing Password Information" du *System Administration Guide: Security Services*.

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. Le SE Solaris fournit une protection contre les mots de passe non sécurisés, mais ne peut pas empêcher un utilisateur de divulguer son mot de passe ou de l'écrire.

---

3 **Si vous envisagez d'administrer le site à partir de ce système, ajoutez-y les packages Solaris pour la Console de gestion Solaris.**

Trusted Extensions utilise la Console de gestion Solaris pour administrer le réseau. Si le système a été installé avec le groupe End User ou un groupe plus petit, le système ne dispose pas des packages pour la Console de gestion Solaris.

4 **Si vous avez créé un fichier `xorg.conf`, vous devez le modifier.**

Ajoutez la ligne suivante à la fin de la section Module du fichier `/etc/X11/xorg.conf`.

```
load "xtsol"
```

Remarque – Par défaut, le fichier `xorg.conf` n'existe pas. Si c'est le cas, ne faites rien.

---

5 **Dans les versions Solaris 10 9/09 et Solaris 10 9/10, si votre système fait partie d'une configuration Oracle Solaris Cluster, vous pouvez activer Trusted Extensions dans le cluster.**

Remarque – Les applications doivent s'exécuter uniquement dans les clusters de zone Oracle Solaris Cluster.

Pour en savoir plus sur la prise en charge d'Oracle Solaris Cluster par Trusted Extensions, reportez-vous à la section Préparation de l'utilisation de Trusted Extensions avec des clusters de zone du Chapitre 7, Création de zones non globales et de clusters de zone du *Oracle Solaris Cluster Software Installation Guide* .

6 **Si vous mettez à niveau un système Trusted Extensions, lisez les informations suivantes avant de procéder :**

- Chapitre 1, “Nouveautés de la version Solaris 10 10/08,” du guide *Nouveautés de Solaris10*
- *Notes de version de Solaris 10 10/08*

Astuce – Pour trouver les informations pertinentes, recherchez la chaîne `Trusted Extensions`.

---

7 **Si vous prévoyez de cloner des zones, créez une partition pour le pool ZFS.**

Pour décider de votre méthode de création de zone, reportez-vous à la section “Planification de zones dans Trusted Extensions” à la page 24.

8 **Si vous prévoyez d'installer des zones étiquetées sur ce système, vérifiez que vos partitions disposent d'un espace disque suffisant pour les zones.**

La plupart des systèmes configurés avec Trusted Extensions installent des zones étiquetées. Les zones étiquetées peuvent nécessiter plus d'espace disque que ce que le système installé a prévu.

Cependant, certains systèmes Trusted Extensions ne nécessitent pas l'installation de zones étiquetées. Par exemple, un serveur d'impression multiniveau, un serveur LDAP multiniveau ou un serveur proxy LDAP multiniveau ne nécessitent pas de zones étiquetées pour être installés. Ces systèmes n'ont pas forcément besoin d'espace disque supplémentaire.

9 **(Facultatif) Ajoutez de l'espace de swap supplémentaire pour les rôles.**

Les rôles administrent Trusted Extensions. Envisagez l'ajout de swap supplémentaire pour les processus de rôle.

10 **(Facultatif) Dédiez une partition aux fichiers de contrôle.**

Trusted Extensions active le contrôle par défaut. Pour les fichiers de contrôle, il est préférable de créer une partition dédiée.

11 **(Facultatif) Pour exécuter une configuration sécurisée, exécutez la commande `netservices limited` avant d'activer Trusted Extensions.**

```
# netservices limited
```

Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions

Pour chaque système sur lequel Trusted Extensions va être configuré, vous devez connaître certaines informations et prendre des décisions relatives à la configuration. Par exemple, si vous prévoyez de créer des zones étiquetées, vous pouvez souhaiter réserver de l'espace disque où les zones pourront être clonées en tant que système de fichiers ZFS Solaris. Le ZFS Solaris offre un isolement supplémentaires pour les zones.

▼ Collecte d'informations système avant l'activation de Trusted Extensions

1 Déterminez le nom d'hôte et l'adresse IP du système principal.

Le nom d'hôte est le nom de l'hôte sur le réseau et correspond à la zone globale. Sur un système Solaris, la commande `getent` renvoie le nom d'hôte, comme suit :

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

2 Déterminez les allocations d'adresses IP des zones étiquetées.

Un système doté de deux adresses IP peut fonctionner comme un serveur multiniveau. Un système doté d'une adresse IP doit disposer d'un accès à un serveur multiniveau afin d'effectuer des tâches d'impression ou multiniveau. Pour obtenir une description des options d'adresse IP, reportez-vous à la section "Planification pour l'accès multiniveau" à la page 26.

La plupart des systèmes exigent une seconde adresse IP pour les zones étiquetées. Par exemple, l'hôte suivant contient une deuxième adresse IP pour les zones étiquetées :

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

3 Collectez les informations de configuration LDAP.

Pour le serveur LDAP qui exécute le logiciel Trusted Extensions, vous avez besoin des informations suivantes :

- Le nom du domaine Trusted Extensions servi par le serveur LDAP
- L'adresse IP du serveur LDAP
- Le nom du profil LDAP qui sera chargé

Pour un serveur proxy LDAP, vous aurez également besoin du mot de passe pour le proxy LDAP.

▼ Prise de décisions relatives au système et 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.**

Sur un site sécurisé, cette étape a été effectuée pour chaque système Solaris installé.

- Pour les systèmes SPARC, un niveau de sécurité PROM et un mot de passe ont été fournis.
- Pour les systèmes x86, le BIOS est protégé.
- Sur tous les systèmes, l'utilisateur `root` est protégé par 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 Sun. Oracle fournit également d'autres fichiers `label_encodings`, que vous pouvez trouver dans le répertoire `/etc/security/tsol`. Les fichiers Sun 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 *Oracle Solaris 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.**

Le tableau ci-dessous répertorie les noms d'étiquettes et les noms de zones suggérés pour le fichier `label_encodings` par défaut.

Étiquette	Nom de zone
`PUBLIC`	`public`
`CONFIDENTIAL : INTERNAL`	`internal`
`CONFIDENTIAL : NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL : RESTRICTED`	`restricted`

Pour simplifier le montage NFS, le nom de zone d'une étiquette donnée doit être identique sur tous les systèmes. Certains systèmes, tels que serveurs d'impression multiniveau, ne nécessitent pas l'installation de zones étiquetées. Cependant, si vous installez des zones étiquetées sur un serveur d'impression, les noms de zones doivent être identiques à ceux des autres systèmes de votre réseau.

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, vous pouvez choisir de configurer le système en tant que superutilisateur. Cette méthode de configuration est moins sûre. Les enregistrements de contrôle n'indiquent pas l'identité de l'utilisateur qui a été superutilisateur lors de la configuration. Le superutilisateur peut exécuter toutes les tâches sur le système, tandis qu'un rôle peut effectuer un nombre plus limité de tâches. Par conséquent, la configuration est plus contrôlée lorsqu'elle est effectuée par les rôles.

5 **Choisissez une méthode de création de zone.**

Vous pouvez créer des zones à partir de zéro, les copier ou les cloner. Ces méthodes diffèrent en termes de vitesse de création, d'espace disque requis et de fiabilité. Pour plus d'informations sur les compromis, reportez-vous à la section "Planification de zones dans Trusted Extensions" à la page 24.

6 **Planifiez votre configuration LDAP.**

L'utilisation de fichiers locaux pour l'administration est pratique pour les systèmes qui ne sont pas en réseau.

LDAP est le service de nommage pour un environnement en réseau. Un serveur LDAP rempli est nécessaire lorsque vous configurez plusieurs machines.

- Si vous disposez déjà d'un Sun Java System Directory Server (serveur LDAP), vous pouvez créer un serveur proxy LDAP sur un système qui exécute Trusted Extensions. Le serveur proxy multiniveau gère les communications avec le serveur LDAP sans étiquette.
- Si vous ne disposez pas de serveur LDAP, vous pouvez configurer un système qui exécute le logiciel Trusted Extensions en tant que serveur LDAP multiniveau.

7 **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

Depuis la version Solaris 10 5/08, 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.

▼ Activation de Trusted Extensions

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 "Installation ou mise à niveau du SE Solaris pour Trusted Extensions" à la page 42 et "Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions" à la page 46.

1 Sur un Solaris, activez le service `labeld`.

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

Le service `labeld` ajoute des étiquettes au système et lance le service de contrôle et l'allocation des périphériques Solaris. N'effectuez pas d'autres tâches jusqu'à ce que le curseur revienne à l'invite.

2 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.
```

Remarque – Les étiquettes ne s'affichent qu'après redémarrage du système. La section "Configuration de la zone globale dans Trusted Extensions" à la page 51 inclut des tâches que vous pouvez être amené à effectuer avant de redémarrer.

Erreurs fréquentes

Les message suivants indiquent que vous n'exécutez pas une version de Solaris prenant en charge Trusted Extensions en tant que service : `svcs: Pattern 'labeld' doesn't match any instances`.

Pour exécuter Trusted Extensions sur un système Solaris ne prenant pas en charge le service `labeld`, suivez les instructions du guide *Installation et configuration de Solaris Trusted Extensions*.

◆ ◆ ◆ 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 nécessite la configuration des éléments suivants : étiquettes, zones, réseau, utilisateurs pouvant assumer les rôles, rôles et outils.

- "Configuration de la zone globale dans Trusted Extensions" à la page 51
- "Création de zones étiquetées" à la page 68
- (Facultatif) "Ajout d'interfaces réseau et acheminement vers les zones étiquetées" à la page 84
- "Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92
- "Création de répertoires personnels dans Trusted Extensions" à la page 104
- "Ajout d'utilisateurs et d'hôtes à un réseau Trusted Network existant" à la page 107
- "Dépannage de votre configuration Trusted Extensions" à la page 110
- "Tâches de configuration supplémentaires de Trusted Extensions" à la page 113

Pour d'autres tâches de configuration, reportez-vous aux *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Configuration de la zone globale dans Trusted Extensions

Avant de configurer la zone globale, vous devez prendre des décisions concernant votre configuration. Pour en savoir plus sur la prise de décisions, reportez-vous à la section "Collecte d'informations et prise de décisions avant l'activation de Trusted Extensions" à la page 46.

Tâche	Description	Voir
Protection du matériel.	Le matériel peut être protégé en demandant un mot de passe pour modifier les paramètres matériels.	"Controlling Access to System Hardware" du *System Administration Guide: Security Services*

Tâche	Description	Voir
Configuration des étiquettes.	Les étiquettes *doivent* être configurées pour votre site. Si vous envisagez d'utiliser le fichier `label_encodings` par défaut, vous pouvez ignorer cette étape.	"Vérification et installation du fichier de votre fichier label_encodings" à la page 52
Pour IPv6, modification du fichier `/etc/system`.	Si vous exécutez un réseau IPv6, vous pouvez modifier le fichier `/etc/system` afin que l'IP reconnaisse les paquets étiquetés.	"Activation du réseau IPv6 dans Trusted Extensions" à la page 56
Pour un DOI dont la valeur n'est pas `1`, modification du fichier `/etc/system`.	Si le domaine d'interprétation CIPSO de vos nœuds réseau est différent de `1`, spécifiez-le dans le fichier `/etc/system`.	"Configuration du domaine d'interprétation" à la page 57
Création de l'espace pour un instantané ZFS Solaris.	Si vous prévoyez d'utiliser un instantané ZFS Solaris pour cloner des zones, créez le pool ZFS. Effectuez cette tâche si vous allez cloner la première zone pour créer le reste des zones étiquetées.	"Création d'un pool ZFS pour le clonage des zones" à la page 58
Redémarrage et connexion.	Une fois connecté, vous êtes dans la zone globale, qui est un environnement qui reconnaît et met en œuvre le contrôle d'accès obligatoire.	"Redémarrage et connexion à Trusted Extensions" à la page 59
Initialisation de la Console de gestion Solaris.	Trusted Extensions ajoute des outils à la Console de gestion Solaris pour l'administration des utilisateurs, des rôles, des zones et du réseau.	"Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61
Configuration d'un LDAP.	Si vous utilisez le service de nommage LDAP, configurez le service LDAP.	Chapitre 5, "Configuration de LDAP pour Trusted Extensions (tâches)"
	Si vous avez configuré le service LDAP, faites de ce système un client LDAP.	"Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 64

▼ Vérification et installation du fichier de votre 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 familier avec les fichiers de codage, consultez la section *Oracle Solaris 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)`.

1. **Insérez le support contenant le fichier `label_encodings` dans le périphérique approprié.**
2. **Copiez le fichier `label_encodings` sur le disque.**
3. **Vérifiez la syntaxe du fichier et faites-en le fichier `label_encodings` actif.**
   - **Dans Trusted JDS, vérifiez et installez le fichier à partir de la ligne de commande.**
     a. **Ouvrez une fenêtre de terminal.**
     b. **Exécutez la commande `chk_encodings`.**

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

     c. **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, “Making a Label Encodings File (Tasks)” du *Oracle Solaris 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* passer le test `chk_encodings` avant de pouvoir continuer.

- **Dans Trusted CDE, utilisez l'action Check Encodings (Vérifier le fichier de codage).**

  a. **Ouvrez le dossier Trusted_Extensions.**

     Avec la souris, cliquez sur le bouton 3 sur l'arrière-plan.

  b. **Dans le menu Workspace (Espace de travail), sélectionnez Applications → Application Manager (Applications → Gestionnaire d'applications).**

  c. **Double-cliquez sur l'icône du dossier Trusted_Extensions.**

  d. **Double-cliquez sur l'action Check Encodings (Vérifier le fichier de codage).**

     Dans la boîte de dialogue qui s'affiche, entrez le nom du chemin d'accès complet au fichier :

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

     La commande `chk_encodings` est appelée pour vérifier la syntaxe du fichier. Les résultats sont affichés dans la boîte de dialogue de vérification du fichier de codage (Check Encodings).

  e. **Lisez le contenu de la boîte de dialogue Check Encodings (Vérification du fichier de codage) et effectuez l'une des opérations suivantes :**

     - **Résolvez les erreurs.**

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

     - **Cliquez sur `Yes` (Oui) pour faire du fichier le fichier `label_encodings` actif.**

       L'action Check Encodings (Vérifier le fichier de codage) entraîne la création d'une copie de sauvegarde du fichier d'origine, puis installe la version vérifiée dans `/etc/security/tsol/label_encodings`. L'action redémarre alors le démon d'étiquette.

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

4 **Vérifiez la syntaxe du fichier et faites-en le fichier `label_encodings` actif.**

Utilisez la ligne de commande.

a. **Ouvrez une fenêtre de terminal.**

b. Exécutez la commande `chk_encodings`.

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

c. 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, “Making a Label Encodings File (Tasks)” du *Oracle Solaris 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* passer 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 10/10/2006

---> 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.10.10.06
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.06 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 10/10/2006
```

▼ Activation du réseau IPv6 dans Trusted Extensions

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`.

- **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 n'a pas été redémarré après l'ajout de l'entrée correcte au fichier `/etc/system`.
- Si vous installez Trusted Extensions sur un système Solaris sur lequel IPv6 est actuellement activé, mais 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*
- Si vous installez Trusted Extensions sur un système Solaris sur lequel IPv6 n'est pas activé et si vous n'avez pas réussi à ajouter l'entrée IP dans le fichier `/etc/system`, l'un des types suivants de messages d'erreur s'affiche :
  - `WARNING: IPv6 not enabled via /etc/system`
  - `Failed to configure IPv6 interface(s): hme0`

- `rpcbind: Unable to join IPv6 multicast group for rpc broadcast` *broadcast-number*

Configuration du domaine d'interprétation

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 DOI n'est pas `1`, vous devez ajouter une entrée dans le fichier `/etc/system` et modifier la valeur `doi` dans les modèles de sécurité par défaut.

1 Saisissez votre entrée DOI dans le fichier `/etc/system` :

```
set default_doi = n
```

Ce numéro positif, autre que zéro, doit correspondre au numéro DOI dans la base de données `tnrhtp` pour votre nœud et les systèmes avec lesquels votre nœud communique.

2 Avant d'ajouter la base de données `tnrhtp` au serveur LDAP, modifiez la valeur `doi` dans les entrées par défaut et toutes les entrées pour les adresses locales.

Trusted Extensions fournit deux modèles dans la base de données `tnrhtp`, `cipso` et `admin_low`. Si vous avez ajouté des entrées pour les adresses locales, modifiez également ces entrées.

a. Ouvrez la base de données `tnrhtp` dans l'éditeur de confiance.

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

Dans Solaris Trusted Extensions (CDE), vous pouvez également utiliser l'action Admin Editor dans le dossier Trusted_Extensions du Gestionnaire d'applications.

b. Copiez l'entrée de modèle `cipso` sur une autre ligne.

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

c. Commentez l'une des entrées `cipso`.

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

d. Modifiez la valeur `doi` dans l'entrée `cipso` non commentée.

Définissez cette valeur sur une valeur identique à la valeur `default_doi` dans le fichier `/etc/system`.

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

e. Modifiez la valeur `doi` pour l'entrée `admin_low`.

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

Vous avez terminé lorsque toutes les valeurs `doi` de toutes les entrées de la base de données `tnrhtp` sont identiques.

Erreurs fréquentes

Si le fichier `/etc/system` définit une valeur `default_doi` autre que `1` et si un modèle de sécurité pour ce système définit une valeur qui ne correspond pas à cette valeur `default_doi`, des messages similaires au suivant s'affichent sur la console du système pendant la configuration de l'interface :

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

L'échec de la configuration de l'interface peut entraîner l'échec de la connexion :

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

Pour corriger le problème, démarrez le système en mode mono-utilisateur et corrigez les modèles de sécurité comme décrit dans cette procédure.

Voir aussi

Pour de plus amples informations sur le DOI, reportez-vous à la section "Attributs de sécurité réseau dans Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Pour changer la valeur `doi` dans les modèles de sécurité que vous créez, reportez-vous à la section "Procédure de construction d'un modèle d'hôte distant" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Pour utiliser l'éditeur de votre choix en tant qu'éditeur de confiance, reportez-vous à la section "Affectation de l'éditeur de votre choix en tant qu'éditeur de confiance" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

▼ Création d'un pool ZFS pour le clonage des zones

Si vous envisagez d'utiliser un instantané ZFS Solaris comme modèle de zone, vous devez créer un pool ZFS à partir d'un fichier ZFS ou d'un périphérique ZFS. Ce pool contient l'instantané pour le clonage de chaque zone. Vous utilisez le périphérique `/zone` pour le pool ZFS.

Avant de commencer

Vous avez mis de côté de l'espace disque pendant l'installation d'Solaris, pour un système de fichiers ZFS. Pour en savoir plus, reportez-vous à la section "Planification de zones dans Trusted Extensions" à la page 24.

1. **Démontez la partition `/zone`.**

   Au cours de l'installation, vous avez créé une partition `/zone` d'environ 2 000 Mo contenant suffisamment d'espace disque.

   ```
   # umount /zone
   ```

2. **Supprimez le point de montage `/zone`.**

   ```
   # rmdir /zone
   ```

3. **Commentez l'entrée `/zone` dans le fichier `vfstab`.**

   a. **Empêchez l'entrée `/zone` d'être lue.**

      Ouvrez le fichier `vfstab` dans un éditeur. Ajoutez un préfixe à l'entrée `/zone` avec une marque de commentaire.

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

   b. **Copiez la tranche de disque, `cn tndn sn`, dans le presse-papiers.**

   c. **Enregistrez le fichier et quittez l'éditeur.**

4. **Utilisez la tranche de disque pour recréer `/zone` sous la forme d'un pool ZFS.**

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

   Par exemple, si votre entrée `/zone` utilise la tranche de disque `c0t0d0s5`, alors la commande sera la suivante :

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

5. **Vérifiez si le pool ZFS est en bon état de fonctionnement.**

   Utilisez l'une des commandes suivantes :

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

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

   Dans cet exemple, l'équipe chargée de la configuration initiale a réservé une partition de 6 000 Mo pour les zones. Pour plus d'informations, reportez-vous à la page de manuel `zpool(1M)`.

▼ Redémarrage et connexion à Trusted Extensions

Sur la plupart des sites, au moins deux administrateurs, qui composent l'équipe chargée de la configuration initiale, sont présents lors de la configuration du système.

Avant de commencer

Avant la première connexion, familiarisez-vous avec le bureau et les options d'étiquette de Trusted Extensions. Pour plus d'informations, reportez-vous au Chapitre 2, “Connexion à Trusted Extensions (tâches)” du *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

1 Redémarrez le système.

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

Si votre système ne dispose pas d'affichage graphique, passez au Chapitre 6, “Configuration d'un écouteur avec Trusted Extensions (tâches)”.

2 Connectez-vous en tant que superutilisateur au bureau Solaris Trusted Extensions (CDE) ou Solaris Trusted Extensions (JDS).

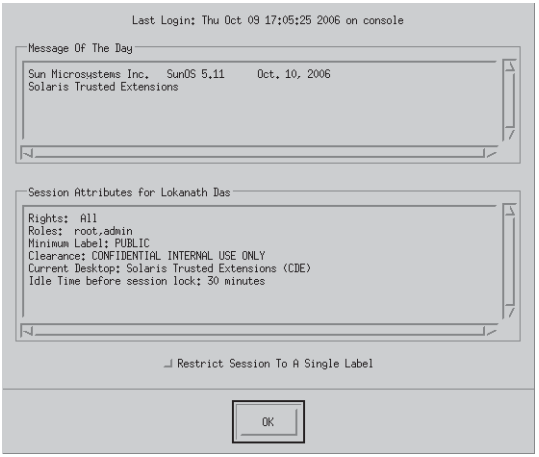
a. Dans la fenêtre de connexion, sélectionnez l'un des ordinateurs de confiance.

Le bureau Trusted CDE contient des actions qui sont utiles lors de la configuration du système. À partir de la version Solaris 10 10/08, le script `txzonemgr` est le programme préféré pour la configuration du système.

b. Dans la boîte de dialogue de connexion, tapez `root` et le mot de passe root.

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. Le logiciel Trusted Extensions assure une protection contre les mots de passe non sécurisés, mais ne peut pas empêcher un utilisateur de divulguer son mot de passe ou de l'écrire.

3 Lisez les informations dans la boîte de dialogue Last Login (Dernière connexion).



Cliquez sur OK pour fermer la boîte de dialogue.

4 **Lisez le générateur d'étiquettes (Label Builder).**

Cliquez sur OK pour accepter l'étiquette par défaut.

Une fois le processus de connexion terminé, l'écran Trusted Extensions s'affiche brièvement, et vous vous trouvez dans une session de bureau avec quatre espaces de travail. Le symbole `Trusted Path` s'affiche dans la bande de confiance.

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.

▼ Initialisation du serveur Console de gestion Solaris dans Trusted Extensions

Cette procédure vous permet d'administrer les utilisateurs, les rôles, les hôtes, les zones et le réseau sur ce système. Sur le premier système que vous configurez, seule l'étendue `files` est disponible.

Avant de commencer Vous devez être connecté en tant que superutilisateur.

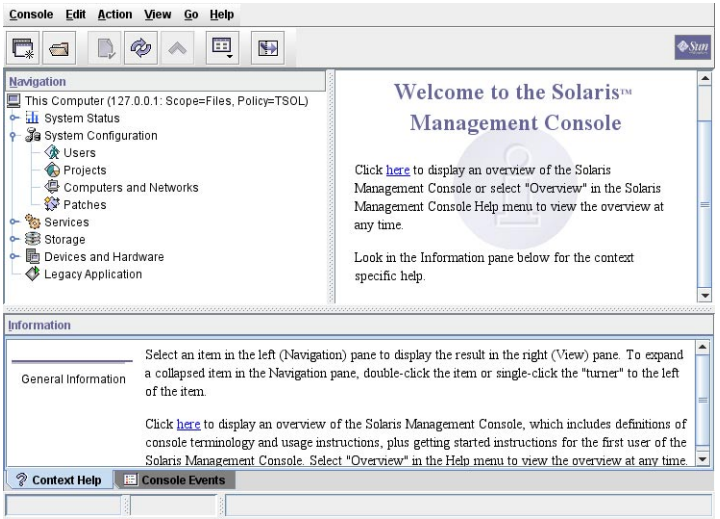
Pour utiliser la boîte à outils LDAP sur le serveur LDAP à partir d'une console de gestion Solaris qui s'exécute sur un client, vous devez d'abord terminer toutes les tâches de la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132.

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

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

Remarque – Lors du premier démarrage de la Console de gestion Solaris, plusieurs tâches d'enregistrement sont effectuées. Cela peut prendre quelques minutes.

FIGURE 4–1 Fenêtre initiale de la Console de gestion Solaris



2 **Exécutez l'une des procédures suivantes si les icônes de la boîte à outils n'apparaissent pas dans la Console de gestion Solaris :**

- **Si le volet Navigation n'est pas visible :**

  a. **Dans la boîte de dialogue Open Toolbox (Ouvrir boîte à outils) qui s'affiche, cliquez sur Load (Charger) en regard du nom de ce système sous Server (Serveur).**

  Si ce système ne dispose pas de la quantité recommandée de mémoire et de swap, les boîtes à outils peuvent mettre quelques minutes à s'afficher. Pour obtenir des conseils, reportez-vous à la section "Installation ou mise à niveau du SE Solaris pour Trusted Extensions" à la page 42.

  b. **Dans la liste des boîtes à outils, sélectionnez une boîte à outils avec la stratégie `Policy=TSOL`.**

  La Figure 4–2 représente une boîte à outils Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`). Trusted Extensions modifie les outils sous le nœud System Configuration (Configuration système).

Attention – Ne choisissez pas de boîte à outils qui n'a pas de stratégie. Les boîtes à outils n'ayant pas de stratégie répertoriée ne prennent pas en charge Trusted Extensions.

Votre choix de boîte à outils dépend de l'étendue que vous souhaitez influencer.

- Pour modifier les fichiers locaux, sélectionnez l'étendue Files (Fichiers).
- Pour modifier les bases de données LDAP, choisissez l'étendue LDAP.

Une fois toutes les tâches de la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132 effectuées, l'étendue LDAP est disponible.

c. Cliquez sur Open (Ouvrir).

- **Si le volet Navigation est visible, mais des signes Stop apparaissent à la place des icônes de la boîte à outils :**

  a. Quittez la Console de gestion Solaris.

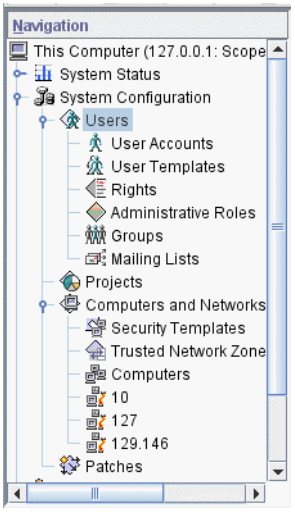
  b. Redémarrez la Console de gestion Solaris.

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

3 Si ce n'est pas encore fait, sélectionnez une boîte à outils avec la stratégie `Policy=TSOL` .

La figure suivante montre une boîte à outils Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`). Trusted Extensions modifie les outils sous le nœud System Configuration (Configuration système).

FIGURE 4–2 Outils Trusted Extensions dans la Console de gestion Solaris



4 **(Facultatif) Enregistrez la boîte à outils active.**

L'enregistrement d'une boîte à outils `Policy=TSOL` permet le chargement par défaut de la boîte à outils Trusted Extensions. Les préférences sont enregistrées par rôle, par hôte. L'hôte est le serveur Console de gestion Solaris.

a. **Choisissez Preferences (Préférences) dans le menu Console.**

La boîte à outils Home est sélectionnée.

b. **Définissez une boîte à outils `Policy=TSOL` en tant que boîte à outils Home.**

Placez la boîte à outils active dans le champ Location (Emplacement) en cliquant sur le bouton Use Current Toolbox (Utiliser la boîte à outils actuelle).

c. **Cliquez sur OK pour enregistrer les préférences.**

5 **Quittez la Console de gestion Solaris.**

Voir aussi Pour une présentation des ajouts de Trusted Extensions à la Console de gestion Solaris, reportez-vous à la section "Outils de la Console de gestion Solaris" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*. Pour utiliser la Console de gestion Solaris pour créer des modèles de sécurité, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

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

Pour LDAP, cette procédure permet d'établir la configuration du service de nommage pour la zone globale. Si vous n'utilisez pas LDAP, vous pouvez ignorer cette procédure.

À partir de la version Solaris 10 5/08, si vous êtes dans un espace de travail Solaris Trusted Extensions (CDE), vous pouvez utiliser le script `txzonemgr` ou une action Trusted CDE pour créer un client LDAP. Si vous êtes dans un espace de travail Solaris Trusted Extensions (JDS) ou Solaris Trusted Extensions (GNOME), vous devez utiliser 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 Sun Java System Directory Server, c'est-à-dire le serveur LDAP, doit exister. Le serveur doit être rempli avec les bases de données Trusted Extensions, et ce système doit être en mesure de

contacter le serveur. Ainsi, le système que vous configurez doit disposer d'une entrée dans la base de données `tnrhdb` sur le serveur LDAP, ou ce système doit être inclus dans une entrée générique avant d'exécuter cette procédure.

S'il n'y a aucun serveur LDAP configuré avec Trusted Extensions, vous devez effectuer les procédures décrites au Chapitre 5, “Configuration de LDAP pour Trusted Extensions (tâches)” avant d'exécuter celle-ci.

1 Si vous utilisez DNS, modifiez le fichier `nsswitch.ldap`.

a. Enregistrez une copie du fichier `nsswitch.ldap` original.

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

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

b. Modifiez les entrées du fichier `nsswitch.ldap` pour les services suivants.

Les entrées correctes sont similaires aux suivantes :

```
hosts:    files dns ldap

ipnodes:    files dns ldap

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

services:   files
```

Notez que Trusted Extensions ajoute deux entrées :

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

c. Copiez le fichier `nsswitch.ldap` modifié sur `nsswitch.conf`.

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

2 Effectuez l'une des étapes suivantes pour créer un client LDAP.

- **Exécutez le script `txzonemgr` et répondez aux invites relatives à LDAP.**

  L'option de menu Create LDAP Client (Créer client LDAP) permet de configurer la zone globale uniquement.

  a. **Suivez les instructions de la section "Exécution du script `txzonemgr`" à la page 69.**

     Le titre de la boîte de dialogue est Labeled Zone Manager (Gestionnaire de zones étiquetées).

  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 validez, le script `txzonemgr` ajoute le client LDAP. Ensuite, une fenêtre affiche la sortie de la commande.

- **Dans un espace de travail Trusted CDE, trouvez et utilisez l'action Create LDAP Client (Créer client LDAP).**

  a. **Accédez au dossier Trusted_Extensions en cliquant sur bouton de souris 3 à l'arrière-plan.**

  b. **Dans le menu Workspace (Espace de travail), sélectionnez Applications → Application Manager (Applications → Gestionnaire d'applications).**

  c. **Double-cliquez sur l'icône du dossier Trusted_Extensions.**

     Ce dossier contient des actions qui définissent les interfaces, les clients LDAP et les zones étiquetées.

  d. **Double-cliquez sur l'action Create LDAP Client (Créer client LDAP).**

     Répondez aux invites suivantes :

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

```
LDAP Proxy Password:          Type the password to the server
Profile Name:                 Type the profile name
```

e. Cliquez sur OK.

Le compte-rendu d'exécution suivant s'affiche :

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

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

f. Fermez la fenêtre d'action.

3 Dans une fenêtre de terminal, définissez le paramètre `enableShadowUpdate` sur `TRUE`.

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

L'action Create LDAP Client (Créer client LDAP) et le script `txzonemgr` exécutent uniquement la commande `ldapclient init`. Dans Trusted Extensions, vous devez également modifier un client LDAP initialisé pour activer les mises à jour en double.

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, créez de nouveau le client LDAP et fournissez les valeurs correctes. 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.

Exemple 4–2 L'utilisation des noms d'hôtes après le chargement d'un fichier `resolv.conf`

Dans cet exemple, l'administrateur souhaite qu'un ensemble particulier de serveurs DNS soit disponible pour le système. L'administrateur copie un fichier `resolv.conf` à partir d'un serveur sur un réseau sécurisé. Étant donné que le serveur DNS n'est pas encore actif, l'administrateur utilise l'adresse IP du serveur pour trouver le serveur.

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

Une fois le fichier `resolv.conf` copié et si le fichier `nsswitch.conf` inclus `dns` dans l'entrée `hosts`, l'administrateur peut utiliser des noms d'hôtes pour localiser les systèmes.

Création de zones étiquetées

Le script `txzonemgr` vous guide à travers les tâches suivantes, qui permettent de configurer les zones étiquetées.

Attention – Vous devez exécuter la version Solaris 10 8/07 de Trusted Extensions ou une version ultérieure pour utiliser les procédures `txzonemgr`, ou vous devez installer tous les patchs pour la version Solaris 10 11/06.

Si vous exécutez la version Solaris 10 11/06 sans les patchs actuels, suivez les procédures décrites à l'Annexe B, “Utilisation d'actions CDE pour installer des zones dans Trusted Extensions” pour configurer les zones étiquetées.

Les instructions de cette section permettent de configurer les zones étiquetées sur un système auquel au moins deux adresses IP ont été affectées. Pour d'autres configurations, reportez-vous aux options de configuration décrites à la section “Liste des tâches : préparation et activation de Trusted Extensions” à la page 35.

Tâche	Description	Voir
1. Exécution du script `txzonemgr`.	Le script `txzonemgr` crée une interface graphique qui présente les tâches appropriées pendant que vous configurez vos zones.	“Exécution du script `txzonemgr`” à la page 69
2. Gestion des interfaces réseau dans la zone globale.	Configurez les interfaces dans la zone globale ou créez des interfaces logiques et configurez-les dans la zone globale.	“Configuration des interfaces réseau dans Trusted Extensions” à la page 70
3. Attribution de nom et étiquetage de la zone.	Nommez la zone avec une version de son étiquette et affectez l'étiquette.	“Attribution de nom et étiquetage de la zone” à la page 74
4. Installation et initialisation de la zone.	Installez les packages dans la zone. Configurez les services dans la zone. Une console de terminal de zone vous permet de visualiser l'activité dans la zone.	“Installation de la zone étiquetée” à la page 77 “Démarrage de la zone étiquetée” à la page 78
5. Vérification de l'état de la zone.	Vérifiez que la zone étiquetée est en cours d'exécution et que la zone peut communiquer avec la zone globale.	“Vérification de l'état de la zone” à la page 79

Tâche	Description	Voir
6. Personnalisation de la zone.	Supprimez les services non désirés de la zone. Si la zone est destinée à être utilisée pour créer d'autres zones, supprimez les informations spécifiques à cette zone uniquement.	"Personnalisation de la zone étiquetée" à la page 81
7. Création des autres zones.	Utilisez la méthode de votre choix pour créer votre seconde zone. Pour une description des méthodes de création de zones, reportez-vous à la section "Planification de zones dans Trusted Extensions" à la page 24.	"Copie ou clonage d'une zone dans Trusted Extensions" à la page 82
8. (Facultatif) Ajout d'interfaces réseau spécifiques à la zone.	Pour obtenir l'isolement du réseau, ajoutez une ou plusieurs interfaces réseau à une zone étiquetée. En règle générale, de telles configurations sont utilisées pour isoler les sous-réseaux étiquetés.	"Ajout d'interfaces réseau et acheminement vers les zones étiquetées" à la page 84

▼ Exécution du script `txzonemgr`

Ce script vous guide à travers les tâches afin de correctement configurer, installer, initialiser et démarrer les zones étiquetées. Dans le script, vous pouvez attribuer un nom à chaque zone, associer ce nom avec une étiquette, installer les packages pour créer un système d'exploitation virtuel, puis initialiser la zone pour démarrer des services dans cette zone. Ce script comprend les tâches de copie et de clonage de zones. Vous pouvez également arrêter une zone, modifier son état et ajouter des interfaces réseau spécifiques aux zones.

Ce script présente un menu dynamique qui affiche uniquement les options valides dans le contexte actuel. Par exemple, lors de la configuration de l'état d'une zone, l'option de menu Install zone (Installer la zone) n'est pas affichée. Les tâches qui sont terminées ne s'affichent pas dans la liste.

Avant de commencer

Vous êtes superutilisateur.

Si vous avez l'intention de cloner des zones, vous avez terminé la préparation du clonage des zones. Si vous avez l'intention d'utiliser vos propres modèles de sécurité, vous avez créé les modèles.

1 Ouvrez une fenêtre de terminal dans la zone globale.

2 Exécutez le script `txzonemgr`.

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

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

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 (Labeled Zone Manager).

▼ Configuration des interfaces réseau dans Trusted Extensions

Remarque – Si vous configurez votre système pour utiliser le protocole DHCP, reportez-vous aux instructions relatives aux ordinateurs portables à la section Trusted Extensions de la page Web relative à la sécurité de la communauté OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

À partir de la version Solaris 10 10/08, si vous configurez un système sur lequel chaque zone étiquetée se trouve sur son propre sous-réseau, vous pouvez ignorer cette étape et passer à l'étape "Attribution de nom et étiquetage de la zone" à la page 74. L'étape "Ajout d'une interface réseau pour acheminer une zone étiquetée existante" à la page 85 décrit l'ajout d'interfaces réseau pour chaque zone étiquetée après avoir terminé l'installation et la personnalisation des zones.

Cette tâche permet de configurer le réseau dans la zone globale. Vous devez créer une seule interface `all-zones`. Une interface `all-zones` est partagée par les zones étiquetées et la zone globale. L'interface partagée est utilisée pour acheminer le trafic entre les zones étiquetées et la zone globale. Pour configurer cette interface, procédez de l'une des manières suivantes :

- Créez une interface logique à partir d'une interface physique, puis partagez l'interface physique.

  Cette configuration est la plus simple à administrer. Choisissez cette configuration lorsque deux adresses IP ont été affectées à votre système. Dans cette procédure, l'interface logique devient l'adresse spécifique de la zone globale et l'interface physique est partagée entre la zone globale et les zones étiquetées.
- Partagez une interface physique

  Choisissez cette configuration lorsqu'une seule adresse IP a été affectée à votre système. Dans cette configuration, l'interface physique est partagée entre la zone globale et les zones étiquetées.
- Partagez une interface réseau virtuelle, `vni0`

Choisissez cette configuration lorsque vous configurez le protocole DHCP ou lorsque chaque sous-réseau se trouve sur une étiquette différente. Pour un exemple de procédure, reportez-vous aux instructions relatives aux ordinateurs portables dans la section Trusted Extensions de la page Web relative à la sécurité de la communauté OpenSolaris (`http://hub.opensolaris.org/bin/view/Community+Group+security/`).

À partir de la version Solaris 10 10/08, l'interface de loopback dans Trusted Extensions est créée en tant qu'interface all-zones. Par conséquent, vous n'avez pas besoin de créer d'interface `vni0` partagée.

Pour ajouter des interfaces réseau spécifiques aux zones, terminez et contrôlez la création de la zone avant d'ajouter les interfaces. Pour plus d'informations sur cette procédure, reportez-vous à la section "Ajout d'une interface réseau pour acheminer une zone étiquetée existante" à la page 85.

Avant de commencer

Vous êtes superutilisateur dans la zone globale.

Le gestionnaire de zones étiquetées est affiché. Pour ouvrir cette interface graphique, reportez-vous à la section "Exécution du script `txzonemgr`" à la page 69.

1. **Dans le gestionnaire de zones étiquetées, sélectionnez Manage Network Interfaces (Gérer les interfaces réseau) et cliquez sur OK.**

   Une liste d'interfaces s'affiche.

   Remarque – Dans cet exemple, un nom d'hôte et une adresse IP ont été affectés à l'interface physique au cours de l'installation.

2. **Sélectionnez l'interface physique.**

   Un système avec une seule interface affiche un menu similaire à celui-ci. L'annotation est ajoutée à des fins d'aide :

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

   a. **Sélectionnez l'interface `eri0`.**

   b. **Cliquez sur OK.**

3. **Sélectionnez la tâche appropriée pour cette interface réseau.**

   Trois options vous sont proposées :

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

   - **Si votre système dispose d'une seule adresse IP, passez à l'Étape 4.**

- **Si votre système dispose de deux adresses IP, passez à l'Étape 5.**

4 Sur un système disposant d'une seule adresse IP, partagez l'interface physique.

Dans cette configuration, l'adresse IP de l'hôte s'applique à toutes les zones. Par conséquent, l'adresse de l'hôte est l'adresse `all-zones`. Cet hôte ne peut pas être utilisé comme un serveur multiniveau. Par exemple, les utilisateurs ne peuvent pas partager de fichiers à partir de ce système. Le système ne peut pas être un serveur proxy LDAP, un serveur d'annuaires personnel NFS ou un serveur d'impression.

a. Sélectionnez Share (Partager) et cliquez sur OK.

b. Cliquez sur OK dans la boîte de dialogue qui affiche l'interface partagée.

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

Cette opération fonctionne lorsque l'interface physique est une interface `all-zones`. Passez à la section "Attribution de nom et étiquetage de la zone" à la page 74.

5 Sur un système disposant de deux adresses IP, créez une interface logique.

Ensuite, partagez l'interface physique.

Il s'agit de la configuration réseau Trusted Extensions la plus simple. Dans cette configuration, l'adresse IP principale peut être utilisée par d'autres systèmes pour atteindre n'importe quelle zone sur ce système, et l'interface logique est spécifique à la zone globale. La zone globale peut être utilisée en tant que serveur multiniveau.

a. Sélectionnez Create Logical Interface (Créer l'interface logique) et cliquez sur OK.

Fermez la boîte de dialogue confirmant la création d'une nouvelle interface logique.

b. Sélectionnez Set IP Address (Configurer l'adresse IP) et cliquez sur OK.

c. À l'invite, spécifiez le nom d'hôte pour l'interface logique et cliquez sur OK.

Par exemple, spécifiez `machine1-services` comme nom d'hôte pour l'interface logique. Le nom indique que cet hôte offre des services multiniveau.

d. À l'invite, spécifiez l'adresse IP pour l'interface logique et cliquez sur OK.

Par exemple, spécifiez `10.10.9.2` comme adresse IP de l'interface logique.

e. Sélectionnez de nouveau l'interface logique et cliquez sur OK.

f. Sélectionnez Bring Up (Afficher) et cliquez sur OK.

L'interface s'affiche comme `Up`.

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

g. Partagez l'interface physique.

i. Sélectionnez l'interface physique et cliquez sur OK.

ii. Sélectionnez Share (Partager) et cliquez sur OK.

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

Cette opération fonctionne lorsqu'au moins une interface est une interface `all-zones`.

Exemple 4–3 Affichage du fichier `/etc/hosts` sur un système avec une interface logique partagée

Sur un système où la zone globale a une interface unique et où les zones étiquetées partagent une deuxième interface avec la zone globale, le fichier `/etc/hosts` est similaire à la sortie suivante :

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

Dans la configuration par défaut, le fichier `tnrhdb` s'affiche comme suit :

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

Si l'interface `all-zones` ne se trouve pas dans le fichier `tnrhdb`, l'interface passe par défaut à `cipso`.

Exemple 4–4 Affichage de l'interface partagée sur un système Trusted Extensions avec une seule adresse IP

Dans cet exemple, l'administrateur n'envisage pas d'utiliser le système en tant que serveur multiniveau. Pour conserver les adresses IP, la zone globale est configurée de façon à partager son adresse IP avec toutes les zones étiquetées.

L'administrateur sélectionne l'option Share (Partage) pour l'interface `hme0` sur le système. Le logiciel configure toutes les zones afin qu'elles aient une NIC logique. Ces NIC logiques partagent une seule NIC physique dans la zone globale.

L'administrateur exécute la commande **`ifconfig -a`** pour vérifier que l'interface physique `hme0` sur l'interface réseau `192.168.0.11` est partagée. La valeur `all-zones` s'affiche :

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

À partir de la version Solaris 10 10/08, l'interface de loopback dans Trusted Extensions est créée en tant qu'interface all-zones.

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

L'administrateur examine également le contenu du fichier `/etc/hostname.hme0` :

```
192.168.0.11 all-zones
```

▼ Attribution de nom et étiquetage de la zone

Vous n'êtes pas obligé de créer une zone pour chaque étiquette de votre fichier `label_encodings`, mais vous pouvez le faire. Les interfaces graphiques d'administration énumèrent les étiquettes pour lesquelles des zones peuvent être créées sur ce système.

Avant de commencer Vous êtes superutilisateur dans la zone globale. La boîte de dialogue Labeled Zone Manager (Gestionnaire de zones étiquetées) s'affiche. Pour ouvrir cette interface graphique, reportez-vous à la section "Exécution du script `txzonemgr`" à la page 69. Vous avez configuré les interfaces réseau dans la zone globale.

Vous avez créé les modèles de sécurité dont vous avez besoin. Un modèle de sécurité définit, entre autres attributs, la plage d'étiquettes qui peut être affectée à une interface réseau. Les modèles de sécurité par défaut peuvent répondre à vos besoins.

- Pour obtenir un aperçu des modèles de sécurité, reportez-vous à la section "Attributs de sécurité réseau dans Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
- Pour utiliser la Console de gestion Solaris pour créer des modèles de sécurité, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

1 Dans le gestionnaire de zones étiquetées, sélectionnez Create a new zone (Créer une zone) et cliquez sur OK.

Vous êtes invité à saisir un nom.

a. Saisissez un nom pour la zone.

Astuce – Attribuez à la zone un nom similaire à l'étiquette de la zone. Par exemple, le nom d'une zone dont l'étiquette est `CONFIDENTIAL: RESTRICTED` serait `restricted`.

Par exemple, le fichier `label_encodings` par défaut contient les étiquettes suivantes :

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

Bien que vous puissiez créer une zone par étiquette, vous pouvez envisager de créer les zones suivantes :

- Sur un système destiné à tous les utilisateurs, créez une zone pour l'étiquette `PUBLIC` et trois zones pour les étiquettes `CONFIDENTIAL`.
- Sur un système destiné aux développeurs, créez une zone pour l'étiquette `SANDBOX: PLAYGROUND`. L'étiquette `SANDBOX: PLAYGROUND` est définie en tant qu'étiquette disjointe pour les développeurs, de sorte que seuls les systèmes utilisés par les développeurs ont besoin d'une zone pour cette étiquette.
- Ne créez pas de zone pour l'étiquette `MAX LABEL`, qui est définie pour être une autorisation.

b. Cliquez sur OK.

La boîte de dialogue affiche *zone-name* `: configured` au-dessus d'une liste de tâches.

2 Pour attribuer une étiquette à la zone, choisissez l'une des options suivantes :

- **Si vous utilisez un fichier `label_encodings` personnalisé, étiquetez la zone à l'aide de l'outil Trusted Network Zones.**

  a. Ouvrez l'outil Trusted Network Zones dans la Console de gestion Solaris.

  i. Démarrez la Console de gestion Solaris.

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

  ii. Ouvrez la boîte à outils Trusted Extensions pour le système local.

  Choisissez Console → Open Toolbox (Console → Ouvrir la boîte à outils).

  Sélectionnez la boîte à outils nommée Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`).

Cliquez sur Open (Ouvrir).

iii. **Sous System Configuration (Configuration système), accédez à Computers and Networks (Ordinateurs et réseaux).**

À l'invite, saisissez un mot de passe.

iv. **Double-cliquez sur l'outil Trusted Network Zones.**

b. **Pour chaque zone, associez l'étiquette appropriée au nom de la zone.**

i. **Choisissez Action → Add Zone Configuration (Action → Ajouter la configuration de zone).**

La boîte de dialogue affiche le nom d'une zone à laquelle aucune étiquette n'a été assignée.

ii. **Vérifiez le nom de zone, puis cliquez sur Edit (Modifier).**

iii. **Dans le générateur d'étiquettes (Label Builder), cliquez sur l'étiquette appropriée pour le nom de zone.**

Si vous sélectionnez la mauvaise étiquette, cliquez de nouveau sur l'étiquette pour la désélectionner, puis cliquez sur l'étiquette appropriée.

iv. **Enregistrez l'allocation.**

Cliquez sur OK dans le générateur d'étiquettes, puis cliquez sur OK dans la boîte de dialogue Trusted Network Zones Properties (Propriétés des zones Trusted Network).

Vous avez terminé lorsque toutes les zones de votre choix sont répertoriées dans le panneau ou lorsque l'option de menu Add Zone Configuration (Ajouter la configuration de zone) ouvre une boîte de dialogue ne contenant aucune valeur pour le nom de zone (Zone Name).

- **Si vous utilisez le fichier `label_encodings` par défaut, utilisez le gestionnaire de zones étiquetées.**

Cliquez sur l'option de menu Select Label (Sélectionner une étiquette) et sur OK pour afficher la liste des étiquettes disponibles.

a. **Sélectionnez l'étiquette pour la zone.**

Pour une zone nommée `public`, vous devez sélectionner l'étiquette `PUBLIC` dans la liste.

b. **Cliquez sur OK.**

Une liste de tâches s'affiche.

▼ Installation de la zone étiquetée

Avant de commencer

Vous êtes superutilisateur dans la zone globale. La zone est configurée et une interface réseau lui a été affectée.

La boîte de dialogue Labeled Zone Manager (Gestionnaire de zones étiquetées) est affichée avec le sous-titre *zone-name*`:configured`. Pour ouvrir cette interface graphique, reportez-vous à la section "Exécution du script `txzonemgr`" à la page 69.

1 À partir du gestionnaire de zones étiquetées, sélectionnez Install (Installer) et cliquez sur OK.

Attention – Ce processus prend un certain temps. N'exécutez aucune autre tâche tant que celle-ci n'est pas terminée.

Le système copie les packages de la zone globale vers la zone non globale. Cette tâche permet d'installer un système d'exploitation virtuel étiqueté dans la zone. Pour poursuivre l'exemple, cette tâche installe la zone `public`. L'interface graphique affiche une sortie similaire à la suivante.

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

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

Remarque – Les messages tels que `cannot create ZFS dataset zone/` *zonename*`: dataset already exists` sont fournis à titre d'information. La zone utilise les jeux de données existant.

Lorsque l'installation est terminée, vous êtes invité à indiquer le nom de l'hôte. Un nom est proposé.

2 Acceptez le nom de l'hôte.

La boîte de dialogue affiche *zone-name*`:installed` au-dessus d'une liste de tâches.

Erreurs fréquentes

Si des avertissements semblables à celui-ci s'affichent : `Installation of these packages generated errors: SUNW` *pkgname*, lisez le journal d'installation et terminez l'installation des packages.

▼ Démarrage de la zone étiquetée

Avant de commencer Vous êtes superutilisateur dans la zone globale. La zone est installée et une interface réseau lui a été affectée.

La boîte de dialogue Labeled Zone Manager (Gestionnaire de zones étiquetées) s'affiche avec le sous-titre *zone-name*:`installed`. Pour ouvrir cette interface graphique, reportez-vous à la section "Exécution du script `txzonemgr`" à la page 69.

1 Dans le gestionnaire de zones étiquetées, sélectionnez Zone Console (Console de zone) et cliquez sur OK.

Une fenêtre de console séparée s'affiche pour la zone étiquetée actuelle.

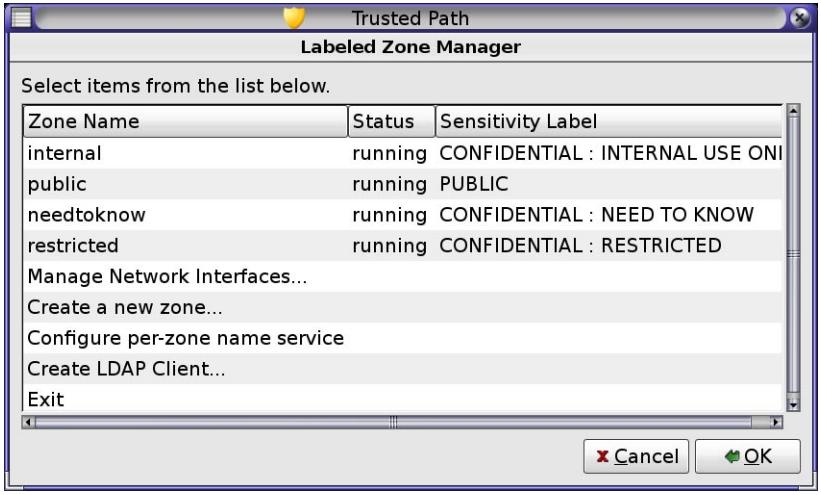
2 Sélectionnez Boot (Initialiser).

La console de terminal de zone suit le progrès de l'initialisation de la zone. Si la zone est créée à partir de zéro, des messages semblables à celui-ci s'affichent sur la console :

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

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

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

[NOTICE: Zone rebooting]
```

Attention – N'exécutez aucune autre tâche tant que celle-ci n'est pas terminée.

Lorsque les quatre zones par défaut sont configurées et initialisées, le gestionnaire de zones étiquetées affiche les zones de la manière suivante :



Erreurs fréquentes Parfois, des messages d'erreur s'affichent et la zone n'est pas réinitialisée. Dans la console de terminal de zone, appuyez sur la touche Entrée. Si vous êtes invité à saisir y pour procéder à la réinitialisation, saisissez y et appuyez sur la touche Entrée. La zone redémarre.

Étapes suivantes Si cette zone a été copiée ou clonée à partir d'une autre zone, passez à la section "Vérification de l'état de la zone" à la page 79.

S'il s'agit de la première zone, passez à la section "Personnalisation de la zone étiquetée" à la page 81.

▼ Vérification de l'état de la zone

Remarque – Le serveur X est exécuté dans la zone globale. Chaque zone étiquetée doit être en mesure de se connecter à la zone globale pour utiliser le serveur X. Par conséquent, la mise en réseau des zones doit fonctionner avant qu'une zone puisse être utilisée. Pour plus d'informations générales, reportez-vous à la section "Planification pour l'accès multiniveau" à la page 26.

1 Vérifiez que la zone a été complètement démarrée.

a. Dans la console de terminal de zone *zone-name*, connectez-vous en tant que root.

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

b. Dans la console de terminal de zone, vérifiez que les services critiques sont en cours d'exécution.

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

Les services `sendmail` et `print` ne sont pas des services critiques.

c. Vérifiez que la zone dispose d'une adresse IP valide.

```
# ifconfig -a
```

Par exemple, la sortie suivante indique une adresse IP pour l'interface `hme0`.

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

d. (Facultatif) Vérifiez que la zone peut communiquer avec la zone globale.

i. Définissez la variable `DISPLAY` afin qu'elle pointe vers le serveur–X.

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

ii. Dans la fenêtre de terminal, affichez une interface graphique.

Par exemple, affichez une horloge.

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

Si l'horloge sur l'étiquette de la zone ne s'affiche pas, le réseau de la zone n'a pas été correctement configuré. Des conseils de débogage sont fournis à la section "La zone étiquetée ne peut accéder au serveur X" à la page 111.

iii. Fermez l'interface graphique avant de poursuivre.

2 À partir de la zone globale, vérifiez l'état des zones étiquetées.

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

Étapes suivantes Vous avez terminé de configurer la zone étiquetée. Pour ajouter des interfaces réseau spécifiques aux zones ou établir un routage par défaut par zone étiquetée, passez à la section

"Ajout d'interfaces réseau et acheminement vers les zones étiquetées" à la page 84. Sinon, passez à la section "Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92.

▼ Personnalisation de la zone étiquetée

Si vous avez l'intention de cloner ou de copier des zones, cette procédure permet de configurer une zone en tant que modèle pour d'autres zones. En outre, cette procédure permet de configurer une zone qui n'a pas été créée à partir d'un modèle afin de l'utiliser.

Avant de commencer Vous êtes superutilisateur dans la zone globale. Vous avez terminé les tâches de la section "Vérification de l'état de la zone" à la page 79.

1 Dans la console de terminal de zone, désactivez les services inutiles dans une zone étiquetée.

Si vous copiez ou clonez cette zone, les services que vous désactivez sont désactivés dans les nouvelles zones. Les services en ligne sur votre système dépendent du fichier manifest du service pour la zone. Utilisez la commande `netservices limited` pour désactiver les services dont les zones étiquetées n'ont pas besoin.

a. Supprimez les nombreux services inutiles.

```
# netservices limited
```

b. Répertoriez les services restants.

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

c. Désactivez la connexion graphique.

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

Pour en savoir plus sur l'utilitaire de gestion des services, reportez-vous à la page de manuel `smf(5)`.

2 Dans le gestionnaire de zones étiquetées, sélectionnez Halt (Arrêter) pour arrêter la zone.

3 Avant de poursuivre, vérifiez que la zone est arrêtée.

Dans la console de terminal de zone *zone-name*, le message suivant indique que la zone est arrêtée.

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

Si vous ne copiez ou ne clonez pas cette zone, créez les zones restantes de la même manière que vous avez créé cette première zone. Sinon, passez à l'étape suivante.

4 **Si vous utilisez cette zone comme modèle pour d'autres zones, effectuez les opérations suivantes :**

a. **Supprimez le fichier `auto_home_`*zone-name*.**

Dans une fenêtre de terminal dans la zone globale, supprimez ce fichier à partir de la zone *zone-name*.

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

Par exemple, si la zone `public` est le modèle pour le clonage d'autres zones, supprimez le fichier `auto_home_public` :

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

b. **Si vous envisagez de cloner cette zone, créez l'instantané ZFS à l'étape suivante, puis passez à la section "Copie ou clonage d'une zone dans Trusted Extensions" à la page 82.**

c. **Si vous envisagez de copier cette zone, effectuez l'Étape 6, puis passez à la section "Copie ou clonage d'une zone dans Trusted Extensions" à la page 82.**

5 **Pour créer un modèle de zone pour le clonage des zones restantes, sélectionnez Create Snapshot (Créer l'instantané) et cliquez sur OK.**

Attention – La zone pour l'instantané doit se trouver dans un système de fichiers ZFS. Vous avez créé un système de fichiers ZFS pour la zone à l'étape "Création d'un pool ZFS pour le clonage des zones" à la page 58.

6 **Pour vérifier que la zone personnalisée peut toujours être utilisée, sélectionnez Boot from the Labeled Zone Manager (Démarrer à partir du Gestionnaire de zones étiquetées).**

La console de terminal de zone suit la progression de l'initialisation de la zone. Des messages semblables à celui-ci s'affichent sur la console :

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

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

Appuyez sur la touche Entrée pour une invite de connexion. Vous pouvez vous connecter en tant qu'utilisateur root.

▼ Copie ou clonage d'une zone dans Trusted Extensions

Avant de commencer Vous avez terminé les tâches de la section "Personnalisation de la zone étiquetée" à la page 81.

La boîte de dialogue Labeled Zone Manager (Gestionnaire de zones étiquetées) s'affiche. Pour ouvrir cette interface graphique, reportez-vous à la section "Exécution du script `txzonemgr`" à la page 69.

1. **Créez la zone.**

   Pour plus de détails, reportez-vous à la section "Attribution de nom et étiquetage de la zone" à la page 74.

2. **Poursuivez votre stratégie de création de zones en procédant de l'une des manières suivantes :**

   Répétez ces étapes pour chaque nouvelle zone.

   - **Copiez la zone que vous venez d'étiqueter.**

     a. **Dans le gestionnaire de zones étiquetées, sélectionnez Copy (Copier), puis cliquez sur OK.**

     b. **Sélectionnez le modèle de zone et cliquez sur OK.**

        Une fenêtre indique l'avancement du processus de copie. Une fois ce processus terminé, la zone est installée.

        Si le gestionnaire de zones étiquetées affiche *zone-name* `:configured`, passez à l'étape suivante. Sinon, poursuivez avec l'Étape e.

     c. **Sélectionnez l'option de menu Select another zone (Sélectionner une autre zone) et cliquez sur OK.**

     d. **Sélectionnez la zone récemment installée et cliquez sur OK.**

     e. **Exécutez les tâches de la section "Démarrage de la zone étiquetée" à la page 78.**

     f. **Exécutez le processus "Vérification de l'état de la zone" à la page 79.**

   - **Clonez la zone que vous venez d'étiqueter.**

     a. **Dans le gestionnaire de zones étiquetées, sélectionnez Clone (Cloner) et cliquez sur OK.**

     b. **Sélectionnez un instantané ZFS dans la liste et cliquez sur OK.**

        Par exemple, si vous avez créé un instantané de `public`, sélectionnez `zone/public@snapshot`.

        Une fois le processus de clonage terminé, la zone est installée. Continuer avec l'Étape c.

c. **Ouvrez une console de zone et initialisez la zone.**

   Pour obtenir davantage d'instructions, reportez-vous à la section "Démarrage de la zone étiquetée" à la page 78.

d. **Exécutez le processus "Vérification de l'état de la zone" à la page 79.**

Étapes suivantes

- Une fois que vous avez terminé les tâches de la section "Vérification de l'état de la zone" à la page 79 pour chaque zone, si vous souhaitez que chaque zone se trouve sur un réseau physique distinct, passez à la section "Ajout d'une interface réseau pour acheminer une zone étiquetée existante" à la page 85.
- Si vous n'avez pas encore créé de rôles, passez à la section "Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92.
- Si vous avez déjà créé les rôles, passez à la section "Création de répertoires personnels dans Trusted Extensions" à la page 104.

Ajout d'interfaces réseau et acheminement vers les zones étiquetées

Les tâches suivantes prennent en charge des environnements où chaque zone est connectée à un réseau physique distinct.

Tâche	Description	Voir
1a : Ajout d'une interface réseau à chaque zone étiquetée et utilisation de la zone globale pour atteindre le réseau externe.	Permet de connecter chaque zone étiquetée à un réseau physique distinct. Les zones étiquetées utilisent l'acheminement des données fourni par la zone globale.	"Ajout d'une interface réseau pour acheminer une zone étiquetée existante" à la page 85
OU 1b : Ajout d'une interface réseau à chaque zone étiquetée avec une route par défaut.	Permet de connecter chaque zone à un réseau physique distinct. Les zones étiquetées n'utilisent *pas* la zone globale pour l'acheminement.	"Ajout d'une interface réseau qui n'utilise pas la zone globale pour acheminer une zone étiquetée existante" à la page 87
2. Création d'un cache de service de noms dans chaque zone étiquetée.	Permet de configurer un démon du service de noms pour chaque zone.	"Configuration d'un cache de service de noms dans chaque zone étiquetée" à la page 91

▼ Ajout d'une interface réseau pour acheminer une zone étiquetée existante

Cette procédure permet d'ajouter des zone interfaces réseau spécifiques à des zones étiquetées existantes. Cette configuration prend en charge les environnements dans lesquels chaque zone étiquetée est connectée à un réseau physique distinct. Les zones étiquetées utilisent l'acheminement des données fourni par la zone globale.

Remarque – La zone globale doit configurer une adresse IP pour chaque sous-réseau dans lequel une adresse de zone non globale est configurée.

Avant de commencer

Vous êtes superutilisateur dans la zone globale.

Pour chaque zone, vous avez terminé les tâches de la section "Création de zones étiquetées" à la page 68.

1 Dans la zone globale, saisissez les adresses IP et les noms d'hôtes des interfaces réseau supplémentaires dans le fichier `/etc/hosts`.

Utilisez une convention de nommage standard, par exemple ajoutez *zone-name* au nom de l'hôte.

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

2 Ajoutez des entrées pour le réseau de chaque interface dans le fichier `/etc/netmasks` .

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

Pour plus d'informations, reportez-vous à la page de manuel `netmasks(4)`.

3 Dans la zone globale, montez les interfaces physiques spécifiques aux zones.

a. Identifiez les interfaces physiques déjà montées.

```
# ifconfig -a
```

b. Configurez les adresses de la zone globale sur chaque interface.

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

c. Pour chaque adresse de zone globale, créez un fichier `hostname.` *interface-nameN*.

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

Les adresses de zone globale sont configurées immédiatement après le démarrage du système. Les adresses spécifiques aux zones sont configurées lors de l'initialisation de la zone.

4 Affectez un modèle de sécurité à chaque interface réseau spécifique à une zone.

Si la passerelle vers le réseau n'est pas configurée avec des étiquettes, affectez le modèle de sécurité `admin_low`. Si la passerelle vers le réseau est étiquetée, affectez un modèle de sécurité `cipso`.

Vous pouvez créer des modèles de sécurité de type d'hôte `cipso` qui reflètent l'étiquette de chaque réseau. Pour plus d'informations sur les procédures de création et d'affectation de modèles, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

5 Arrêtez chaque zone étiquetée à laquelle vous prévoyez d'ajouter une interface spécifique.

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

6 Démarrez le gestionnaire de zones étiquetées.

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

7 Pour chaque zone à laquelle vous voulez ajouter une interface spécifique, procédez comme suit :

a. Sélectionnez la zone.

b. Sélectionnez Add Network (Ajouter un réseau).

c. Nommez l'interface réseau.

d. Saisissez l'adresse IP de l'interface.

8 Dans le gestionnaire de zones étiquetées, pour chaque zone terminée, sélectionnez Zone Console (Console de zone).

9 Sélectionnez Boot (Initialiser).

10 Dans la console de zone, vérifiez que les interfaces ont été créées.

```
# ifconfig -a
```

11 Vérifiez que la zone est acheminée vers la passerelle pour le sous-réseau.

```
# netstat -rn
```

Erreurs fréquentes

Pour déboguer la configuration de zone, reportez-vous aux sections suivantes :

- Chapitre 30, "Troubleshooting Miscellaneous Solaris Zones Problems" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*
- "Dépannage de votre configuration Trusted Extensions" à la page 110
- "Dépannage du réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

▼ Ajout d'une interface réseau qui n'utilise pas la zone globale pour acheminer une zone étiquetée existante

Cette procédure permet de définir des routes par défaut spécifiques à une zone pour les zones étiquetées existantes. Dans cette configuration, les zones étiquetées n'utilisent *pas* la zone globale pour l'acheminement.

La zone étiquetée doit être montée dans la zone globale avant l'initialisation de la zone. Cependant, pour isoler la zone étiquetée de la zone globale, l'interface doit se trouver en état `down` lors de l'initialisation de la zone. Pour plus d'informations, reportez-vous au Chapitre 17, "Non-Global Zone Configuration (Overview)" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

Remarque – Une route par défaut unique doit être configurée pour chaque zone non globale initialisée.

Avant de commencer

Vous êtes superutilisateur dans la zone globale.

Pour chaque zone, vous avez terminé les tâches de la section "Création de zones étiquetées" à la page 68. Vous utilisez l'interface `vni0` ou `lo0` pour connecter les zones étiquetées à la zone globale.

1. **Pour chaque interface réseau, déterminez son adresse IP, son masque de réseau et son routeur par défaut.**

   Utilisez la commande `ifconfig -a` pour déterminer l'adresse IP et le masque de réseau. Utilisez la commande `zonecfg -z zonename info net` pour déterminer si un routeur par défaut a été attribué.

2. **Créer un fichier `/etc/hostname.`*interface* vide pour chaque zone étiquetée.**

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

   Pour plus d'informations, reportez-vous à la page de manuel `netmasks(4)`.

3 Montez les interfaces réseau des zones étiquetées.

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

4 Vérifiez que les interfaces de la zone étiquetée se trouvent dans l'état `down`.

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

Les adresses spécifiques aux zones sont configurées lors de l'initialisation de la zone.

5 Ajoutez des entrées pour le réseau de chaque interface dans le fichier `/etc/netmasks` .

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

Pour plus d'informations, reportez-vous à la page de manuel `netmasks(4)`.

6 Affectez un modèle de sécurité à chaque interface réseau spécifique à une zone.

Créez des modèles de sécurité de type d'hôte `cipso` qui reflètent l'étiquette de chaque réseau. Pour créer et affecter les modèles, reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

7 Exécutez le script `txzonemgr`, puis ouvrez une autre fenêtre de terminal.

Dans le gestionnaire de zones étiquetées, vous ajoutez les interfaces réseau pour les zones étiquetées. Dans la fenêtre de terminal, vous affichez les informations relatives à la zone et définissez le routeur par défaut.

8 Pour chaque zone à laquelle vous allez ajouter une interface réseau spécifique et un routeur, procédez comme suit :

a. Dans la fenêtre de terminal, arrêtez la zone.

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

b. Dans le gestionnaire de zones étiquetées, procédez comme suit :

i. Sélectionnez la zone.

ii. Sélectionnez Add Network (Ajouter un réseau).

iii. Nommez l'interface réseau.

iv. Saisissez l'adresse IP de l'interface.

v. Dans la fenêtre de terminal, vérifiez la configuration de la zone.

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

c. Dans la fenêtre de terminal, configurez le routeur par défaut pour le réseau de la zone étiquetée.

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

Pour en savoir plus, reportez-vous à la page de manuel `zonecfg(1M)` et à la section "How to Configure the Zone" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

d. Démarrez la zone étiquetée.

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

e. Dans la zone globale, vérifiez que la zone étiquetée possède une route vers la passerelle pour le sous-réseau.

```
# netstat -rn
```

Une table de routage s'affiche. La destination et l'interface de la zone étiquetée sont différentes de l'entrée de la zone globale.

9 Pour supprimer la route par défaut, sélectionnez l'adresse IP de la zone, puis supprimez la route.

```
# zonecfg -z zone-name

zonecfg:zone-name > select net address=zone-IP-address
zonecfg:zone-name:net> remove net defrouter=zone-default-route
zonecfg:zone-name:net>  info net
net:
   address: zone-IP-address
   physical: zone-network-interface
   defrouter not specified
```

Exemple 4–5 Définition d'une route par défaut pour une zone étiquetée

Dans cet exemple, l'administrateur achemine la zone Secret vers un autre sous-réseau physique. Le trafic en provenance et à destination de la zone Secret n'est pas acheminé par le biais de la zone globale. L'administrateur utilise le gestionnaire de zones étiquetées et la commande `zonecfg`, puis vérifie que l'acheminement fonctionne.

L'administrateur détermine si `qfe1` et `qfe1:0` ne sont pas en cours d'utilisation et crée un mappage pour deux zones étiquetées. `qfe1` est l'interface désignée pour la zone Secret.

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

Tout d'abord, l'administrateur crée le fichier `/etc/hostname.qfe1` et configure le fichier `/etc/netmasks`.

```
# touch /etc/hostname.qfe1

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

Ensuite, l'administrateur monte l'interface réseau et vérifie si elle est en état down.

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

Ensuite, dans la Console de gestion Solaris, l'administrateur crée un modèle de sécurité à l'aide d'une seule étiquette, Secret, et affecte l'adresse IP de l'interface au modèle.

L'administrateur arrête la zone.

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

L'administrateur exécute le script `txzonemgr` pour ouvrir le gestionnaire de zones étiquetées.

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

Dans le gestionnaire de zones étiquetées, l'administrateur sélectionne la zone Secret, Add Network (Ajouter un réseau), puis une interface réseau. L'administrateur ferme le gestionnaire de zones étiquetées.

Sur la ligne de commande, l'administrateur sélectionne l'adresse IP de la zone, puis définit sa route par défaut. Avant de quitter la commande, l'administrateur vérifie la route et la valide.

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

L'administrateur initialise la zone.

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

Dans une autre fenêtre de terminal dans la zone globale, l'administrateur vérifie l'envoi et la réception de paquets.

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

Configuration d'un cache de service de noms dans chaque zone étiquetée

Cette procédure permet de configurer séparément un démon du service de noms (`nscd`) dans chaque zone étiquetée. 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 – 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.

Avant de commencer

Vous êtes superutilisateur dans la zone globale. `root` ne doit pas encore être un rôle. Vous avez exécuté les tâches de la section "Ajout d'une interface réseau pour acheminer une zone étiquetée existante" à la page 85.

Pour procéder à cette configuration, vous devez posséder des compétences avancées en matière de gestion de réseaux. Si votre service de nommage est LDAP, vous êtes chargé d'établir la connexion client LDAP pour chaque zone étiquetée. Le démon `nscd` met en cache les informations relatives au service de noms, mais ne les achemine pas.

1. **Si vous utilisez LDAP, vérifiez la route entre le serveur LDAP et la zone étiquetée.**

   Dans une fenêtre de terminal dans chaque zone étiquetée, exécutez la commande suivante :

   zone-name `# netstat -rn`

2. **Dans la zone globale, démarrez le gestionnaire de zones étiquetées.**

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

3. **Sélectionnez le service de noms Configure per-zone (Configuration par zone), puis cliquez sur OK.**

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

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

   Pour obtenir de l'aide, reportez-vous aux pages de manuel `nscd(1M)` and `nscd.conf(4)`.

5. **Redémarrez le système.**

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

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

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

7. **Pour supprimer les démons du service de noms spécifiques à des zones, procédez comme suit dans la zone globale :**

   a. **Ouvrez le gestionnaire de zones étiquetées.**

   b. **Sélectionnez le service de noms Unconfigure per-zone (Annulation de la configuration par zone), puis cliquez sur OK.**

      Cette sélection supprime le démon `nscd` de toutes les zones étiquetées.

   c. **Redémarrez le système.**

Création de rôles et d'utilisateurs dans Trusted Extensions

Si vous utilisez déjà des rôles d'administration, vous pouvez être amené à ajouter un rôle d'administrateur de sécurité. Pour les sites qui n'ont pas encore mis en œuvre les rôles, leur procédure de création est semblable à la procédure dans le SE Solaris. Trusted Extensions ajoute le rôle d'administrateur de sécurité et requiert l'utilisation de la Console de gestion Solaris pour administrer un domaine Trusted Extensions.

Si la sécurité du site nécessite deux personnes pour créer les comptes d'utilisateur et de rôle, créez des profils de droits personnalisés et affectez-les à des rôles afin d'appliquer la *séparation des tâches*.

Tâche	Description	Voir
Création de trois profils de droits plus restrictifs que les profils par défaut.	Permet de créer des profils de droits pour gérer les utilisateurs. Ces profils sont plus restrictifs que les profils de gestion des utilisateurs par défaut.	"Création de profils de droits permettant d'appliquer la séparation des tâches" à la page 93
Création d'un rôle d'administrateur de sécurité.	Permet de créer un rôle d'administrateur de sécurité qui gère les tâches relatives à la sécurité.	"Création du rôle d'administrateur de sécurité dans Trusted Extensions" à la page 96
Création d'un administrateur système qui ne peut pas définir de mot de passe utilisateur.	Permet de créer un rôle d'administrateur système et de lui assigner un profil de droits d'administrateur système limité.	"Création d'un rôle d'administrateur système limité" à la page 99
Création d'utilisateurs qui assumeront les rôles d'administration.	Permet de créer un ou plusieurs utilisateurs qui peuvent assumer des rôles.	"Création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions" à la page 99
Vérification de la capacité des rôles à exécuter leurs tâches.	Permet de tester les rôles dans divers scénarios.	"Vérification du fonctionnement des rôles Trusted Extensions" à la page 102
Autorisation des utilisateurs à se connecter à une zone étiquetée.	Permet de démarrer le service `zones` afin que les utilisateurs standard puissent se connecter.	"Autorisation des utilisateurs à se connecter à une zone étiquetée" à la page 104

▼ Création de profils de droits permettant d'appliquer la séparation des tâches

Ignorez cette procédure si la séparation des tâches n'est pas une exigence de sécurité du site. Si votre site requiert la séparation des tâches, vous devez créer ces profils de droits et rôles avant de remplir le serveur LDAP.

Cette procédure permet de créer des profils de droits disposant de capacités séparées pour la gestion des utilisateurs. Lorsque vous affectez ces profils à des rôles distincts, deux rôles sont nécessaires pour créer et configurer les utilisateurs. Un rôle peut créer des utilisateurs, mais ne peut pas leur affecter d'attributs de sécurité. L'autre rôle peut affecter les attributs de sécurité, mais ne peut pas créer d'utilisateurs. Lorsque vous vous connectez à la Console de gestion Solaris dans un rôle qui est affecté à l'un de ces profils, seuls les onglets et les champs pertinents sont disponibles pour le rôle.

Avant de commencer

Vous devez être connecté en tant que superutilisateur, dans le rôle `root` ou dans le rôle d'administrateur principal. Lorsque vous lancez cette procédure, la Console de gestion Solaris doit être fermée.

1. **Créez des copies des profils de droits par défaut qui ont une incidence sur la configuration des utilisateurs.**

   a. **Copiez le fichier `prof_attr` dans le fichier `prof_attr.orig`.**

   b. **Ouvrez le fichier `prof_attr` dans un éditeur de confiance.**

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

   c. **Copiez les trois profils de droits et renommez les copies.**

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

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

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

   d. **Enregistrez les modifications.**

   e. **Vérifiez vos modifications.**

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

   En copiant un profil de droits plutôt qu'en le modifiant, vous pouvez mettre à niveau le système vers une version ultérieure de Solaris, tout en conservant vos modifications. Dans la mesure où ces profils de droits sont complexes, la modification d'une copie du profil par défaut est moins sujette à erreur que la création d'un profil plus restrictif à partir de zéro.

2. **Démarrez la Console de gestion Solaris.**

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

3. **Sélectionnez la boîte à outils Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`).**

4. **Cliquez sur System Configuration (Configuration système), puis sur Users (Utilisateurs).**

   Vous êtes invité à saisir votre mot de passe.

5. **Saisissez le mot de passe approprié.**

6. **Double-cliquez sur Rights (Droits).**

7. **Modifiez le profil de droits Custom User Security (Sécurité utilisateur personnalisée).**

   Vous pouvez également empêcher ce profil de créer des utilisateurs.

   a. **Double-cliquez sur Custom User Security (Sécurité utilisateur personnalisée).**

b. Cliquez sur l'onglet Authorizations (Autorisations), puis effectuez les opérations suivantes :

i. Dans la liste Included (Inclus), supprimez l'autorisation `Manage Users and Roles` (Gérer les utilisateurs et les rôles).

Les droits de comptes utilisateur (User Accounts) suivants sont conservés :

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

ii. Ajoutez le droit Manage Privileges (Gérer les privilèges) à la liste Included (Inclus).

c. Cliquez sur OK pour enregistrer vos modifications.

8 Modifiez le profil Custom User Management (Gestion des utilisateurs personnalisée).

Vous pouvez empêcher ce profil de définir un mot de passe.

a. Double-cliquez sur Custom User Management (Gestion des utilisateurs personnalisée).

b. Cliquez sur l'onglet Authorizations (Autorisations), puis effectuez les opérations suivantes :

i. Faites défiler la barre de la liste Included (Inclus) jusqu'à User Accounts (Comptes utilisateur).

ii. Dans la liste Included (Inclus), supprimez l'autorisation `Modify Extended Security Attributes` (Modifier les attributs de sécurité étendue).

Les droits de comptes utilisateur (User Accounts) suivants sont conservés :

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

c. Enregistrez vos modifications.

9 Modifiez le profil de droits Custom System Administrator (Administrateur système personnalisé).

Le profil User Management (Gérer les utilisateurs) est un profil supplémentaire inclus dans ce profil. Vous pouvez empêcher l'administrateur système de définir des mots de passe.

a. Double-cliquez sur Custom System Administrator (Administrateur système personnalisé).

b. Cliquez sur l'onglet Supplementary Rights (Droits supplémentaires), puis effectuez les opérations suivantes :

i. Supprimez le profil de droits User Management (Gérer les utilisateurs).

ii. **Ajoutez le profil de droits Custom User Management (Gestion utilisateur personnalisée).**

iii. **Déplacez le profil de droits Custom User Management (Gestion utilisateur personnalisée) au-dessus du profil de droits All (Tous).**

c. **Enregistrez vos modifications.**

Étapes suivantes Pour éviter que les profils par défaut ne soient utilisés, reportez-vous à l'Étape 7 in "Vérification du fonctionnement des rôles Trusted Extensions" à la page 102 après avoir vérifié que les profils personnalisés appliquent la séparation des tâches.

▼ Création du rôle d'administrateur de sécurité dans Trusted Extensions

La création de rôles dans Trusted Extensions est identique à création de rôles dans le SE Solaris. Toutefois, dans Trusted Extensions, un rôle d'administrateur de sécurité est obligatoire. Pour créer un rôle d'administrateur de sécurité local, vous pouvez également utiliser l'interface de ligne de commande, comme illustré dans l'Exemple 4–6.

Avant de commencer Vous devez être connecté en tant que superutilisateur, dans le rôle `root` ou dans le rôle d'administrateur principal.

Pour créer le rôle sur le réseau, vous devez avoir exécuté les tâches de la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132.

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

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

2. **Sélectionnez la boîte à outils appropriée.**

   - **Pour créer le rôle en local, utilisez Cet ordinateur (***this-host***`:Scope=Files,Policy=TSOL`).**
   - **Pour créer le rôle dans le service LDAP, utilisez Cet ordinateur (***ldap-server***`:Scope=LDAP,Policy=TSOL`).**

3. **Cliquez sur System Configuration (Configuration système), puis sur Users (Utilisateurs).**

   Vous êtes invité à saisir votre mot de passe.

4. **Saisissez le mot de passe approprié.**

5. **Double-cliquez sur Administrative Roles (Rôles d'administration).**

6. **Sélectionnez Add Administrative Role (Ajouter un rôle d'administration) dans le menu Action.**

7 Créez le rôle d'administrateur de sécurité.

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

- Nom du rôle : `secadmin`
- Nom complet : `Security Administrator`
- Description : directeur de la sécurité du site *Aucune information propriétaire ici*.
- Numéro d'ID du rôle : ≥100
- Shell du rôle : Bourne de l'administrateur (shell de profil)
- Créer une liste de diffusion du rôle : laissez la case à cocher sélectionnée.
- Mot de passe et validation : attribuez un mot de passe d'au moins 6 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.

  Remarque – Pour tous les rôles d'administration, appliquez l'état Always Available (Toujours disponible) au compte et ne définissez pas de dates d'expiration des mots de passe.

- Droits disponibles et accordés : Information Security (Sécurité des informations), User Security (Sécurité de l'utilisateur)
  - Si la sécurité du site ne requiert pas de séparation des tâches, sélectionnez les profils de droits Information Security (Sécurité des informations) et User Security (Sécurité de l'utilisateur) par défaut.
  - Si la sécurité du site nécessite la séparation des tâches, sélectionnez les profils de droits Information Security (Sécurité des informations) et Custom User Security (Sécurité de l'utilisateur personnalisée).
- Serveur d'annuaires personnel : *home-directory-server*
- Chemin du répertoire personnel : /*mount-path*
- Affecter des utilisateurs : ce champ est automatiquement rempli lorsque vous affectez un rôle à un utilisateur.

8 Après avoir créé le rôle, vérifiez que les paramètres sont corrects.

Sélectionnez le rôle, puis double-cliquez dessus.

Passez en revue les valeurs des champs suivants :

- Groupes disponibles : ajoutez des groupes si nécessaire.
- Attributs Trusted Extensions : les valeurs par défaut sont correctes.

  Pour un système à une seule étiquette dans lequel les étiquettes ne doivent pas être visibles, choisissez l'option Hide (Masquer) sous Label: Show or Hide (Étiquette : afficher ou masquer).
- Contrôles exclus et inclus : définissez des indicateurs de contrôle uniquement si les indicateurs de contrôle du rôle sont des exceptions par rapport aux paramètres système dans le fichier `audit_control`.

9 Pour créer d'autres rôles, procédez de la même manière que pour la création du rôle d'administrateur de sécurité.

Pour obtenir des exemples, reportez-vous à la section "How to Create and Assign a Role by Using the GUI" du *System Administration Guide: Security Services*. Donnez à chaque rôle un ID unique, et affectez au rôle le profil de droits approprié. Les rôles suivants sont possibles :

- Rôle admin : droits de `System Administrator` (Administrateur système) accordés
- Rôle primaryadmin : droits de `Primary Administrator` (Administrateur principal) accordés
- Rôle oper : droits d'`Operator` (opérateur) accordés

Exemple 4–6 Utilisation de la commande `roleadd` pour créer un rôle d'administrateur de sécurité local

Dans cet exemple, l'utilisateur `root` ajoute le rôle d'administrateur de sécurité sur le système local à l'aide de la commande `roleadd`. Pour plus d'informations, reportez-vous à la page de manuel `roleadd`(1M). L'utilisateur `root` peut consulter le Tableau 1–2 avant de créer le rôle. Sur ce site, la séparation des tâches n'est pas nécessaire pour créer un utilisateur.

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

L'utilisateur `root` fournit 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
#
```

Pour connaître la procédure d'affectation du rôle à un utilisateur local, reportez-vous à l'Exemple 4–7.

▼ Création d'un rôle d'administrateur système limité

Ignorez cette procédure si la séparation des tâches n'est pas une exigence de sécurité du site.

Dans cette procédure, vous attribuez un profil de droits plus limité au rôle d'administrateur système.

Avant de commencer

Vous devez être connecté en tant que superutilisateur, dans le rôle `root` ou dans le rôle d'administrateur principal.

Vous avez terminé les tâches de la section "Création de profils de droits permettant d'appliquer la séparation des tâches" à la page 93. Vous utilisez la même boîte à outils que pour la création du profil de droits.

1. **Dans la Console de gestion Solaris, créez le rôle d'administrateur système.**

   Pour obtenir de l'aide, reportez-vous à la section "Création du rôle d'administrateur de sécurité dans Trusted Extensions" à la page 96.

2. **Affectez le profil de droits Custom System Administrator (Administrateur système personnalisé) au rôle.**

3. **Enregistrez les modifications.**

4. **Fermez la Console de gestion Solaris.**

▼ Création d'utilisateurs pouvant assumer des rôles dans Trusted Extensions

Pour créer un utilisateur local, vous pouvez utiliser l'interface de ligne de commande, comme décrit dans l'Exemple 4–7, au lieu de la procédure suivante. 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 le rôle d'administrateur de sécurité affecte les attributs relatifs à la sécurité tels que les mots de passe.

Avant de commencer

Vous devez être connecté en tant que superutilisateur, dans le rôle `root`, dans le rôle d'administrateur de sécurité ou dans le rôle d'administrateur principal. Le rôle d'administrateur de sécurité dispose du minimum de privilèges requis pour la création d'utilisateurs.

La Console de gestion Solaris s'affiche. Pour en savoir plus, reportez-vous à la section "Création du rôle d'administrateur de sécurité dans Trusted Extensions" à la page 96.

1. **Dans la Console de gestion Solaris, double-cliquez sur User Accounts (Comptes utilisateurs).**

2. **Dans le menu Action, choisissez Add User → User Wizard (Ajouter un utilisateur → Assistant utilisateur).**

Attention – Les noms et les ID des utilisateurs et des rôles proviennent du même pool. N'utilisez pas de noms ou d'ID existants pour les utilisateurs que vous ajoutez.

3. **Suivez l'aide en ligne.**

   Vous pouvez également suivre les procédures décrites à la section "How to Add a User With the Solaris Management Console's Users Tool" du *System Administration Guide: Basic Administration*.

4. **Après avoir créé l'utilisateur, double-cliquez sur l'utilisateur créé pour modifier les paramètres.**

Remarque – Pour les utilisateurs qui peuvent assumer plusieurs rôles, définissez l'état du compte utilisateur sur Always Available (Toujours disponible) et ne définissez pas de dates d'expiration des mots de passe.

Assurez-vous que les champs suivants sont correctement définis :

- Description : aucune information propriétaire ici.
- Mot de passe et validation : attribuez un mot de passe d'au moins 6 caractères alphanumériques.

  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.

- Disponibilité du compte : Always Available (Toujours disponible).
- Attributs Trusted Extensions : les valeurs par défaut sont correctes.

  Pour un système à une seule étiquette dans lequel les étiquettes ne doivent pas être visibles, choisissez l'option Hide (Masquer) sous Label: Show or Hide (Étiquette : afficher ou masquer).
- Utilisation du compte : définissez le temps d'inactivité et l'action d'inactivité (Idle).

  Verrouillage du compte : sélectionnez No (Non) pour tout utilisateur qui peut assumer un rôle.

5. **Fermez la Console de gestion Solaris.**

6 Personnalisez l'environnement de l'utilisateur.

a. Attribuez les autorisations appropriées.

Après avoir revu la stratégie de sécurité de votre site, vous pouvez décider d'accorder à vos premiers utilisateurs le profil Convenient Authorization (Autorisations appropriées). Avec ce profil, vous pouvez autoriser les utilisateurs à 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" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

b. Personnalisez les fichiers d'initialisation utilisateur.

Reportez-vous au Chapitre 7, "Gestion des utilisateurs, des droits et des rôles dans Trusted Extensions (tâches) " du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Reportez-vous également à la section "Gestion des utilisateurs et des droits à l'aide de la Console de gestion Solaris (liste des tâches) " du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

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

Sur un système multiétiquettes, 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" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Exemple 4–7 Utilisation de la commande `useradd` pour créer un utilisateur local

Dans cet exemple, l'utilisateur `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)`.

D'abord, 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, l'utilisateur `root` doit consulter le Tableau 1–2, puis créer l'utilisateur.

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

L'utilisateur `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, l'utilisateur `root` ajoute le rôle d'administrateur de sécurité à la définition de l'utilisateur. Le rôle a été créé à la section "Création du rôle d'administrateur de sécurité dans Trusted Extensions" à la page 96.

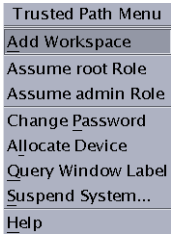
```
# usermod -R secadmin jandoe
```

▼ Vérification du fonctionnement des rôles Trusted Extensions

Pour vérifier chaque rôle, assumez le rôle correspondant. Effectuez ensuite des tâches que seul ce rôle peut exécuter.

Avant de commencer Si vous avez configuré DNS ou le routage, vous devez redémarrer 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. **Ouvrez le menu Trusted Path (Chemin de confiance).**
   - **Dans Trusted CDE, cliquez sur la zone de sélection d'espace de travail.**

     Assumez le rôle à partir du menu.
   - **Dans Trusted JDS, cliquez sur votre nom d'utilisateur dans la bande de confiance.**

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

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

3. **Dans l'espace de travail du rôle, lancez la Console de gestion Solaris.**

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

4. **Sélectionnez l'étendue appropriée pour le rôle que vous testez.**

5. **Cliquez sur System Services (Services système) et accédez aux utilisateurs (Users).**

   Vous êtes invité à saisir un mot de passe.

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

   b. **Double-cliquez sur User Accounts (Comptes utilisateur).**

6. **Cliquez sur un utilisateur.**

   - Le rôle d'administrateur système doit être en mesure de modifier les champs situés sous les onglets General (Général), Home Directory (Répertoire personnel) et Group (Groupe).

     Si vous avez configuré les rôles afin d'appliquer la séparation des tâches, le rôle d'administrateur système ne peut pas définir le mot de passe initial de l'utilisateur.
   - Le rôle d'administrateur de sécurité doit pouvoir modifier les champs sous tous les onglets.

     Si vous avez configuré les rôles afin d'appliquer la séparation des tâches, le rôle d'administrateur de sécurité ne peut pas créer d'utilisateur.
   - Le rôle d'administrateur principal doit pouvoir modifier des champs sous tous les onglets.

7. **(Facultatif) Si vous appliquez la séparation des tâches, empêchez l'utilisation des profils de droits par défaut.**

   Remarque – Lorsque le système est mis à niveau vers une version plus récente du SE Solaris, les profils System Administrator (Administrateur système), User Management (Gestion des utilisateurs) et User Security (Sécurité utilisateur) par défaut sont remplacés.

   Dans l'éditeur de confiance, effectuez l'une des étapes suivantes :

   - **Supprimez les trois profils de droits du fichier `prof_attr`.**

     La suppression permet d'empêcher un administrateur d'afficher ou d'attribuer ces profils. Supprimez également le fichier `prof_attr.orig`.
   - **Commentez les trois profils de droits dans le fichier `prof_attr`.**

     Le fait de commenter les profils de droits empêche ces profils d'être affichés dans la Console de gestion Solaris ou d'être utilisés dans les commandes de gestion des utilisateurs. Les profils et leur contenu peuvent tout de même être consultés dans le fichier `prof_attr`.

- **Saisissez une description différente pour les trois profils de droits dans le fichier `prof_attr`.**

  Modifiez le fichier `prof_attr` pour modifier le champ de description de ces profils de droits. Vous pouvez par exemple remplacer les descriptions par `Do not use this profile`. Cette modification indique à l'administrateur de ne pas utiliser le profil, mais n'empêche pas le profil d'être utilisé.

▼ Autorisation des utilisateurs à se connecter à une zone étiquetée

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

Avant de commencer Vous avez créé au moins une zone étiquetée. Cette zone n'est pas utilisée pour le clonage.

1. **Redémarrez le système.**

2. **Connectez-vous en tant qu'utilisateur `root`.**

3. **Redémarrez le service de zone.**

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

# 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 dans Trusted Extensions

Dans Trusted Extensions, les utilisateurs ont besoin d'accéder à leurs répertoires personnels sur chaque étiquette sur laquelle ils travaillent. Pour que tous les répertoires personnels soient à la disposition de l'utilisateur, vous devez créer un serveur d'annuaires personnel multiniveau, exécuter l'agent de montage automatique sur le serveur, puis exporter les répertoires personnels. Du côté client, vous pouvez exécuter des scripts pour trouver le répertoire personnel de chaque zone pour chaque utilisateur, ou vous pouvez faire en sorte que l'utilisateur se connecte au serveur d'annuaires personnel.

▼ Création du serveur d'annuaires personnel dans Trusted Extensions

Avant de commencer Vous devez être connecté en tant que superutilisateur, dans le rôle `root` ou dans le rôle d'administrateur principal.

1. **Installez et configurez le serveur d'annuaires personnel avec le logiciel Trusted Extensions.**
   - Si vous clonez les zones, assurez-vous que vous utilisez un instantané ZFS Solaris dont le répertoire personnel est vide.
   - Étant donné que les utilisateurs nécessitent un répertoire personnel sur chaque étiquette à laquelle ils peuvent se connecter, créez toutes les zones auxquelles un utilisateur peut se connecter. Par exemple, si vous utilisez le fichier `label_encodings` par défaut, vous devez créer une zone pour l'étiquette `PUBLIC`.

2. **Si vous utilisez UFS et non ZFS Solaris, activez le serveur NFS afin qu'il se serve lui-même.**

   a. **Dans la zone globale, modifiez l'entrée `automount` dans le fichier `nsswitch.conf`.**

      Utilisez l'éditeur de confiance pour modifier le fichier `/etc/nsswitch.conf`. Pour plus d'informations sur cette procédure, reportez-vous à la section "Modification des fichiers d'administration dans Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

      ```
      automount: files
      ```

   b. **Dans la zone globale, exécutez la commande `automount`.**

3. **Pour chaque zone étiquetée, suivez la procédure de montage automatique décrite à la section "Procédure de montage NFS de fichiers dans une zone étiquetée" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*. Revenez ensuite à cette procédure.**

4. **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.**

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

▼ Activation de l'accès des utilisateurs à leurs répertoires personnels dans Trusted Extensions

Les utilisateurs peuvent d'abord se connecter au serveur d'annuaires personnel pour créer un répertoire personnel qui peut être partagé avec d'autres systèmes. Pour créer un répertoire personnel sur chaque étiquette, les utilisateurs doivent se connecter au serveur d'annuaires personnel sur chaque étiquette.

En tant qu'administrateur, vous pouvez également créer un script afin de créer un point de montage pour les répertoires personnels sur tous les systèmes personnels de chaque utilisateur avant sa première connexion. Le script crée des points de montage sur chaque étiquette sur laquelle l'utilisateur est autorisé à travailler.

Avant de commencer Le serveur d'annuaires personnel pour votre domaine Trusted Extensions est configuré.

- **Choisissez d'autoriser la connexion directe au serveur ou d'exécuter un script.**
  - **Autorisez la connexion directe des utilisateurs au serveur d'annuaires personnel.**
    a. **Demandez à tous les utilisateurs de se connecter au serveur d'annuaires personnel.**
       Une fois la connexion établie, l'utilisateur doit se déconnecter.
    b. **Demandez aux utilisateurs de se connecter de nouveau, et, cette fois, de choisir une autre étiquette de connexion.**
       L'utilisateur utilise le générateur d'étiquettes pour choisir une étiquette de connexion différente. Une fois la connexion établie, l'utilisateur doit se déconnecter.
    c. **Demandez aux utilisateurs de répéter la procédure de connexion pour chaque étiquette qu'ils peuvent utiliser.**
    d. **Demandez aux utilisateurs de se connecter à partir de leur poste de travail normal.**
       Le répertoire personnel pour leur étiquette par défaut est disponible. 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.
  - **Écrivez un script qui crée un point de montage de répertoire personnel pour chaque utilisateur, puis exécutez-le.**

```
#!/bin/sh
#
for zoneroot in ‘/usr/sbin/zoneadm list -p | cut -d ":" -f4‘ ; do
```

```
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in ‘getent passwd|tr ’ ’ _‘ ; do
            uid=‘echo $j|cut -d ":" -f3‘
            if [ $uid -ge 100 ]; then
                gid=‘echo $j|cut -d ":" -f4‘
                homedir=‘echo $j|cut -d ":" -f6‘
                mkdir -m 711 -p $prefix$homedir
                chown $uid:$gid $prefix$homedir
            fi
        done
    fi
done
```

a. **À partir de la zone globale, exécutez ce script sur le serveur NFS.**

b. **Ensuite, exécutez le script sur tous les bureaux multiniveau auxquels l'utilisateur va se connecter.**

Ajout d'utilisateurs et d'hôtes à un réseau Trusted Network existant

Si des utilisateurs ne sont pas définis dans les cartes NIS, vous pouvez les ajouter à votre réseau.

Pour ajouter des hôtes et des étiquettes aux hôtes, reportez-vous aux procédures suivantes :

- Pour ajouter un hôte, utilisez l'outil Computers and Networks défini dans la Console de gestion Solaris. Pour plus d'informations, reportez-vous à la section “Procédure d’ajout d’hôtes au réseau connu du système ” du *Procédures de l’administrateur Oracle Solaris Trusted Extensions*.

  Lorsque vous ajoutez un hôte au serveur LDAP, ajoutez toutes les adresses IP associées à l'hôte. Toutes les adresses des zones, y compris les adresses des zones étiquetées, doivent être ajoutées au serveur LDAP.
- Pour connaître la procédure d'étiquetage d'un hôte, reportez-vous à la section “Procédure d’assignation d’un modèle de sécurité à un hôte ou à un groupe d’hôtes” du *Procédures de l’administrateur Oracle Solaris Trusted Extensions*.

▼ Ajout d'un utilisateur NIS au serveur LDAP

Avant de commencer

Vous devez être connecté en tant que superutilisateur, dans le rôle `root` ou dans le rôle d'administrateur principal.

1. **Collectez les informations dont vous avez besoin dans la base de données NIS.**

   a. **Créez un fichier à partir de l'entrée de l'utilisateur dans la base de données `aliases`.**

      ```
      % ypcat -k aliases | grep login-name > aliases.name
      ```

   b. **Créez un fichier à partir de l'entrée de l'utilisateur dans la base de données `passwd`.**

      ```
      % ypcat -k passwd | grep "Full Name" > passwd.name
      ```

   c. **Créez un fichier à partir de l'entrée de l'utilisateur dans la base de données `auto_home_`.**

      ```
      % ypcat -k auto_home | grep login-name > auto_home_label
      ```

2. **Reformatez les informations pour LDAP et Trusted Extensions.**

   a. **Utilisez la commande `sed` pour reformater l'entrée `aliases`.**

      ```
      % sed 's/ /:/g' aliases.login-name > aliases
      ```

   b. **Utilisez la commande `nawk` pour reformater l'entrée `passwd` .**

      ```
      % nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
      ```

   c. **Utilisez la commande `nawk` pour créer une entrée `shadow`.**

      ```
      % nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
      ```

   d. **Utilisez la commande `nawk` pour créer une entrée `user_attr` .**

      ```
      % nawk -F: '{print $1"::::lock_after_retries=yes-or-no;profiles=user-profile, ...;
      labelview=int-or-ext,show-or-hide;min_label=min-label;
      clearance=max-label;type=normal;roles=role-name,...;
      auths=auth-name,..."}' passwd.name > user_attr
      ```

3. **Copiez les fichiers modifiés dans le répertoire `/tmp` sur le serveur LDAP.**

   ```
   # cp aliases auto_home_internal passwd shadow user_attr /tmp/name
   ```

4. **À l'Étape 3, ajoutez des entrées aux fichiers pour les bases de données du serveur LDAP.**

   ```
   # /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
   -a simple -f /tmp/name/aliases aliases
   # /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
   -a simple -f /tmp/name/auto_home_internal auto_home_internal
   # /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
   -a simple -f /tmp/name/passwd passwd
   # /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
   -a simple -f /tmp/name/shadow shadow
   # /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
   -a simple -f /tmp/name/user_attr user_attr
   ```

Exemple 4–8 Ajout d'un utilisateur au serveur LDAP à partir d'une base de données NIS

Dans l'exemple suivant, l'administrateur ajoute un nouvel utilisateur au réseau approuvé. Les informations de l'utilisateur sont à l'origine stockées dans une base de données NIS. Pour protéger le mot de passe du serveur LDAP, l'administrateur exécute les commandes `ldapaddent` sur le serveur.

Dans Trusted Extensions, le nouvel utilisateur peut allouer des périphériques et joue un rôle Operator. Dans la mesure où l'utilisateur peut assumer un rôle, le compte utilisateur n'est pas verrouillé. L'étiquette minimale de l'utilisateur est `PUBLIC`. L'étiquette sur laquelle l'utilisateur travaille est `INTERNAL`, de sorte que `Jan` est ajouté à la base de données `auto_home_internal`. La base de données `auto_home_internal` monte automatiquement le répertoire personnel de `Jan`, avec des autorisations de lecture-écriture.

- Sur le serveur LDAP, l'administrateur extrait les informations utilisateur des bases de données NIS.

```
# ypcat -k aliases | grep jan.doe > aliases.jan
# ypcat passwd | grep "Jan Doe" > passwd.jan
# ypcat -k auto_home | grep jan.doe > auto_home_internal
```

- Ensuite, l'administrateur reformate les entrées pour le service LDAP.

```
# sed 's/ /:/g' aliases.jan > aliases
# nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
# nawk -F: '{print $1":"$2":6445::::::"}' passwd.jan > shadow
```

- L'administrateur crée une entrée `user_attr` pour Trusted Extensions.

```
# nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
labelview=internal,showsl;min_label=0x0002-08-08;
clearance=0x0004-08-78;type=normal;roles=oper;
auths=solaris.device.allocate"}' passwd.jan > user_attr
```

- L'administrateur copie les fichiers dans le répertoire `/tmp/jan`.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

- L'administrateur remplit le serveur avec les fichiers du répertoire `/tmp/jan`.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

Dépannage de votre configuration Trusted Extensions

Dans Trusted Extensions, les zones étiquetées communiquent avec le serveur X par l'intermédiaire de la zone globale. Par conséquent, les zones étiquetées doivent disposer de routes utilisables vers la zone globale. En outre, les options sélectionnées au cours d'une installation Solaris peuvent empêcher Trusted Extensions d'utiliser les interfaces vers la zone globale.

La commande `netservices limited` a été exécutée après l'activation de Trusted Extensions

Description :

Au lieu d'exécuter la commande `netservices limited` avant d'activer Trusted Extensions, vous avez exécuté la commande dans la zone globale par la suite. Par conséquent, les zones étiquetées ne parviennent pas à se connecter au serveur X dans la zone globale.

Solution :

Exécutez les commandes suivantes pour ouvrir les services dont Trusted Extensions a besoin pour communiquer entre les zones :

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

Impossible d'ouvrir la fenêtre de console dans une zone étiquetée

Description :

Lorsque vous essayez d'ouvrir une fenêtre de console dans une zone étiquetée, l'erreur suivante s'affiche dans une boîte de dialogue :

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

Solution :

Vérifiez que les deux lignes ci-après sont présentes dans chaque entrée de la zone dans le fichier `/etc/security/exec_attr` :

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

Si elles n'y sont pas, le package Trusted Extensions qui ajoute ces entrées n'a pas été installé dans les zones étiquetées. Dans ce cas, recréez les zones étiquetées. Pour plus d'informations sur cette procédure, reportez-vous à la section “Création de zones étiquetées” à la page 68.

La zone étiquetée ne peut accéder au serveur X

Description :

Si une zone étiquetée ne peut accéder au serveur X, des messages tels que les suivants s'affichent :

- `Action failed. Reconnect to Solaris Zone?`
- `No route available`
- `Cannot reach globalzone-`*`hostname`* `:0`

Cause :

Les zones étiquetées peuvent ne pas être en mesure d'accéder au serveur X pour l'une des raisons suivantes :

- La zone n'est pas initialisée et attend que le processus `sysidcfg` s'achève.
- Le nom d'hôte de la zone étiquetée n'est pas reconnu par le service de nommage qui s'exécute dans la zone globale.
- Aucune interface n'est spécifiée comme `all-zones`.
- L'interface réseau de la zone étiquetée est en panne.
- La recherche de nom LDAP a échoué.
- Les montages NFS ne fonctionnent pas.

Procédure de résolution :

Effectuez les opérations suivantes :

1. Connectez-vous à la zone.

   Vous pouvez utiliser la commande `zlogin` ou l'action Zone Terminal Console (Console de terminal de zone).

   ```
   # zlogin -z zone-name
   ```

   Si vous ne pouvez pas vous connecter en tant que superutilisateur, utilisez la commande `zlogin -S` pour contourner l'authentification.

2. Vérifiez que la zone est en cours d'exécution.

   ```
   # zoneadm list
   ```

   Si une zone a un statut `running`, elle exécute au moins un processus.

3. Résolvez tout problème empêchant les zones étiquetées d'accéder au serveur X.
   - Initialisez la zone en exécutant le processus `sysidcfg`.

     Exécutez le programme `sysidcfg` de manière interactive. Répondez aux invites dans la console de terminal de zone ou dans la fenêtre de terminal dans laquelle vous avez exécuté la commande `zlogin`.

Pour exécuter le processus `sysidcfg` de manière non interactive, vous pouvez effectuer l'une des opérations suivantes :

- Spécifiez l'option Initialize (Initialiser) pour le script `/usr/sbin/txzonemgr`.

  L'option Initialize (Initialiser) vous permet de fournir des valeurs par défaut aux questions `sysidcfg`.
- Écrivez votre propre script `sysidcfg`.

  Pour plus d'informations, reportez-vous à la page de manuel `sysidcfg(4)`.

- Vérifiez que le serveur X est disponible pour la zone.

  Connectez-vous à la zone étiquetée. Définissez la variable `DISPLAY` de sorte qu'elle pointe vers le serveur X, puis ouvrez une fenêtre.

  ```
  # DISPLAY=global-zone-hostname:n.n
  # export DISPLAY
  # /usr/openwin/bin/xclock
  ```

  Si aucune fenêtre étiquetée n'apparaît, le réseau de la zone n'a pas été correctement configuré pour cette zone étiquetée.

  Remarque – Si vous exécutez une version ultérieure à la version Solaris 10 5/09 de Trusted CDE, reportez-vous à la section "Résolution de l'acheminement zone locale-zone globale dans Trusted CDE" à la page 167.

- Configurez le nom d'hôte de la zone avec le service de nommage.

  Le fichier `/etc/hosts` local de la zone n'est pas utilisé. Au lieu de cela, les informations équivalentes doivent être spécifiées dans la zone globale ou sur le serveur LDAP. Ces informations doivent inclure l'adresse IP du nom de l'hôte affecté à la zone.
- Aucune interface n'est spécifiée comme `all-zones`.

  À moins que toutes les zones aient des adresses IP sur le même sous-réseau que la zone globale, il peut être nécessaire de configurer une interface `all-zones` (partagée). Cette configuration permet la connexion d'une zone étiquetée au serveur X de la zone globale. Si vous souhaitez limiter les connexions à distance au serveur X de la zone globale, vous pouvez utilisez `vni0` comme adresse `all-zones`.

  Si vous ne souhaitez *pas* configurer d'interface `all-zones`, vous devez fournir une route au serveur X de la zone globale pour chaque zone. Ces routes doivent être configurées dans la zone globale.
- L'interface réseau de la zone étiquetée est en panne.

  ```
  # ifconfig -a
  ```

Utilisez la commande `ifconfig` pour vérifier que l'interface réseau de la zone étiquetée est à la fois `UP` et `RUNNING`.

- La recherche de nom LDAP a échoué.

  Utilisez la commande `ldaplist` pour vérifier que chaque zone peut communiquer avec le serveur LDAP ou le serveur proxy LDAP. Sur le serveur LDAP, vérifiez que la zone est répertoriée dans la base de données `tnrhdb`.

- Les montages NFS ne fonctionnent pas.

  En tant que superutilisateur, redémarrez `automount` dans la zone ou ajoutez une entrée `crontab` pour exécuter la commande `automount` toutes les cinq minutes.

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 Solaris.

▼ Copie de fichiers sur un support amovible dans Trusted Extensions

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

Remarque – Au cours de la configuration de Trusted Extensions, le superutilisateur ou un rôle équivalent copie les fichiers d'administration depuis et vers un support amovible. Étiquetez le support avec `Trusted Path`.

Avant de commencer Pour copier les fichiers d'administration, vous devez être connecté en tant que superutilisateur ou assumer un rôle dans la zone globale.

1 Allouez le périphérique approprié.

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

- Dans Solaris Trusted Extensions (CDE), un *gestionnaire de fichiers* (File Manager) affiche le contenu du support amovible.

- Dans Solaris Trusted Extensions (JDS), un *navigateur de fichiers* (File Browser) affiche le contenu.

Dans le cadre de cette procédure, le terme navigateur de fichiers est utilisé pour faire référence à cette interface graphique.

2 Ouvrez un deuxième navigateur de fichiers.

3 Accédez au dossier contenant les fichiers à copier.

Par exemple, vous avez peut-être copié les fichiers dans un dossier `/export/clientfiles`.

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 support amovible.

5 Libérez le périphérique.

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

6 Dans le navigateur de fichiers du support amovible, sélectionnez Eject (Éjecter) dans le menu File (Fichier).

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

Exemple 4–9 Conservation de fichiers de configuration identiques sur tous les systèmes

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

Par exemple, il copie la boîte à outils Trusted Extensions utilisée par la Console de gestion Solaris pour l'étendue LDAP, `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`. Il personnalise les modèles d'hôte distant dans le fichier `tnrhtp`, crée une liste des serveurs DNS et de fichiers de configuration du contrôle. Il modifie également le fichier `policy.conf` pour son site. Tous ces fichiers sont alors copiés dans le répertoire permanent.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
```

```
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

Le gestionnaire d'allocation de périphériques (Device Allocation Manager) est utilisé pour allouer une disquette dans la zone globale, et l'administrateur transfère les fichiers sur la disquette. Sur une disquette séparée, étiquetée `ADMIN_HIGH`, il place le fichier `label_encodings` pour le site.

Lors de la copie de fichiers sur un système, il modifie les entrées `dir:` du fichier `/etc/security/audit_control` pour ce système.

Copie de fichiers dans Trusted Extensions à partir d'un support 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 connecté en tant que superutilisateur ou assumer un rôle 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 *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

   - Dans Solaris Trusted Extensions (CDE), un *gestionnaire de fichiers* (File Manager) affiche le contenu du support amovible.
   - Dans Solaris Trusted Extensions (JDS), un *navigateur de fichiers* (File Browser) affiche le contenu.

   Dans le cadre de cette procédure, le terme navigateur de fichiers est utilisé pour faire référence à cette interface graphique.

2. **Insérez le support 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/tnrhtp /etc/security/tsol/tnrhtp.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 support 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 *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.

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

Exemple 4–10 Chargement des fichiers de configuration du contrôle dans Trusted Extensions

Dans cet exemple, les rôles ne sont pas encore configurés sur le système. L'utilisateur `root` a besoin de copier les fichiers de configuration sur un support amovible. Le contenu du support peut ensuite être copié sur d'autres systèmes. Ces fichiers doivent être copiés sur chaque système configuré avec le logiciel Trusted Extensions.

L'utilisateur `root` alloue le périphérique `floppy_0` dans le gestionnaire d'allocation de périphériques (Device Allocation Manager) et répond `yes` (oui) à la requête de montage. Ensuite, l'utilisateur `root` insère la disquette contenant les fichiers de configuration et les copie sur le disque. La disquette porte l'étiquette `Trusted Path`.

Pour lire les données à partir du support, l'utilisateur `root` alloue le périphérique sur l'hôte récepteur, puis télécharge le contenu.

Si les fichiers de configuration se trouvent sur une bande, l'utilisateur `root` alloue le périphérique `mag_0`. Si les fichiers de configuration se trouvent sur un CD-ROM, l'utilisateur `root` alloue le périphérique `cdrom_0`.

▼ Suppression de Trusted Extensions du système

Pour supprimer Trusted Extensions de votre système Solaris, vous devez effectuer des étapes spécifiques afin de supprimer les personnalisations Trusted Extensions du système Solaris.

1. **Comme dans le SE Solaris, archivez les données contenues dans les zones étiquetées que vous souhaitez conserver.**

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

   Pour plus d'informations, reportez-vous à la section "How to Remove a Non-Global Zone" du *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.

3 **Désactivez le service Trusted Extensions.**

```
# svcadm disable labeld
```

4 **Exécutez la commande `bsmunconv`.**

Pour connaître l'effet de cette commande, reportez-vous à la page de manuel `bsmunconv(1M)`.

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

6 **Configurez le système.**

La configuration de différents services peuvent être nécessaire pour votre système Solaris. Peuvent être concernés par exemple le contrôle, 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 Sun Java System Directory Server et de la Console de gestion Solaris en cas d'utilisation avec Trusted Extensions. Le serveur d'annuaire fournit les services LDAP. LDAP est le service de nommage pris en charge pour Trusted Extensions. La Console de gestion Solaris est l'interface graphique d'administration pour les bases de données locales et 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. Suivez les instructions données de l'*une* des listes de tâches suivantes :

- "Configuration d'un serveur LDAP sur un hôte Trusted Extensions (liste des tâches)" à la page 119
- "Configuration d'un serveur proxy LDAP sur un hôte Trusted Extensions (liste des tâches)" à la page 120

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

Tâche	Description	Voir
Définition d'un serveur LDAP Trusted Extensions.	Si vous n'avez pas encore de Sun Java System Directory Server, montez votre premier système Trusted Extensions du serveur d'annuaire. Ce système n'a aucune zone étiquetée installée. Les autres systèmes Trusted Extensions sont des clients de ce serveur.	"Collecte d'informations pour le serveur d'annuaire pour LDAP" à la page 121 "Installation du Sun Java System Directory Server" à la page 122 "Configuration des journaux pour le Sun Java System Directory Server" à la page 127

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 Sun Java System Directory Server" à la page 129
Configuration de la Console de gestion Solaris afin qu'elle fonctionne avec le serveur d'annuaire.	Configurez manuellement une boîte à outils LDAP pour la Console de gestion Solaris. La boîte à outils peut être utilisée pour modifier les attributs Trusted Extensions des objets du réseau.	"Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132
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 64

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

Utilisez cette liste des tâches si vous avez déjà un Sun Java System Directory Server 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 Sun Java System Directory Server" à la page 129
Configuration d'un serveur proxy LDAP.	Faites du système Trusted Extensions le serveur proxy pour tous les autres systèmes Trusted Extensions. Les autres systèmes Trusted Extensions utilisent ce serveur proxy pour accéder au serveur LDAP.	"Création d'un serveur proxy LDAP" à la page 132
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 Sun Java System Directory Server" à la page 128
Configuration de la Console de gestion Solaris afin qu'elle fonctionne avec le serveur proxy LDAP.	Configurez manuellement une boîte à outils LDAP pour la Console de gestion Solaris. La boîte à outils peut être utilisée pour modifier les attributs Trusted Extensions des objets du réseau.	"Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132
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 64

Configuration du Sun Java System Directory Server 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 Sun Java System Directory Server (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 ou en tant que serveur pour les clients Sun Ray, 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
Sun Java System Directory Server *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.

Invite de l'Assistant d'installation	Action ou informations
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`.
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 `software-version TIMES 1000`. Pour la version 5.2 du logiciel, cette convention donnerait le port `5200`.

▼ Installation du Sun Java System Directory Server

Les packages du serveur d'annuaire sont disponibles sur le site Web Sun Software Gateway (`http://www.oracle.com/solaris`).

Avant de commencer

Vous vous trouvez sur un système Trusted Extensions avec une seule zone globale installée. Le système n'a aucune zone étiquetée.

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 que vous pouvez définir sur le client, reportez-vous à la section "Managing Password Information" du *System Administration Guide: Security Services*. 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
```

Sur un système exécutant une version antérieure à la version Solaris 10 8/07, insérez les entrées IPv4 et IPv6 dans le fichier `/etc/inet/ipnodes`. Les entrées d'un système doivent être contiguës dans le fichier.

Si vous n'exécutez pas la dernière version du SE Solaris, les patchs suivants doivent être installés. Le premier nombre correspond à un patch SPARC. Le deuxième nombre correspond à un patch X86.

- 138874–05, 138875–05 : LDAP natif, PAM, name-service-switch patch
- 119313-35, 119314-36 : patch WBEM
- 121308-21, 121308-21 : patch de la console de gestion Solaris
- 119315-20, 119316-20 : patch d'applications de gestion Solaris

2 **Vous trouverez les packages Sun Java System Directory Server sur le site Web Oracle Sun.**

a. **Sur la page Sun Software Gateway (`http://www.oracle.com/solaris`), cliquez sur l'onglet Get It.**

b. **Cliquez sur la case à cocher correspondant à Sun Java Identity Management Suite.**

c. **Cliquez sur Submit (Envoyer).**

d. **Si vous n'êtes pas enregistré, enregistrez-vous.**

e. **Connectez-vous pour télécharger le logiciel.**

f. **Cliquez sur le centre de téléchargement dans le coin supérieur gauche de l'écran.**

g. **Sous Identity Management, téléchargez le logiciel le plus récent adapté à 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 121. Pour obtenir une liste complète des questions, des valeurs par défaut et des réponses suggérées, reportez-vous au

Chapitre 11, "Configuration de Sun Java System Directory Server avec les clients LDAP (tâches)" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* et au Chapitre 12, "Configuration des clients LDAP (tâches)" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

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 Sun Java System Directory Server 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 *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ 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.

1 Installez Trusted Extensions sur un système.

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

Remarque – Si vous n'exécutez pas la dernière version du SE Solaris, les patchs suivants doivent être installés. Le premier nombre correspond à un patch SPARC. Le deuxième nombre correspond à un patch X86.

- 138874–05, 138875–05 : LDAP natif, PAM, name-service-switch patch
- 119313-35, 119314-36 : patch WBEM
- 121308-21, 121308-21 : patch de la console de gestion Solaris
- 119315-20, 119316-20: patch d'applications de gestion Solaris

---

2 Sur le client, modifiez le fichier `/etc/nsswitch.ldap` par défaut.

Les entrées en gras indiquent les modifications. Le fichier se présente de la manière suivante :

```
# /etc/nsswitch.ldap
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses LDAP in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

# LDAP service requires that svc:/network/ldap/client:default be enabled
# and online.

# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:     files ldap
group:      files ldap

# consult /etc "files" only if ldap is down.
hosts:      files ldap dns [NOTFOUND=return] files

# Note that IPv4 addresses are searched for in all of the ipnodes databases
# before searching the hosts databases.
ipnodes:    files ldap [NOTFOUND=return] files
```

```
networks:   files ldap [NOTFOUND=return] files
protocols:  files ldap [NOTFOUND=return] files
rpc:        files ldap [NOTFOUND=return] files
ethers:     files ldap [NOTFOUND=return] files
netmasks:   files ldap [NOTFOUND=return] files
bootparams: files ldap [NOTFOUND=return] files
publickey:  files ldap [NOTFOUND=return] files

netgroup:   ldap

automount:  files ldap
aliases:    files ldap

# for efficient getservbyname() avoid ldap
services:   files ldap

printers:   user files ldap

auth_attr:  files ldap
prof_attr:  files ldap

project:    files ldap

tnrhtp:     files ldap
tnrhdb:     files ldap
```

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

Cette commande copie le fichier `nsswitch.ldap` dans le fichier `nsswitch.conf`.

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 profileNmae=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4 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 "Commutateur enableShadowUpdate" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* et à la page de manuel `ldapclient`(1M).

▼ Configuration des journaux pour le Sun Java System Directory Server

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 droits d'accès au 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.

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 Sun Java System Directory Server

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

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

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

2 **Sélectionnez la boîte à outils Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`).**

3 **Cliquez sur Configuration, puis cliquez Computers and Networks (Ordinateurs et réseaux).**

Vous êtes invité à saisir votre mot de passe.

4 **Saisissez le mot de passe approprié.**

5 **Double-cliquez sur Trusted Network Zones (Zones de réseau de confiance).**

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

7 **Ajoutez un port multiniveau pour le protocole TCP :**

a. **Cliquez sur Add for the Multilevel Ports for Zone's IP Addresses (Ajouter pour les ports multiniveau pour les adresses IP de la zone).**

b. **Saisissez le numéro de port 389, puis cliquez sur OK.**

8 **Ajoutez un port multiniveau pour le protocole UDP :**

   a. **Cliquez sur Add for the Multilevel Ports for Zone's IP Addresses (Ajouter pour les ports multiniveau pour les adresses IP de la zone).**

   b. **Saisissez le numéro de port 389.**

   c. **Choisissez le protocole UDP et cliquez sur OK.**

9 **Cliquez sur OK pour enregistrer les paramètres.**

10 **Mettez à jour le noyau.**

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

▼ Remplissage du Sun Java System Directory Server

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 remplir la base de données à partir d'un client LDAP sur lequel 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 125.

Si la sécurité du site requiert la séparation des tâches, exécutez les procédures suivantes avant de remplir le serveur d'annuaire :

- "Création de profils de droits permettant d'appliquer la séparation des tâches" à la page 93
- "Création du rôle d'administrateur de sécurité dans Trusted Extensions" à la page 96
- "Création d'un rôle d'administrateur système limité" à la page 99

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

Si vous exécutez la version Solaris 10 11/06 sans patch, copiez le fichier `ipnodes`.

```
# cd /etc/inet
# cp ipnodes /setup/files
```

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

4 Supprimez l'entrée `?:::::?` du fichier `/setup/files/auth_attr`.

5 Supprimez l'entrée `::::` du fichier `/setup/files/prof_attr`.

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

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/&
```

7 Ajoutez tous les systèmes sur le réseau au fichier `/setup/files/tnrhdb`.

Aucun mécanisme de caractère générique ne peut être utilisé ici. L'adresse IP de chaque système qui doit être contacté, y compris les adresses IP des zones étiquetées, *doit* se trouver dans ce fichier.

a. Ouvrez l'éditeur de confiance et modifiez le fichier `/setup/files/tnrhdb`.

b. Ajoutez toutes les adresses IP présentes sur un système étiqueté dans le domaine Trusted Extensions.

Les systèmes étiquetés sont de type `cipso`. En outre, le nom du modèle de sécurité pour les systèmes étiquetés est `cipso`. Par conséquent, dans la configuration par défaut, une entrée `cipso` est similaire à l'exemple suivant :

```
192.168.25.2:cipso
```

Remarque – Cette liste inclut les adresses IP des zones globales et étiquetées.

c. Ajoutez tous les systèmes non étiquetés avec lesquels le domaine peut communiquer.

Les systèmes sans étiquette sont de type `unlabeled`. Le nom du modèle de sécurité pour les systèmes sans étiquette est `admin_low`. Par conséquent, dans la configuration par défaut, une entrée correspondant à un système sans étiquette est similaire à l'exemple suivant :

```
192.168.35.2:admin_low
```

d. Enregistrez le fichier et quittez l'éditeur.

e. Vérifiez la syntaxe du fichier.

```
# tnchkdb -h /setup/files/tnrhdb
```

f. Corrigez les erreurs éventuelles avant de poursuivre.

8 Copiez le fichier `/setup/files/tnrhdb` dans le fichier `/etc/security/tsol/tnrhdb`.

9 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
```

10 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)`.

Création d'un proxy Trusted Extensions pour un Sun Java System Directory Server existant

Tout d'abord, vous devez ajouter les bases de données Trusted Extensions au serveur d'annuaire existant sur un système 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 125.

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 Sun Java System Directory Server" à la page 129.

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`.

Pour plus d'informations, reportez-vous au Chapitre 12, "Configuration des clients LDAP (tâches)" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

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 *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)

La Console de gestion Solaris est l'interface graphique permettant d'administrer le réseau de systèmes exécutant Trusted Extensions.

Tâche	Description	Voir
Initialisation de la Console de gestion Solaris.	Initialisez la Console de gestion Solaris. Cette procédure est exécutée une fois par système dans la zone globale.	"Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61

Tâche	Description	Voir
Enregistrement des informations d'identification et de connexion.	Authentifiez la Console de gestion Solaris avec le serveur LDAP.	"Enregistrement des informations d'identification et de connexion LDAP avec la Console de gestion Solaris" à la page 133
Activation de l'administration à distance sur un système.	Par défaut, un client Console de gestion Solaris ne peut pas communiquer avec un serveur de console sur un autre système. Vous devez explicitement activer l'administration à distance.	"Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau" à la page 134
Création de la boîte à outils LDAP.	Créez la boîte à outils LDAP pour Trusted Extensions dans la Console de gestion Solaris.	"Modification de la boîte à outils LDAP dans la Console de gestion Solaris" à la page 135
Vérification des communications.	Vérifiez si les hôtes Trusted Extensions peuvent devenir des clients LDAP.	"Vérification des informations Trusted Extensions contenues dans la Console de gestion Solaris" à la page 136

▼ Enregistrement des informations d'identification et de connexion LDAP avec la Console de gestion Solaris

Avant de commencer

Vous devez être l'utilisateur `root` sur un serveur LDAP exécutant Trusted Extensions. Le serveur peut être un serveur proxy.

Votre Sun Java System Directory Server doit être configuré. Vous avez terminé l'une des configurations suivantes :

- "Configuration d'un serveur LDAP sur un hôte Trusted Extensions (liste des tâches)" à la page 119
- "Configuration d'un serveur proxy LDAP sur un hôte Trusted Extensions (liste des tâches)" à la page 120

1 Enregistrez les informations d'identification et de connexion d'administration LDAP.

```
LDAP-Server # /usr/sadm/bin/dtsetup storeCred
Administrator DN:       Type the value for cn on your system
Password:       Type the Directory Manager password
Password (confirm):       Retype the password
```

2 Répertoriez les étendues sur le serveur d'annuaire.

```
LDAP-Server # /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:       Displays name of file scope
Scope 2 ldap:       Displays name of ldap scope
```

La configuration de votre serveur LDAP détermine les étendues répertoriées. L'étendue LDAP n'est pas répertoriée jusqu'à ce que la boîte à outils LDAP soit modifiée. La boîte à outils ne peut pas être modifiée avant que le serveur ne soit enregistré.

Exemple 5–1 Enregistrement des informations d'identification et de connexion LDAP

Dans cet exemple, le nom du serveur LDAP est `LDAP1` et la valeur de `cn` est la valeur par défaut, `Directory Manager`.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:/LDAP1/LDAP1
Scope 2 ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com
```

▼ Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau

Par défaut, les systèmes Solaris ne sont pas configurés pour écouter sur les ports qui présentent des risques liés à la sécurité. Par conséquent, vous devez configurer explicitement tous les systèmes que vous prévoyez d'administrer à distance afin qu'ils acceptent les communications réseau. Par exemple, pour administrer les bases de données réseau sur le serveur LDAP à partir d'un client, le serveur Console de gestion Solaris sur le serveur LDAP doit accepter les communications réseau.

Pour voir une illustration de la configuration requise de la Console de gestion Solaris pour un réseau avec un serveur LDAP, reportez-vous à la section "Communication client-serveur avec la Console de gestion Solaris" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Avant de commencer Vous devez être connecté en tant que superutilisateur dans la zone globale sur le système serveur Console de gestion Solaris. Dans cette procédure, ce système est appelé le système distant. En outre, vous devez avoir accès à la ligne de commande pour le système client en tant que superutilisateur.

1 Sur le système distant, activez le système afin qu'il accepte les connexions à distance.

Le démon `smc` est contrôlé par le service `wbem`. Si le service `options/tcp_listen` `wbem` est défini sur `true`, le serveur Console de gestion Solaris accepte les connexions à distance.

```
# /usr/sbin/svcprop -p options wbem
options/tcp_listen boolean false
# svccfg -s wbem setprop options/tcp_listen=true
```

2. **Actualisez et redémarrez le service `wbem`.**

```
# svcadm refresh wbem
# svcadm restart wbem
```

3. **Vérifiez que le service `wbem` est configuré pour accepter les connexions à distance.**

```
# svcprop -p options wbem
options/tcp_listen boolean true
```

4. **Sur le système distant et tous les clients qui devront accéder à la Console de gestion Solaris, assurez-vous que les connexions à distance sont activées dans le fichier `smcserver.config`.**

   a. **Ouvrez le fichier `smcserver.config` dans l'éditeur de confiance.**

   ```
   # /usr/dt/bin/trusted_edit /etc/smc/smcserver.config
   ```

   b. **Définissez le paramètre `remote.connexions` sur `true`.**

   ```
   ## remote.connections=false
   remote.connections=true
   ```

   c. **Enregistrez le fichier et quittez l'éditeur de confiance.**

Erreurs fréquentes Si vous redémarrez ou activez le service `wbem`, vous devez vous assurer que le paramètre `remote.connections` du fichier `smcserver.config` reste défini sur `true`.

▼ Modification de la boîte à outils LDAP dans la Console de gestion Solaris

Avant de commencer Vous devez être connecté au serveur LDAP en tant que superutilisateur. Les informations d'identification et de connexion LDAP doivent être enregistrées avec la Console de gestion Solaris, et vous devez connaître la sortie de la commande `/usr/sadm/bin/dtsetup scopes`. Pour plus d'informations, reportez-vous à la section "Enregistrement des informations d'identification et de connexion LDAP avec la Console de gestion Solaris" à la page 133.

1. **Accédez à la boîte à outils LDAP.**

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# ls *tbx
tsol_ldap.tbx
```

2. **Indiquez le nom du serveur LDAP.**

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

b. Copiez et collez le chemin d'accès complet à la boîte à outils `tsol_ldap.tbx` comme argument dans l'éditeur.

Par exemple, le chemin d'accès suivant correspond à l'emplacement par défaut de la boîte à outils LDAP :

```
/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
```

c. Remplacez les informations d'étendue.

Remplacez la balise `server` entre les balises `<Scope>` et `</Scope>` par la sortie de la ligne `ldap:/.....` de la commande `/usr/sadm/bin/dtsetup scopes`.

```
<Scope>ldap:/<ldap-server-name>/<dc=domain,dc=suffix></Scope>
```

d. Remplacez chaque occurrence de `<?Server?>` ou `<?server ?>` par le serveur LDAP.

```
<Name>This Computer (ldap-server-name: Scope=ldap, Policy=TSOL)</Name>
services and configuration of ldap-server-name.</Description>
and configuring ldap-server-name.</Description>
...
```

e. Enregistrez le fichier et quittez l'éditeur.

3 Actualisez et redémarrez le service `wbem`.

```
# svcadm refresh wbem
# svcadm restart wbem
```

Exemple 5–2 Configuration de la boîte à outils LDAP

Dans cet exemple, le nom du serveur LDAP est `LDAP1`. Pour configurer la boîte à outils, l'administrateur remplace les instances de `<?server ?>` par `LDAP1`.

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# /usr/dt/bin/trusted_edit /tsol_ldap.tbx
<Scope>ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com</Scope

...
<Name>This Computer (LDAP1: Scope=ldap, Policy=TSOL)</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
...
```

▼ Vérification des informations Trusted Extensions contenues dans la Console de gestion Solaris

Pour voir une illustration de la configuration requise de la Console de gestion Solaris pour un réseau avec un serveur LDAP et pour un réseau sans serveur LDAP, reportez-vous à la section "Communication client-serveur avec la Console de gestion Solaris" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Avant de commencer

Vous devez être connecté à un client LDAP dans un rôle d'administration ou en tant que superutilisateur. Pour faire d'un système un client LDAP, reportez-vous à la section "Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 64.

Pour administrer le système local, vous devez avoir exécuté les tâches de la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61.

Pour vous connecter à un serveur de console sur un système distant à partir du système local, vous devez avoir exécuté les tâches de la section "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61 sur les deux systèmes. En outre, sur le système distant, vous devez avoir exécuté les tâches de la section "Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau" à la page 134.

Pour administrer les bases de données dans le service de nommage LDAP à partir du client LDAP, sur le serveur LDAP, vous devez avoir exécuté les tâches de la section "Modification de la boîte à outils LDAP dans la Console de gestion Solaris" à la page 135 en plus de procédures précédentes.

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

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

2 **Ouvrez une boîte à outils Trusted Extensions.**

Une boîte à outils Trusted Extensions a la valeur `Policy=TSOL`.

- **Sur un réseau sécurisé qui utilise le protocole LDAP en tant que service de nommage, effectuez les tests suivants :**

  a. **Pour vérifier qu'il est possible d'accéder aux bases de données d'administration locales, ouvrez la boîte à outils suivante :**

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

  b. **Pour vérifier que les bases de données d'administration locale du serveur LDAP sont accessibles, spécifiez la boîte à outils suivante :**

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

  c. **Pour vérifier que les bases de données du service de nommage sur le serveur LDAP sont accessibles, spécifiez la boîte à outils suivante :**

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

- **Sur un réseau sécurisé qui n'utilise pas LDAP en tant que service de nommage, effectuez les tests suivants :**

  a. **Pour vérifier qu'il est possible d'accéder aux bases de données d'administration locales, ouvrez la boîte à outils suivante :**

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

  b. **Pour vérifier qu'il est possible d'accéder aux bases de données d'administration locales d'un système distant, ouvrez la boîte à outils suivante :**

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

3 **Sous System Configuration (Configuration système), accédez à Computers and Networks (Ordinateurs et réseaux), puis Security Templates (Modèles de sécurité).**

4 **Vérifiez que les bons modèles et étiquettes ont été appliqués aux systèmes distants.**

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

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

Erreurs fréquentes

Pour dépanner la configuration LDAP, reportez-vous au Chapitre 13, “LDAP Troubleshooting (Reference)” du *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

◆ ◆ ◆ CHAPITRE 6

Configuration d'un écouteur avec Trusted Extensions (tâches)

La configuration et l'administration du logiciel Trusted Extensions sur des écouteurs, tels que la série Netra, requièrent une modification des paramètres de sécurité sur l'écouteur afin d'activer l'accès distant. L'administration d'un système Trusted Extensions distant requiert une configuration similaire. Pour exécuter une interface graphique d'administration, il peut être nécessaire d'exécuter le processus sur le système distant et d'afficher l'interface graphique sur l'ordinateur de bureau.

Pour en savoir plus sur la configuration requise, reportez-vous au Chapitre 8, "Administration à distance dans Trusted Extensions (tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

Remarque – Les méthodes de configuration exigées par l'écouteur et les 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 20.

Configuration de l'écouteur dans Trusted Extensions (liste des tâches)

Sur les écouteurs, une console est connectée au moyen d'une ligne série à une fenêtre d'émulateur de terminal. La ligne est généralement sécurisée par la commande `tip`. En fonction du type du deuxième système disponible, vous pouvez utiliser l'une des méthodes suivantes pour configurer un écouteur. Les méthodes sont répertoriées de la plus sûre à la moins sûre dans le tableau ci-dessous. Ces instructions s'appliquent également aux systèmes distants.

Tâche	Description	Voir
Activation de la connexion à distance par l'utilisateur `root`.	Si vous n'utilisez pas LDAP, vous devez d'abord vous connecter à l'écouteur en tant qu'utilisateur `root`. Si vous utilisez LDAP, vous pouvez ignorer cette procédure.	"Activation de la connexion à distance par l'utilisateur `root` dans Trusted Extensions" à la page 141
Activation de la connexion à distance.	Activez la connexion à distance pour un utilisateur qui peut prendre le rôle `root` ou un autre rôle d'administration.	"Activation de la connexion à distance par un rôle dans Trusted Extensions" à la page 141
	Activez l'administration des systèmes Trusted Extensions à partir d'un système sans étiquette.	"Activation de la connexion à distance à partir d'un système sans étiquette" à la page 143
	Autorisez un utilisateur à accéder à la zone globale d'un écouteur.	"Procédure d'octroi à des utilisateurs spécifiques de l'autorisation de se connecter à distance à la zone globale dans Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*
(Facultatif) Activation de l'affichage des interfaces graphiques d'administration.	Activez les interfaces graphiques d'administration s'exécutant sur l'écouteur afin de les afficher sur l'ordinateur de bureau.	"Activation de l'affichage à distance des interfaces graphiques d'administration" à la page 145
(Facultatif) Activation de VNC (Virtual Network Computing)	À partir de n'importe quel client, utilisez le serveur Xvnc du système Trusted Extensions distant pour afficher une session multiniveau sur le client.	"Procédure d'utilisation de Xvnc afin d'accéder à distance à un système Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*
Choix d'une méthode de configuration et d'administration pour configurer l'écouteur.	Affectez un rôle ou connectez-vous en tant que superutilisateur pour administrer le système distant.	"Utilisation de la commande `rlogin` ou `ssh` pour se connecter à un écouteur dans Trusted Extensions et l'administrer" à la page 145
	Utilisation de la Console de gestion Solaris sur l'écouteur.	"Utilisation d'une Console de gestion Solaris à distance pour administrer dans l'étendue fichiers" à la page 144
	Si vous n'avez aucun système à multifenêtrage, utilisez la connexion série en tant que superutilisateur. Cette procédure n'est pas sûre.	Aucune configuration requise.

Remarque – Consultez votre stratégie de sécurité pour déterminer les méthodes d'administration à distance possibles sur votre site.

▼ Activation de la connexion à distance par l'utilisateur `root` dans Trusted Extensions

Comme dans le SE Solaris, l'utilisateur `root` peut se connecter à distance à partir d'un système étiqueté lorsque l'entrée `CONSOLE` est désactivée.

Si vous prévoyez d'administrer un système distant en modifiant les fichiers locaux, utilisez cette procédure.

1 **Dans l'éditeur de confiance, commentez la ligne `CONSOLE=` du fichier `/etc/default/login`.**

```
# /usr/dt/bin/trusted_edit /etc/default/login
```

La ligne modifiée se présente de la manière suivante :

```
#CONSOLE=/dev/console
```

2 **Autorisez la connexion de l'utilisateur `root` sur une connexion `ssh`.**

Modifiez le fichier `/etc/ssh/sshd_config`. Par défaut, `ssh` est activé sur les systèmes Solaris.

```
# /usr/dt/bin/trusted_edit /etc/ssh/sshd_config
```

La ligne modifiée se présente de la manière suivante :

```
PermitRootLogin yes
```

Étapes suivantes Pour vous connecter en tant qu'utilisateur `root` à partir d'un système sans étiquette, vous devez également exécuter la tâche "Activation de la connexion à distance à partir d'un système sans étiquette" à la page 143.

Pour activer la connexion à distance via un rôle, continuez en exécutant la tâche "Activation de la connexion à distance par un rôle dans Trusted Extensions" à la page 141.

▼ Activation de la connexion à distance par un rôle dans Trusted Extensions

Suivez cette procédure *uniquement* si vous devez administrer un écouteur en utilisant la commande `rlogin` ou `ssh`.

Des erreurs de configuration peuvent être déboguées à distance.

Avant de commencer Si vous utilisez des fichiers locaux pour administrer le système distant, vous avez terminé la tâche "Activation de la connexion à distance par l'utilisateur `root` dans Trusted Extensions" à la page 141. Exécutez ensuite cette tâche sur les deux systèmes en tant qu'utilisateur `root`.

1. **Sur les deux systèmes, identifiez l'autre système en tant que système étiqueté.**

   L'ordinateur de bureau et l'écouteur doivent s'identifier l'un l'autre comme utilisant le même modèle de sécurité. Pour connaître la procédure, reportez-vous à la section "Procédure d'assignation d'un modèle de sécurité à un hôte ou à un groupe d'hôtes" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

   Pour affecter une étiquette temporaire, reportez-vous à l'Exemple 6–1.

2. **Sur les deux systèmes, créez des utilisateurs et rôles identiques.**

   Les noms et les ID doivent être identiques, et le rôle doit être affecté à l'utilisateur sur les deux systèmes. Pour créer des utilisateurs et des rôles, reportez-vous à la tâche "Création de rôles et d'utilisateurs dans Trusted Extensions" à la page 92.

3. **Pour contacter une Console de gestion Solaris distante, effectuez les opérations suivantes sur les deux systèmes :**

   a. **Ajoutez le nom d'hôte et l'adresse IP de l'autre système au fichier `/etc/hosts`.**

      ```
      # /usr/dt/bin/trusted_edit /etc/hosts

      127.0.0.1    localhost
      192.168.66.66    local-system-name    loghost
      192.168.66.12    remote-system-name
      ```

   b. **Pour autoriser un utilisateur à assumer un rôle distant, modifiez le fichier `pam.conf` afin d'assouplir la stratégie PAM.**

      i. **Copiez le fichier `/etc/pam.conf` dans `/etc/pam.conf.orig`.**

         ```
         # cp /etc/pam.conf /etc/pam.conf.orig
         ```

      ii. **Dans l'éditeur de confiance, ouvrez le fichier `pam.conf`.**

         ```
         # /usr/dt/bin/trusted_edit /etc/pam.conf
         ```

      iii. **Copiez les entrées par défaut sous Gestion des comptes.**

      iv. **Dans chaque entrée copiée, modifiez `other` en `smcconsole`.**

      v. **Dans l'entrée `pam_roles.so.1` copiée, ajoutez `allow_remote`.**

         Utilisez la touche de tabulation pour naviguer entre les champs. Cette section est maintenant semblable à la suivante :

         ```
         # Solaris Management Console definition for Account management
         #
         smcconsole   account requisite   pam_roles.so.1   allow_remote
         smcconsole   account required    pam_unix_account.so.1
         smcconsole   account required    pam_tsol_account.so.1

         # Default definition for Account management
         ```

```
# Used when service name is not explicitly mentioned for account management
#
other   account requisite    pam_roles.so.1
other   account required     pam_unix_account.so.1
other   account required     pam_tsol_account.so.1
```

vi. **Enregistrez le fichier et quittez l'éditeur.**

vii. **(Facultatif) Copiez le fichier sous `/etc/pam.conf.site`.**

```
# cp /etc/pam.conf /etc/pam.conf.site
```

Si vous effectuez une mise à niveau du système vers une version plus récente, vous devez alors évaluer s'il est nécessaire de copier les modifications de `/etc/pam.conf.site` dans le fichier `pam.conf`.

Exemple 6–1 Création d'une définition temporaire de type d'hôte Trusted Extensions

Dans cet exemple, l'administrateur souhaite commencer à configurer un système Trusted Extensions distant avant que les définitions de type d'hôte ne soient configurées. Pour ce faire, l'administrateur utilise la commande `tnctl` sur le système distant pour temporairement définir le type d'hôte de l'ordinateur de bureau :

```
remote-TX# tnctl -h desktop-TX:cipso
```

Par la suite, l'administrateur souhaite accéder au système Trusted Extensions distant à partir d'un ordinateur de bureau qui n'est pas configuré avec Trusted Extensions. Dans ce cas, l'administrateur utilise la commande `tnctl` sur le système distant pour temporairement définir le type d'hôte de l'ordinateur de bureau en tant que système sans étiquette qui s'exécute à l'étiquette `ADMIN_LOW` :

```
remote-TX# tnctl -h desktop-TX:admin_low
```

▼ Activation de la connexion à distance à partir d'un système sans étiquette

Avant de commencer

Cette procédure n'est pas sécurisée.

Vous avez assoupli votre stratégie PAM afin d'autoriser un utilisateur à assumer un rôle distant, comme décrit à la section "Activation de la connexion à distance par un rôle dans Trusted Extensions" à la page 141.

1 **Sur le système de confiance, appliquez le modèle de sécurité approprié au système sans étiquette.**

Attention – Avec les paramètres par défaut, un autre système sans étiquette peut se connecter et administrer le système distant. Par conséquent, vous devez modifier la valeur par défaut du réseau `0.0.0.0` de `ADMIN_LOW` en une étiquette différente. Pour connaître la procédure, reportez-vous à la section "Procédure de limitation des hôtes pouvant être contactés sur le réseau de confiance" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

2 **Dans l'éditeur de confiance, ouvrez le fichier `/etc/pam.conf`.**

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

3 **Recherchez les entrées `smcconsole`.**

4 **Ajoutez `allow_unlabeled` au module `tsol_account`.**

Utilisez la touche de tabulation pour naviguer entre les champs.

```
smcconsole   account required  pam_tsol_account.so.1 allow_unlabeled
```

Une fois les modifications apportées, cette section s'affiche comme suit :

```
# Solaris Management Console definition for Account management
#
smcconsole  account  requisite      pam_roles.so.1    allow_remote
smcconsole  account  required       pam_unix_account.so.1
smcconsole  account  required       pam_tsol_account.so.1 allow_unlabeled
```

▼ Utilisation d'une Console de gestion Solaris à distance pour administrer dans l'étendue fichiers

Si vous n'utilisez pas LDAP et si vous souhaitez utiliser la Console de gestion Solaris sur un système distant, activez la connexion à distance à la console. Cette procédure n'est cependant pas suffisante pour permettre l'accès pour l'étendue LDAP.

Pour activer l'accès pour l'étendue LDAP, vous devez d'abord terminer toutes les procédures de la section "Configuration de la Console de gestion Solaris pour LDAP (liste des tâches)" à la page 132.

Avant de commencer

Les deux systèmes sont étiquetés.

Vous avez effectué les procédures suivantes :

- "Initialisation du serveur Console de gestion Solaris dans Trusted Extensions" à la page 61
- "Activation de la connexion à distance par un rôle dans Trusted Extensions" à la page 141

1 **Exécutez la tâche "Activation de la Console de gestion Solaris afin qu'elle accepte les communications réseau" à la page 134.**

2 **Sur l'ordinateur de bureau, devenez un utilisateur défini à l'identique sur les deux systèmes.**

3 **Sur l'ordinateur de bureau, assumez le rôle défini à l'identique sur les deux systèmes.**

4 **Sur l'ordinateur de bureau, lancez la Console de gestion Solaris.**

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

5 **Dans la boîte de dialogue Server (Serveur), saisissez le nom de l'écouteur.**

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

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

▼ Activation de l'affichage à distance des interfaces graphiques d'administration

La procédure d'affichage à distance sur un ordinateur de bureau est identique à la procédure pour un système Solaris qui n'est pas configuré avec Trusted Extensions. Cette procédure est décrite ici pour plus de commodité.

1 **Sur l'ordinateur de bureau, activez les processus à partir de l'écouteur à afficher.**

a. **Autorisez l'écouteur à accéder au serveur X sur l'ordinateur de bureau.**

```
desktop $ xhost + headless-host
```

b. **Déterminez la valeur de la variable `DISPLAY` de l'ordinateur de bureau.**

```
desktop $ echo $DISPLAY
:n.n
```

2 **Sur l'écouteur, définissez la variable `DISPLAY` sur l'ordinateur de bureau.**

```
headless $ DISPLAY=desktop:n.n
headless $ export DISPLAY=n:n
```

▼ Utilisation de la commande `rlogin` ou `ssh` pour se connecter à un écouteur dans Trusted Extensions et l'administrer

Cette procédure vous permet d'utiliser la ligne de commande et l'interface graphique `txzonemgr` pour administrer un écouteur en tant que superutilisateur ou en tant que rôle.

Remarque – La connexion à distance à l'aide de la commande `rlogin` est moins sûre que la connexion à distance à l'aide de la commande `ssh`.

L'utilisation de la Console de gestion Solaris pour administrer un système distant ne requiert pas d'utiliser une commande de connexion à distance. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure d'administration à distance des systèmes à l'aide de la Console de gestion Solaris dans un système Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Avant de commencer Vous avez terminé les tâches de la section "Activation de la connexion à distance par un rôle dans Trusted Extensions" à la page 141.

Vous êtes un utilisateur autorisé à se connecter à l'écouteur avec le même nom d'utilisateur et le même ID, et vous pouvez assumer le même rôle sur l'écouteur que celui que vous assumez sur l'ordinateur de bureau.

1 Sur l'ordinateur de bureau, activez les processus à partir de l'écouteur à afficher.

```
desktop $ xhost + headless-host
desktop $ echo $DISPLAY
:n.n
```

2 Assurez-vous que vous êtes l'utilisateur défini à l'identique sur les deux systèmes.

3 À partir d'une fenêtre de terminal, connectez-vous à distance à l'écouteur.

- **Utilisez la commande `ssh` pour vous connecter :**

```
desktop $ ssh -l identical-username headless
Password:       Type the user's password
headless $
```

- **Ou utilisez la commande `rlogin` pour vous connecter :**

```
desktop # rlogin headless
Password:       Type the user's password
headless $
```

4 Assumez le rôle défini à l'identique sur les deux systèmes.

Utilisez la même fenêtre de terminal. Par exemple, assumez le rôle `root`.

```
headless $ su - root
Password:       Type the root password
```

Vous êtes à présent dans la zone globale. Vous pouvez maintenant utiliser ce terminal pour administrer l'écouteur à partir de la ligne de commande.

5 Activez les processus de l'écouteur à afficher sur l'ordinateur de bureau.

Remarque – Vous pouvez aussi afficher les interfaces graphiques à distance en vous connectant avec la commande `ssh -X`. Pour plus d'informations, reportez-vous à la page de manuel `ssh(1)`. Reportez-vous à l'Exemple 6–2.

```
headless $  DISPLAY desktop:n.n
headless $ export DISPLAY=n:n
```

Vous pouvez désormais administrer l'écouteur en utilisant les interfaces graphiques Trusted Extensions. Par exemple, lancez l'interface graphique `txzonemgr` :

```
headless $ /usr/sbin/txzonemgr
```

Le gestionnaire de zones étiquetées (Labeled Zone Manager) s'exécute sur le système distant et s'affiche sur l'ordinateur de bureau.

6 (Facultatif) Accédez aux actions Trusted CDE.

Pour ouvrir et fermer le gestionnaire d'applications en toute sécurité, reportez-vous à la section "Procédure d'administration à distance de Trusted Extensions avec dtappsession" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Exemple 6–2 Configuration des zones étiquetées sur un écouteur

Dans cet exemple, l'administrateur utilise l'interface graphique `txzonemgr` pour configurer des zones étiquetées sur un écouteur étiqueté à partir d'un ordinateur de bureau étiqueté. Comme dans le SE Solaris, l'administrateur autorise le serveur X à accéder à l'ordinateur de bureau à l'aide de l'option `-X` de la commande `ssh`. L'utilisateur `install1` est défini à l'identique sur les deux systèmes et peut prendre le rôle `remoterole`.

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
install1

TXdesk1 $ ssh -X -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

Pour atteindre la zone globale, l'administrateur prend le rôle `remoterole`. Ce rôle est défini à l'identique sur les deux systèmes.

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

L'administrateur démarre ensuite l'interface graphique `txzonemgr`.

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Le gestionnaire de zones étiquetées (Labeled Zone Manager) s'exécute sur l'écouteur et s'affiche sur l'ordinateur de bureau.

◆ ◆ ◆ 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 :

- "Stratégie de sécurité du site et Trusted Extensions" à la page 150
- "Recommandations relatives à la sécurité informatique" à la page 151
- "Recommandations relatives à la sécurité physique" à la page 152
- "Recommandations relatives à la sécurité du personnel" à la page 153
- "Violations de sécurité courantes" à la page 153
- "Références de sécurité supplémentaires" à la page 154

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 de contrôle 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 redémarrages 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 de contrôle. 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 supports de stockage amovibles pour les informations sensibles. Verrouillez tous les supports 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 supports 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 supports 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 supports 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

Utilisation d'actions CDE pour installer des zones dans Trusted Extensions

Cette annexe présente la configuration de zones étiquetées dans Trusted Extensions à l'aide d'actions Trusted CDE. Si vous exécutez la version Solaris 10 11/06 sans patch ou si vous êtes familier de ces actions, utilisez les actions Trusted CDE. Pour utiliser le script `txzonemgr`, reportez-vous à la section "Création de zones étiquetées" à la page 68.

- "Association d'interfaces réseau avec des zones à l'aide d'actions CDE (liste des tâches)" à la page 157
- "Préparation de la création de zones à l'aide d'actions CDE (liste des tâches)" à la page 160
- "Création de zones étiquetées à l'aide d'actions CDE (liste des tâches)" à la page 163

Association d'interfaces réseau avec des zones à l'aide d'actions CDE (liste des tâches)

Exécutez uniquement l'une des tâches ci-dessous. Pour les compromis, reportez-vous à la section "Planification pour l'accès multiniveau" à la page 26.

Tâche	Description	Voir
Partage d'une interface logique.	Mappez la zone globale à une adresse IP et mappez des zones étiquetées à une autre adresse IP.	"Spécification de deux adresses IP pour le système à l'aide d'une action CDE" à la page 158
Partage d'une interface physique.	Mappez toutes les zones à une adresse IP.	"Spécification d'une adresse IP pour le système à l'aide d'une action CDE" à la page 159

▼ Spécification de deux adresses IP pour le système à l'aide d'une action CDE

Dans cette configuration, l'adresse de l'hôte s'applique uniquement à la zone globale. Les zones étiquetées partagent une seconde adresse IP avec la zone globale.

Avant de commencer Vous êtes superutilisateur dans la zone globale. Deux adresses IP ont déjà été affectées au système. Vous vous trouvez dans un espace de travail Trusted CDE.

1 Accédez au dossier Trusted_Extensions.

a. Avec la souris, cliquez sur le bouton 3 sur l'arrière-plan.

b. Dans le menu Workspace (Espace de travail), sélectionnez Applications → Application Manager (Applications → Gestionnaire d'applications).

c. Double-cliquez sur l'icône du dossier Trusted_Extensions.

Ce dossier contient des actions qui définissent les interfaces, les clients LDAP et les zones étiquetées.

2 Double-cliquez sur l'action Share Logical Interface (Partager l'interface logique) et répondez aux invites.

Remarque – Deux adresses IP doivent déjà avoir été affectées au système. Pour cette action, fournissez la deuxième adresse et un nom d'hôte correspondant à cette adresse. La seconde adresse est l'adresse partagée.

```
Hostname:       Type the name for your labeled zones interface
IP Address:     Type the IP address for the interface
```

Cette action permet de configurer un hôte avec plusieurs adresses IP. L'adresse IP de la zone globale est le nom de l'hôte. L'adresse IP d'une zone étiquetée a un nom d'hôte différent. En outre, l'adresse IP pour les zones étiquetées est partagée avec la zone globale. Lorsque cette configuration est utilisée, les zones étiquetées sont en mesure d'atteindre une imprimante réseau.

Astuce – Utilisez une convention de nommage standard pour les zones étiquetées. Par exemple, ajoutez `-zones` au nom d'hôte.

---

3 (Facultatif) Dans une fenêtre de terminal, vérifiez les résultats de l'action.

```
# ifconfig -a
```

Par exemple, la sortie suivante montre une interface logique partagée, `hme0:3`, sur l'interface réseau `192.168.0.12` pour les zones étiquetées. L'interface `hme0` est l'adresse IP unique de la zone globale.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.12 netmask fffffe00 broadcast 192.168.0.255
```

À partir de la version Solaris 10 10/08, l'interface de loopback, `lo0`, est également une interface `all-zones` :

```
 lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
...
```

▼ Spécification d'une adresse IP pour le système à l'aide d'une action CDE

Dans cette configuration, l'adresse de l'hôte s'applique à toutes les zones, y compris les zones étiquetées.

Avant de commencer Vous êtes superutilisateur dans la zone globale. Vous vous trouvez dans un espace de travail Trusted CDE.

1 Accédez au dossier Trusted_Extensions.

a. Avec la souris, cliquez sur le bouton 3 sur l'arrière-plan.

b. Dans le menu Workspace (Espace de travail), sélectionnez Applications → Application Manager (Applications → Gestionnaire d'applications).

c. Double-cliquez sur l'icône du dossier Trusted_Extensions.

Ce dossier contient des actions qui définissent les interfaces, les clients LDAP et les zones étiquetées.

2 Double-cliquez sur l'action Share Physical Interface (Partager l'interface physique).

Cette action permet de configurer un hôte avec une adresse IP. La zone globale n'a pas d'adresse unique. Ce système ne peut pas être utilisé comme serveur d'impression multiniveau ou serveur NFS.

3 **(Facultatif) Dans une fenêtre de terminal, vérifiez les résultats de l'action.**

```
# ifconfig -a
```

L'action Share Physical Interface (Partager l'interface physique) permet de configurer toutes les zones pour qu'elles aient des cartes d'interface réseau (NIC) logiques. Ces NIC logiques partagent une seule NIC physique dans la zone globale.

Par exemple, la sortie suivante montre l'interface physique partagée, `hme0`, sur l'interface réseau `192.168.0.11` pour toutes les zones.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
       all-zones
       inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

À partir de la version Solaris 10 10/08, l'interface de loopback, `lo0`, est également une interface `all-zones` :

```
  lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         all-zones
         inet 127.0.0.1 netmask ff000000
         ether 0:0:00:00:00:0
...
```

Préparation de la création de zones à l'aide d'actions CDE (liste des tâches)

La liste des tâches ci-dessous décrit les tâches de préparation du système pour la création d'une zone. Pour une description des méthodes de création de zones, reportez-vous à la section "Planification de zones dans Trusted Extensions" à la page 24.

Tâche	Description	Voir
1. Attribution d'un nom à chaque zone et liaison du nom de zone avec l'étiquette de zone.	Attribuez à chaque zone étiquetée un nom rappelant son étiquette, puis associez le nom à l'étiquette dans la Console de gestion Solaris.	"Spécification des noms et étiquettes de zone à l'aide d'une action CDE" à la page 161
2. Configuration du réseau avant la création de zones.	Affectez une étiquette à l'interface réseau sur chaque hôte et effectuez une configuration avancée.	"Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

▼ Spécification des noms et étiquettes de zone à l'aide d'une action CDE

Vous n'êtes pas obligé de créer une zone pour chaque étiquette de votre fichier `label_encodings`, mais vous pouvez le faire. La base de données `tnzonecfg` répertorie les étiquettes pour lesquelles des zones peuvent être créées sur ce système.

1 Accédez au dossier Trusted_Extensions.

a. Avec la souris, cliquez sur le bouton 3 sur l'arrière-plan.

b. Dans le menu Workspace (Espace de travail), sélectionnez Applications → Application Manager (Applications → Gestionnaire d'applications).

c. Double-cliquez sur l'icône du dossier Trusted_Extensions.

2 Attribuez un nom à chaque zone.

a. Double-cliquez sur l'action Configure Zone (Configurer la zone).

b. À l'invite, saisissez un nom.

Astuce – Attribuez à la zone un nom similaire à l'étiquette de zone. Par exemple, le nom d'une zone dont l'étiquette est `CONFIDENTIAL : INTERNAL USE ONLY` serait `internal`.

---

3 Répétez l'action Configure Zone (Configurer la zone) pour chaque zone.

Par exemple, le fichier `label_encodings` par défaut contient les étiquettes suivantes :

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

Bien que vous puissiez exécuter l'action Configure Zone (Configurer la zone) six fois pour créer une zone par étiquette, vous pouvez envisager de créer les zones suivantes :

- Sur un système destiné à tous les utilisateurs, créez une zone pour l'étiquette `PUBLIC` et trois zones pour les étiquettes `CONFIDENTIAL`.
- Sur un système destiné aux développeurs, créez une zone pour l'étiquette `SANDBOX: PLAYGROUND`. L'étiquette `SANDBOX: PLAYGROUND` est définie en tant qu'étiquette disjointe pour les développeurs, de sorte que seuls les systèmes utilisés par les développeurs ont besoin d'une zone pour cette étiquette.
- Ne créez pas de zone pour l'étiquette `MAX LABEL`, qui est définie pour être une autorisation.

4 Ouvrez l'outil Trusted Network Zones.

Les outils de la Console de gestion Solaris sont conçus pour éviter toute erreur de la part de l'utilisateur. Ces outils vérifient la présence d'erreurs de syntaxe et exécutent automatiquement les commandes dans l'ordre approprié afin de mettre à jour les bases de données.

a. Lancez la Console de gestion Solaris.

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

b. Ouvrez la boîte à outils Trusted Extensions pour le système local.

i. Choisissez Console → Open Toolbox (Console → Ouvrir la boîte à outils).

ii. Sélectionnez la boîte à outils nommée Cet ordinateur (*this-host* : `Scope=Files, Policy=TSOL`).

iii. Cliquez sur Open (Ouvrir).

c. Sous System Configuration (Configuration système), accédez à Computers and Networks (Ordinateurs et réseaux).

À l'invite, saisissez un mot de passe.

d. Double-cliquez sur l'outil Trusted Network Zones.

5 Pour chaque zone, associez l'étiquette appropriée à un nom de zone.

a. Choisissez Action → Add Zone Configuration (Action → Ajouter la configuration de zone).

La boîte de dialogue affiche le nom d'une zone à laquelle aucune étiquette n'a été assignée.

b. Vérifiez le nom de zone, puis cliquez sur Edit (Modifier).

c. Dans le générateur d'étiquettes (Label Builder), cliquez sur l'étiquette appropriée pour le nom de zone.

Si vous sélectionnez la mauvaise étiquette, cliquez de nouveau sur l'étiquette pour la désélectionner, puis cliquez sur l'étiquette appropriée.

d. Enregistrez l'allocation.

Cliquez sur OK dans le générateur d'étiquettes, puis cliquez sur OK dans la boîte de dialogue Trusted Network Zones Properties (Propriétés des zones Trusted Network).

Vous avez terminé lorsque toutes les zones de votre choix sont répertoriées dans le panneau ou lorsque l'option de menu Add Zone Configuration (Ajouter la configuration de zone) ouvre une boîte de dialogue ne contenant aucune valeur pour le nom de zone (Zone Name).

Erreurs fréquentes

Si la boîte de dialogue Trusted Network Zones Properties (Propriétés des zones de réseau de confiance) ne demande pas la zone que vous souhaitez créer, le fichier de configuration du réseau de zone n'existe pas ou vous l'avez déjà créé.

- Vérifiez que le fichier de configuration du réseau de zone n'existe pas déjà. Recherchez son nom dans le panneau.
- Si le fichier n'existe pas, exécutez l'action Configure Zone (Configurer la zone) pour indiquer le nom de la zone. Ensuite, répétez l'Étape 5 pour créer le fichier.

Création de zones étiquetées à l'aide d'actions CDE (liste des tâches)

Il est possible de créer une zone pour chaque entrée de la base de données Trusted Network Zone Configuration (Configuration de zones de réseau de confiance). Vous avez créé les entrées à l'étape "Spécification des noms et étiquettes de zone à l'aide d'une action CDE" à la page 161, en exécutant l'action Configure Zone (Configurer la zone).

Le dossier Trusted_Extensions du gestionnaire d'applications contient les actions suivantes qui créent des zones étiquetées :

- Configure Zone (Configurer la zone) : crée un fichier de configuration de zone pour chaque nom de la zone.
- Install Zone (Installer la zone) : ajoute les systèmes de fichiers et packages corrects à la zone.
- Zone Terminal Console (Console de terminal de zone) : fournit une fenêtre de visualisation d'événements dans une zone.
- Initialize Zone for LDAP (Initialiser la zone pour LDAP) : fait de la zone un client LDAP et prépare la zone pour l'initialisation.
- Start Zone (Démarrer la zone) : initialise la zone, puis démarre tous les services SMF (Service Management Framework, utilitaire de gestion de services).
- Shut Down Zone (Arrêter la zone) : modifie l'état de la zone de Started (Démarré) en Halted (Arrêté).

Les tâches sont exécutées dans l'ordre suivant.

Tâche	Description	Voir
1. Installation et initialisation d'une zone.	Créez la première zone étiquetée. Installez des packages, définissez la zone en client LDAP et démarrez tous les services dans la zone.	"Installation, initialisation et démarrage d'une zone étiquetée à l'aide d'actions CDE" à la page 164
2. Personnalisation de la zone.	Supprimez les services non souhaités. Si vous prévoyez de copier ou cloner la zone, supprimez les informations spécifiques à la zone.	"Personnalisation d'une zone initialisée dans Trusted Extensions" à la page 168

Tâche	Description	Voir
3. Création d'autres zones.	Utilisez l'une des méthodes suivantes pour créer les autres zones. Vous avez sélectionné la méthode à la section "Prise de décisions relatives au système et à la sécurité avant l'activation de Trusted Extensions" à la page 47.	
	Créez chaque zone à partir de zéro.	"Installation, initialisation et démarrage d'une zone étiquetée à l'aide d'actions CDE" à la page 164 "Résolution de l'acheminement zone locale-zone globale dans Trusted CDE" à la page 167 "Personnalisation d'une zone initialisée dans Trusted Extensions" à la page 168
	Copiez la première zone étiquetée vers une autre étiquette. Répétez l'opération pour toutes les zones.	"Utilisation de la méthode de copie de zone dans Trusted Extensions" à la page 170
	Utilisez un instantané ZFS pour cloner les autres zones à partir de la première zone étiquetée.	"Utilisation de la méthode de clonage de zone dans Trusted Extensions" à la page 171

▼ Installation, initialisation et démarrage d'une zone étiquetée à l'aide d'actions CDE

La création d'une zone implique la copie d'un système d'exploitation complet, si bien que ce processus prend du temps. Un processus plus rapide consiste à créer une zone, en faire un modèle pour les autres zones, puis à copier ou cloner ce modèle de zone.

Avant de commencer

Vous avez terminé les tâches de la section "Spécification des noms et étiquettes de zone à l'aide d'une action CDE" à la page 161.

Si vous utilisez le protocole LDAP en tant que service de nommage, vous avez terminé les tâches de la section "Établissement de la zone globale en tant que client LDAP dans Trusted Extensions" à la page 64.

Si vous avez l'intention de cloner des zones, vous avez terminé les tâches de la section "Création d'un pool ZFS pour le clonage des zones" à la page 58. Au cours de la procédure ci-dessous, vous allez installer la zone que vous avez préparée.

1 Dans le dossier Trusted_Extensions, double-cliquez sur l'action Install Zone (Installer la zone).

a. Saisissez le nom de la zone que vous êtes en train d'installer.

Cette action crée un système d'exploitation virtuel étiqueté. Cette étape prend un certain temps. N'effectuez pas d'autre tâche sur le système pendant que l'action d'installation de la zone s'exécute.

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

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

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

b. Ouvrez une console pour contrôler les événements dans la zone installée.

i. Double-cliquez sur l'action Zone Terminal Console (Console de terminal de zone).

ii. Saisissez le nom de la zone qui vient d'être installée.

2 Initialisez la zone.

- **Si vous utilisez LDAP, double-cliquez sur l'action Initialize Zone for LDAP (Initialiser la zone pour LDAP).**

```
Zone name:                  Type the name of the installed zone
Host name for the zone:     Type the host name for this zone
```

Par exemple, sur un système disposant d'une interface logique partagée, les valeurs doivent être similaires aux suivantes :

```
Zone name:              public
Host name for the zone: machine1-zones
```

Cette action fait de la zone étiquetée un client LDAP du même serveur LDAP qui sert la zone globale. L'action est terminée lorsque les informations suivantes s'affichent :

```
zone-name zone will be  LDAP client of IP-address
zone-name is ready for booting
Zone label is LABEL

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

- **Si vous n'utilisez pas LDAP, initialisez la zone manuellement en effectuant l'une des étapes suivantes.**

  La procédure manuelle dans Trusted Extensions est identique à la procédure pour le SE Solaris. Si le système dispose d'au moins une interface `all-zones`, le nom de l'hôte pour toutes les zones doit correspondre au nom d'hôte de la zone globale. En général, les réponses aux questions pendant l'initialisation de la zone sont les mêmes que les réponses pour la zone globale.

  Fournissez les informations relatives à l'hôte en utilisant l'une des méthodes suivantes :

  - **Après avoir démarré la zone à l'Étape 3, répondez aux questions relatives aux caractéristiques du système dans la console de terminal de zone.**

    Vos réponses sont utilisées pour remplir le fichier `sysidcfg` dans la zone.

    Remarque – Vous devez vous assurer qu'un chemin d'accès au bureau Trusted CDE existe entre la zone étiquetée et la zone globale. Pour plus d'informations sur cette procédure, reportez-vous à la section "Résolution de l'acheminement zone locale-zone globale dans Trusted CDE" à la page 167.

  - **Placez un fichier `sysidcfg` personnalisé dans le répertoire `/etc` de la zone avant l'initialisation de la zone à l'Étape 3.**

3 **Double-cliquez sur l'action Start Zone (Démarrer la zone).**

Répondez à l'invite.

`Zone name:` *Type the name of the zone that you are configuring*

Cette action initialise la zone, puis démarre tous les services qui s'exécutent dans la zone. Pour plus d'informations sur ces services, reportez-vous à la page de manuel `smf(5)`.

La console de terminal de zone suit l'avancement de l'initialisation de la zone. Des messages semblables à celui-ci s'affichent sur la console :

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

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

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

[NOTICE: Zone rebooting]
```

4 Contrôlez la sortie de la console.

Avant de poursuivre avec l'étape "Personnalisation d'une zone initialisée dans Trusted Extensions" à la page 168, assurez-vous que la zone a été réinitialisée. L'invite de connexion de la console ci-après indique que la zone a été réinitialisée.

hostname `console login:`

Erreurs fréquentes Pour l'action Install Zone (Installer la zone) : si des avertissements similaires au suivant s'affichent : `Installation of these packages generated errors: SUNW`*pkgname*, consultez le journal d'installation et terminez l'installation des packages.

▼ Résolution de l'acheminement zone locale-zone globale dans Trusted CDE

Pour que toutes les zones puissent accéder à Trusted CDE, la variable `DISPLAY` doit être résolue. Dans Trusted CDE, pour résoudre la variable, le nom de nœud de la zone étiquetée, le nom de nœud de la zone globale et le nom de nœud d'une interface all-zones doivent être résolus avec le même nom.

Avant de commencer Vous utilisez Trusted CDE et initialisez manuellement une zone étiquetée.

1 Activez Trusted CDE pour afficher l'étiquette d'une zone à l'aide de l'une des méthodes suivantes.

- **Méthode 1 : Activez le trafic du serveur X avec d'autres systèmes.**

  Dans cette configuration, les zones étiquetées peuvent atteindre d'autres systèmes par l'intermédiaire du serveur X dans la zone globale.

  a. **Assurez-vous que le fichier `/etc/nodename` spécifie le nom du système.**

  ```
  ## /etc/nodename
  machine1
  ```

  b. **Assurez-vous que le fichier `/etc/hosts` spécifie le nom du système.**

  ```
  ## /etc/hosts
  192.168.2.3  machine1 loghost
  ```

  Pour que les services ToolTalk fonctionnent, le nom du système doit se trouver sur la même ligne que `loghost`.

  c. **Assurez-vous que le fichier `/etc/hostname.`*interface* spécifie le nom du système.**

  Dans cette configuration, `machine1` est l'interface all-zones pour Trusted CDE.

  ```
  ## /etc/hostname.bge0
  machine1 all-zones
  ```

- **Méthode 2 : Limitez le trafic du serveur X vers le système local.**

  Dans cette configuration, les zones étiquetées peuvent communiquer avec le serveur X sur le système local. Cependant, aucun acheminement n'existe du serveur X local vers d'autres systèmes sur le réseau. L'acheminement doit utiliser une autre interface.

  a. **Assurez-vous que le fichier `/etc/nodename` spécifie le nom du système.**

     ```
     ## /etc/nodename
     machine1
     ```

  b. **Assurez-vous que le fichier `/etc/hosts` spécifie le nom du système.**

     À partir de la version Solaris 10 10/08, `lo0` est une interface all-zones. Dans ce cas, le fichier est semblable à ce qui suit :

     ```
     ## /etc/hosts
     127.0.0.1  localhost  machine1 loghost
     ```

     Vous pouvez également utiliser l'interface `vni0`.

     Pour que les services ToolTalk fonctionnent, le nom du système doit se trouver sur la même ligne que `loghost`.

- **Méthode 3 : Résolvez la variable `DISPLAY` d'une autre manière, via les adresses routables sur les interfaces logiques par zone par exemple.**

  Pour en savoir plus sur cette procédure, reportez-vous à la section "Ajout d'interfaces réseau et acheminement vers les zones étiquetées" à la page 84.

2 **Pour initialiser la zone, revenez à l'Étape 3 de la section "Installation, initialisation et démarrage d'une zone étiquetée à l'aide d'actions CDE" à la page 164.**

▼ Personnalisation d'une zone initialisée dans Trusted Extensions

Si vous avez l'intention de cloner des zones, cette procédure permet de configurer une zone en tant que modèle pour d'autres zones. En outre, cette procédure permet de configurer la zone pour son utilisation.

1 **Assurez-vous que la zone a été complètement démarrée.**

a. **Dans la console de terminal de zone *zone-name*, connectez-vous en tant que root.**

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

b. Vérifiez que la zone est en cours d'exécution.

L'état `running` indique qu'au moins un processus est en cours d'exécution dans la zone.

```
# zoneadm list -v
ID NAME        STATUS         PATH
 2 public      running        /
```

c. Vérifiez que la zone peut communiquer avec la zone globale.

Le serveur X est exécuté dans la zone globale. Chaque zone étiquetée doit être en mesure de se connecter à la zone globale pour utiliser ce service. Par conséquent, la mise en réseau des zones doit fonctionner avant de pouvoir utiliser la zone. Pour obtenir de l'aide, reportez-vous à la section "La zone étiquetée ne peut accéder au serveur X" à la page 111.

2 Dans la console de terminal de zone, désactivez les services inutiles dans une zone étiquetée.

Si vous copiez ou clonez cette zone, les services que vous désactivez sont désactivés dans les nouvelles zones. Les services en ligne sur votre système dépendent du fichier manifest du service pour la zone. Utilisez la commande `netservices limited` pour désactiver les services dont les zones étiquetées n'ont pas besoin.

a. Supprimez les nombreux services inutiles.

```
# netservices limited
```

b. Répertoriez les services restants.

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

c. Désactivez la connexion graphique.

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

Pour en savoir plus sur l'utilitaire de gestion des services, reportez-vous à la page de manuel `smf(5)`.

3 Arrêtez la zone.

Vous avez le choix entre les options suivantes :

- **Exécutez l'action Shut Down Zone (Arrêter la zone).**

  Indiquez le nom de la zone.

- **Dans une fenêtre de terminal dans la zone globale, utilisez la commande `zlogin`.**

  ```
  # zlogin zone-name init 0
  ```

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

4 **Vérifiez que la zone est arrêtée.**

Dans la console de terminal de zone *zone-name*, le message suivant indique que la zone est arrêtée :

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

Si vous ne copiez ou ne clonez pas cette zone, créez les zones restantes de la même manière que vous avez créé cette première zone.

5 **Si vous utilisez cette zone comme modèle pour d'autres zones, effectuez les opérations suivantes :**

a. **Supprimez le fichier `auto_home_`*zone-name*.**

Dans une fenêtre de terminal dans la zone globale, supprimez ce fichier à partir de la zone *zone-name*.

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

Par exemple, si la zone `public` était la base pour le clonage d'autres zones, supprimez son fichier `auto_home` :

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

Étapes suivantes

- Si vous copiez une zone, reportez-vous à la section "Utilisation de la méthode de copie de zone dans Trusted Extensions" à la page 170.
- Si vous clonez une zone, reportez-vous à la section "Utilisation de la méthode de clonage de zone dans Trusted Extensions" à la page 171.

▼ Utilisation de la méthode de copie de zone dans Trusted Extensions

Avant de commencer

- Vous avez terminé les tâches de la section "Spécification des noms et étiquettes de zone à l'aide d'une action CDE" à la page 161.
- Vous avez personnalisé une zone qui est le modèle pour le clonage à l'étape "Création de zones étiquetées à l'aide d'actions CDE (liste des tâches)" à la page 163.
- Vous n'êtes pas en train d'exécuter la zone qui est votre modèle pour le clonage.
- Le dossier Trusted_Extensions est affiché.

1. **Pour chaque zone que vous voulez créer, double-cliquez sur l'action Copy Zone (Copier la zone).**

   Répondez aux invites.

   `New Zone Name:` *Type name of target zone*
   `From Zone Name:` *Type name of source zone*

Attention – N'exécutez aucune autre tâche tant que celle-ci n'est pas terminée.

2. **Une fois les zones créées, vérifiez l'état de chacune.**

   a. **Double-cliquez sur l'action Zone Terminal Console (Console de terminal de zone).**

   b. **Connectez-vous à chaque zone.**

   c. **Exécutez le processus "Vérification de l'état de la zone" à la page 79.**

▼ Utilisation de la méthode de clonage de zone dans Trusted Extensions

Avant de commencer

- Vous avez terminé les tâches de la section "Spécification des noms et étiquettes de zone à l'aide d'une action CDE" à la page 161.
- Vous avez terminé les tâches de la section "Création d'un pool ZFS pour le clonage des zones" à la page 58.
- Vous avez créé le modèle de zone en exécutant l'étape "Création d'un pool ZFS pour le clonage des zones" à la page 58.
- Vous avez personnalisé une zone qui est votre modèle pour le clonage à l'étape "Création de zones étiquetées à l'aide d'actions CDE (liste des tâches)" à la page 163.
- La zone qui vous sert de modèle pour le clonage est arrêtée.
- Le dossier Trusted_Extensions est affiché.

1. **Créez un instantané ZFS Solaris du modèle de zone.**

```
# cd /
# zfs snapshot zone/zone-name@snapshot
```

Vous pouvez utiliser cet instantané pour cloner les zones restantes. Pour une zone configurée nommé `public`, la commande d'instantané est la suivante :

```
# zfs snapshot zone/public@snapshot
```

2 **Pour chaque zone que vous voulez créer, double-cliquez sur l'action Clone zone (Cloner la zone).**

Répondez aux invites.

```
New Zone Name:          Type name of source zone
ZFS Snapshot:             Type name of snapshot
```

3 **Lisez les informations dans la boîte de dialogue.**

```
Zone label is <LABEL>
zone-name is ready for booting

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

4 **Pour chaque zone, exécutez l'action Start Zone (Démarrer la zone).**

Démarrez chaque zone avant d'exécuter l'action pour une autre zone.

5 **Une fois les zones créées, vérifiez l'état de chacune.**

a. **Double-cliquez sur l'action Zone Terminal Console (Console de terminal de zone).**

b. **Exécutez le processus "Vérification de l'état de la zone" à la page 79.**

◆ ◆ ◆ ANNEXE C

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 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 des *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
   - Intégrez les exigences en matière de sécurité du site.
   - Lisez l'annexe "Stratégie de sécurité du site et Trusted Extensions" à la page 150.
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.
   - Déterminez la méthode de création de zone.
3. Activez Trusted Extensions.
   a. Installez le SE Oracle Solaris.
      - Pour l'administration à distance, installez le groupe Développeur ou un groupe plus grand des packages Solaris.
      - Pour la méthode de création par clonage de zone, sélectionnez Custom Install (Installation personnalisée), puis préparez une partition `/zone`.

b. Activez `svc:/system/labeld`, le service Trusted Extensions.

4. Si vous utilisez IPv6, activez IPv6 pour Trusted Extensions.
5. Si vous utilisez un DOI différent de `1`, définissez-le dans les fichiers `/etc/system` et `/etc/security/tsol/tnrhtp`.
6. (Facultatif) Créez un pool ZFS pour le clonage de zones.
7. Configurez les étiquettes.
   a. Finalisez le fichier `label_encodings` de votre site.
   b. Vérifiez et installez le fichier.
   c. Réinitialisez le système.
8. Configurez les interfaces de la zone globale et des zones étiquetées.
9. Configurez la Console de gestion Solaris.
10. Configurez le service de nommage.
    - Utilisez le service de nommage de fichiers, qui ne requiert aucune configuration.
    - Ou configurez LDAP.
      a. Créez un serveur proxy Trusted Extensions ou un serveur LDAP Trusted Extensions.
      b. Activez le serveur Console de gestion Solaris afin qu'il accepte les connexions réseau.
      c. Enregistrez la Console de gestion Solaris avec LDAP.
      d. Créez une boîte à outils LDAP pour la Console de gestion Solaris.
11. Configurez les connexions réseau pour LDAP.
    - Affectez un serveur LDAP ou un serveur proxy au type d'hôte `cipso` dans un modèle d'hôte distant.
    - Affectez le système local au type d'hôte `cipso` dans un modèle d'hôte distant.
    - Faites du système local un client du serveur LDAP.
12. Créez des zones étiquetées.
    - OPTION 1 : utilisez le script txzonemgr.
    - OPTION 2 : utilisez des actions Trusted CDE.
      a. Configurez les zones étiquetées
         i. Dans la Console de gestion Solaris, associez les noms de zones avec des étiquettes particulières.
         ii. Exécutez l'action Configure Zone (Configurer la zone).
      b. Exécutez l'action Install zone (Installer la zone).
      c. Exécuter l'action Initialize for LDAP (Initialiser pour LDAP).
      d. Exécutez l'action Start Zone (Démarrer la zone).
      e. Personnalisez la zone en cours d'exécution.
      f. Exécutez l'action Shut Down Zone (Arrêter la zone).

g. Personnalisez la zone lorsqu'elle est arrêtée.

h. (Facultatif) Créez un instantané ZFS.

i. Créez les zones restantes à partir de zéro ou à l'aide de l'action Copy Zone (Copier la zone) ou Clone Zone (Cloner la zone).

13. Configurez le réseau. Reportez-vous à la section "Configuration des bases de données réseau de confiance (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
    - 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 d'hôte distant.
    - Affectez des hôtes spécifiques à des modèles.
    - Affectez les sous-réseaux à des modèles.
14. Établissez le routage statique. Reportez-vous à la section "Configuration de routes et vérification des informations réseau dans Trusted Extensions (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
15. Configurez les utilisateurs locaux et les rôles d'administration locaux.
    - Pour appliquer la séparation des tâches, créez des profils avec des droits personnalisés.
    - 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.
16. Créez des répertoires personnels sur le serveur NFS.
    - Créez les répertoires personnels de chaque utilisateur sur chaque étiquette à laquelle l'utilisateur peut accéder.
    - (Facultatif) Empêchez les utilisateurs de lire leurs répertoires personnels de niveau inférieur.
17. Configurez l'impression. Reportez-vous à la section "Gestion de l'impression dans Trusted Extensions (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
18. Configurez les périphériques. Reportez-vous à la section "Manipulation des périphériques dans Trusted Extensions (liste des tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.
    a. Affectez le profil de gestion des périphériques ou le profil d'administrateur système à un rôle.
    b. 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.

19. Configurez les fonctionnalités Oracle Solaris.
    - Configurez le contrôle.
    - Configurez les paramètres de sécurité.
    - Activez certains clients LDAP en tant que systèmes d'administration LDAP.
    - Configurez les utilisateurs dans LDAP.
    - Configurez les rôles réseau dans LDAP.
    - Montez et partagez les systèmes de fichiers. Reportez-vous au Chapitre 11, "Gestion et montage de fichiers dans Trusted Extensions (tâches)" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

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 principal Personne chargée de la création de nouveaux profils de droits pour l'organisation, ainsi que de la résolution des problèmes matériels qui n'incombent pas à l'administrateur de sécurité ni à l'administrateur système. Ce rôle est très rarement assumé. Après la configuration initiale de la sécurité, des sites plus sécurisés peuvent choisir de ne pas créer ce rôle et de n'affecter aucun rôle au profil d'administrateur principal.

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 CDE, la bande de confiance se trouve au bas de l'écran, et dans Trusted JDS, en haut de l'écran. 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 la forme d'un fichier dans `/etc/security/tsol/tnrhdb` ou à partir du serveur LDAP.

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 accessible sous la forme d'un fichier dans `/etc/security/tsol/tnrhtp` ou à partir du serveur LDAP.

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.

boîte à outils Ensemble de programmes dans la Console de gestion Solaris. Sur un hôte Trusted Extensions, les administrateurs utilisent les boîtes à outils `Policy=TSOL`. Chaque boîte à outils possède des programmes pouvant être utilisés dans le cadre de la boîte à outils. Par exemple, l'outil Trusted Network Zones, qui gère la base de données `tnzonecfg` du système, n'existe que dans la boîte à outils `Files`, car sa portée est toujours locale. Le programme User Accounts existe dans toutes les boîtes à outils. Pour créer un utilisateur local, l'administrateur utilise la boîte à outils `Files`, et pour créer un utilisateur réseau, il utilise la boîte à outils `LDAP`.

bureau multiniveau Sur un système Solaris configuré avec Trusted Extensions, les utilisateurs peuvent exécuter un bureau à un niveau d'étiquette particulier. Si l'utilisateur est autorisé à travailler à plus d'un niveau d'étiquette, l'utilisateur peut créer un espace de travail distinct pour travailler à chaque niveau d'étiquette. Sur ce bureau multiniveau, les utilisateurs autorisés peuvent effectuer des couper-coller entre plusieurs fenêtres sur différentes étiquettes, recevoir des e-mails correspondant à différentes étiquettes et visualiser et utiliser des fenêtres étiquetées dans les espaces de travail d'une autre étiquette.

CDE Voir Common Desktop Environment.

chemin de confiance Sur un système Solaris configuré avec Trusted Extensions, le chemin de confiance est un moyen fiable 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 devant être protégées, 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.

chemin de recherche d'application Dans CDE, le chemin de recherche est utilisé par le système pour rechercher des applications et des informations de configuration. Le chemin de recherche d'application est contrôlé par un rôle de confiance.

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.

Common Desktop Environment Environnement multifenêtre historique pour l'administration du logiciel Trusted Extensions. Trusted Extensions modifie l'environnement pour créer Trusted CDE. Le Sun Java Desktop System est également modifié afin de créer un Trusted JDS.

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.
Console de gestion Solaris	Interface graphique d'administration basée sur Java qui contient les boîte à outils de programmes d'administration. La plupart des tâches de gestion du système, du réseau, et des utilisateurs s'effectuent par l'intermédiaire des boîtes à outils de la console.
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	Partie de la hiérarchie de nommage 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 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.
éditeur de confiance	Sur un système Solaris configuré avec Trusted Extensions, l'éditeur de confiance est utilisé pour créer et modifier les fichiers d'administration. L'éditeur ne peut pas modifier le nom de fichier. En outre, l'utilisation de l'éditeur est contrôlée et les commandes d'accès au shell sont désactivées. Dans Trusted CDE, l'action Admin Editor lance un éditeur de confiance. Dans Trusted JDS, la commande `/usr/dt/bin/trusted_edit` démarre l'éditeur de confiance.
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 supervisent 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` propre à Sun à la fin du fichier. Pour plus d'informations, reportez-vous au Chapitre 5, “Customizing LOCAL DEFINITIONS” du *Oracle Solaris 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 qui envoie des paquets réseau sans étiquette, tel qu'un système exécutant le SE Solaris.

MAC Voir contrôle d'accès obligatoire.

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 Identification d'un groupe de systèmes sur un réseau local. 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 Solaris configuré avec Trusted Extensions, un port multiniveau est utilisé pour fournir un service 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 de contrôle (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 actions CDE, ainsi que les attributs de sécurité affectés à ces fichiers exécutables. Les profils de droits permettant aux administrateurs 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 attribués sont en vigueur et l'utilisateur peut accéder à toutes les commandes, actions CDE et authorisations qui lui sont affectées dans l'ensemble des profils de droits.

relations d'étiquettes Sur un système 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 de commandes, d'autorisations d'accès et d'actions CDE particulier. Voir rôle d'administration.

rôle d'administration rôle qui donne les autorisations, commandes privilégiées, actions privilégiées et attributs de sécurité du chemin de confiance requis pour que le rôle puisse effectuer des tâches d'administration. Les rôles exécutent un sous-ensemble des capacités du superutilisateur de Solaris telles que la sauvegarde ou le contrôle.

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 options de menu pour les options de réseau, les options des services de noms et pour la liaison de la zone globale à un serveur LDAP existant. `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. Un service de nommage vous permet de maintenir, de gérer et d'accéder aux informations système à l'échelle de votre réseau. Sun prend en charge le service de nommage LDAP. 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 Pour un système Solaris configuré avec Trusted Extensions, un système sans étiquette est un système qui n'exécute pas de système d'exploitation multiniveau, comme 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 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 ont deux caractéristiques qui les distinguent des zones non globales d'un système Solaris non configuré avec des étiquettes. Tout d'abord, les zones étiquetées doivent utiliser le même pool d'ID utilisateur et d'ID de groupe. Deuxièmement, les zones étiquetées peuvent partager les adresses IP.

Index

A

Accès au serveur X, 111–113
Acheminement, Spécification de route par défaut pour les zones étiquetées, 87–91
Action, *Voir* Action d'administration
Action Check Encodings (Vérifier le fichier de codage), 52–56
Action Clone Zone (Cloner la zone), 171–172
Action Configure Zone (Configurer la zone), 161
Action Copy Zone (Copier la zone), 170–171
Action Create LDAP Client (Créer client LDAP), 64–68
Action d'administration
  Check Encodings (Vérifier le fichier de codage), 52–56
  Clone Zone (Cloner la zone), 171–172
  Configure Zone (Configurer la zone), 161
  Copy Zone (Copier la zone), 170–171
  Create LDAP Client (Créer client LDAP), 64–68
  Initialize Zone for LDAP (Initialiser la zone pour LDAP), 165
  Install Zone (Installer la zone), 165
  Share Logical Interface (Partager l'interface logique), 158
  Share Physical Interface (Partager l'interface physique), 159
  Shut Down Zone (Arrêter la zone), 169
  Start Zone (Démarrer la zone), 166
  Zone Terminal Console (Console de terminal de zone), 82, 165, 166
Action d'installation, Zone Console (Console de zone), 78
`Action failed. Reconnect to Solaris Zone?`, 111–113
Action Initialize Zone for LDAP (Initialiser la zone pour LDAP), 165
Action Install Zone (Installer la zone), 165
  Dépannage, 167
Action Share Logical Interface (Partager l'interface logique), 158
Action Share Physical Interface (Partager l'interface physique), 159
Action Shut Down Zone (Arrêter la zone), 169
Action Start Zone (Démarrer la zone), 166
Action Zone Terminal Console (Console de terminal de zone)
  Sortie, 82, 166
  Utilisation, 165
Activation
  Administration LDAP à partir d'un client, 134–135
  Connexion à une zone étiquetée, 104
  DOI différent de 1, 57–58
  `dpadm`, service, 124
  `dsadm`, service, 124
  `labeld`, service, 49
  Réseau IPv6, 56–57
  Trusted Extensions sur un système Solaris, 49
Administration, À distance via un rôle, 141–143
Adresse
  Partage entre des zones globale et étiquetées, 158–159
  Spécification d'une adresse IP par système, 73–74, 159–160

Ajout
Base de données réseau pour le serveur LDAP, 129–131
Boîte à outils LDAP, 135–136
Démon `nscd` pour chaque zone étiquetée, 91–92
Démon `nscd` spécifique à une zone, 91–92
Interface réseau partagée, 70–74
Interface réseau spécifique à une zone, 85–87
Rôle, 92–104
Rôle local à l'aide de `roleadd`, 98
Route par défaut pour les zones étiquetées, 87–91
Trusted Extensions à un système Solaris, 49
Utilisateur, à l'aide de `lpaddent`, 107–109
Utilisateur local à l'aide de `useradd`, 101–102
Utilisateur pouvant assumer des rôles, 99–102
Allocation de périphériques
Lecteur de bande, 116
Pour la copie de données, 113–115
Association d'interfaces réseau avec des zones à l'aide d'actions CDE (liste des tâches), 157–160

B

Boîte à outils
Ajout du serveur LDAP à `tsol_ldap.tbx`, 135–136
Chargement dans Trusted Extensions, 61–64
Scope=LDAP, 133–134

C

`Cannot reach global zone`, 111–113
`chk_encodings`, commande, 55–56
Collecte d'informations
Avant l'activation de Trusted Extensions, 46
Pour service LDAP, 121–122
Compte
Création, 92–104
Planification, 28
Configuration
Accès à l'écouteur Trusted Extensions, 139–147
Console de gestion Solaris pour LDAP, 132–138
Interface réseau, 70–74
LDAP pour Trusted Extensions, 121–131
Configuration *(Suite)*
Logiciel Trusted Extensions, 51–117
Rôle ou superutilisateur ?, 48
Serveur proxy LDAP pour les clients Trusted Extensions, 131–132
Zone étiquetée Trusted Extensions, 68–84, 157–172
Configuration d'un serveur LDAP sur un hôte Trusted Extensions (liste des tâches), 119–120
Configuration d'un serveur proxy LDAP sur un hôte Trusted Extensions (liste des tâches), 120–121
Configuration de l'écouteur dans Trusted Extensions (liste des tâches), 139–147
Configuration de la Console de gestion Solaris pour LDAP (liste des tâches), 132–138
Configuration de Trusted Extensions
Accès à l'écouteur, 139–147
Ajout de bases de données réseau à un serveur LDAP, 129–131
Base de données pour LDAP, 121–131
configuration, 20
LDAP, 121–131
Liste de contrôle pour l'équipe chargée de l'installation, 173–176
Liste des tâches, 35–39
Modification de la valeur DOI par défaut, 57–58
Procédure initiale, 51–117
Redémarrage pour l'activation des étiquettes, 59–61
Responsabilités de l'équipe chargée de la configuration initiale, 41
Séparation des tâches, 41
Zone étiquetée, 68–84, 157–172
Configuration LDAP
Création de client, 64–68
Pour Trusted Extensions, 121–131
Serveur Sun Ray, et, 121
Configuration requise de Trusted Extensions
Installation de Solaris, 42–43
Mot de passe root, 44
Configuration requise pour Trusted Extensions
Options d'installation de Solaris, 42–43
Système Solaris installé, 43–45
Configuration Trusted Extensions
Dépannage, 110–113
Écouteur, 139–147

Connexion
  À distance, 141–143
  Serveur d'annuaires personnel, 106–107
  Utilisation de la commande `rlogin`, 145–147
Connexion à distance, Activation pour les rôles, 141–143
Console de gestion Solaris
  Activation de la boîte à outils LDAP à utiliser, 134–135
  Chargement d'une boîte à outils Trusted Extensions, 61–64
  Configuration de la boîte à outils LDAP, 135–136
  Configuration pour LDAP, 132–138
  Dépannage, 61–64
  Enregistrement des informations d'identification et de connexion LDAP, 133–134
  Fonctionnement avec Sun Java System Directory Server, 132–138
  Initialisation, 61–64
  Utilisation de l'outil Trusted Network Zone Configuration, 75, 162
Contrôle
  `label_encodings`, fichier, 52–56
  Planification, 28
Création
  Boîte à outils LDAP, 135–136
  Client LDAP, 64–68
  Compte, 92–104
  Compte au cours ou après la configuration, 48
  Répertoire personnel, 104–107
  Rôle, 92–104
  Rôle local à l'aide de `roleadd`, 98
  Serveur d'annuaires personnel, 105–106
  Serveur proxy LDAP pour les clients Trusted Extensions, 132
  Utilisateur local à l'aide de`useradd`, 101–102
  Utilisateur pouvant assumer des rôles, 99–102
  Zone, 68–84, 164–167
  Zone étiquetée, 68–84
Création d'une nouvelle option de menu de zone, 74
Création d'une option de menu de zone, 82–84
Création de zones étiquetées, 68–84
Création de zones étiquetées à l'aide d'actions CDE (liste des tâches), 163–172

D

Décision à prendre, Avant l'activation de Trusted Extensions, 47–48
Décisions à prendre, Selon la stratégie de sécurité du site, 150
Démarrage
  Zone, 78–79, 166
Démon de cache de service de noms, *Voir* `nscd`, démon
Dépannage
  Accès au serveur X, 111–113
  Configuration IPv6, 56
  Configuration Trusted Extensions, 110–113
  Console de gestion Solaris, 61–64
  Fenêtre de console qui ne s'ouvre pas, 110
  `Installation of these packages generated errors: SUNW`*pkgname*, 77, 167
  Trusted Network Zones Properties (Propriétés des zones de réseau de confiance), 163
  Version de Solaris prenant en charge le service `labeld`, 49
Déroulement
  Liste des tâches : configuration de Trusted Extensions, 37–39
  Liste des tâches : préparation d'un système Solaris pour Trusted Extensions, 35
  Liste des tâches : préparation et activation de Trusted Extensions, 35–37
Désactivation, Trusted Extensions, 116–117
Domaine d'interprétation (DOI), Entrée dans le fichier `/etc/system`, 57–58
`dpadm`, Service, 124
`dsadm`, service, 124

E

Écran, Affichage initial, 61
Enregistrement, Informations d'identification et de connexion LDAP avec la Console de gestion Solaris, 133–134
Équipe chargée de la configuration initiale, Liste de contrôle pour la configuration de Trusted Extensions, 173–176
Espace de travail, Affichage initial, 61

/etc/system, fichier
Modification pour le réseau IPv6, 56–57
Modification pour un DOI différent de 1, 57–58
Étiquetage
Activation des étiquettes, 59–61
Zone, 74–76, 161–163
Étiquette
Attribution aux zones nommées, 75, 162
Bande de confiance, 61
Planification, 22–23
Spécification pour une zone, 74–76, 161–163

F

Fenêtre de console, Résolution des problèmes d'ouverture, 110
Fichier
Copie à partir d'un support amovible, 115
resolv.conf, 67–68
Fichier de codage, *Voir* label_encodings, fichier
Fichier de configuration, Copie, 113–115
Fichier journal, Protection des journaux du serveur d'annuaire, 127–128

G

Gestionnaire de zones étiquetées, *Voir* txzonemgr, script

I

Impression, Planification, 26–27
Informations d'identification et de connexion, Enregistrement de LDAP avec la Console de gestion Solaris, 133–134
Informations de sécurité, Planification pour Trusted Extensions, 31
Initialisation
Console de gestion Solaris, 61–64
Zone, 78–79, 165, 166
Zone pour LDAP, 164–167
Installation
label_encodings, fichier, 52–56
SE Solaris pour Trusted Extensions, 41–49
Sun Java System Directory Server, 121–131
Zone, 77, 164–167
IPv6
Dépannage, 56
Entrée dans le fichier /etc/system, 56–57

L

label_encodings, fichier
Contrôle, 52–56
Installation, 52–56
Localisation, 22–23
Modification, 52–56
labeld, service, 49
Dépannage, 49
Désactivation, 117
LDAP
Activation de l'administration à partir d'un client, 134–135
Planification, 27
Lecteur de bande, Allocation, 116
Liste des tâches : configuration de Trusted Extensions, 37–39
Liste des tâches : préparation d'un système Solaris pour Trusted Extensions, 35
Liste des tâches : préparation et activation de Trusted Extensions, 35–37
Listes de contrôle pour l'équipe chargée de la configuration initiale, 173–176
lpaddent, commande, 107–109

M

Menu d'installation
Create a new zone (Créer une zone), 74
Création d'une zone, 82–84
Message d'erreur
Dépannage, 49, 111–113
Modification, label_encodings, fichier, 52–56
Mot de passe root, Requis dans Trusted Extensions, 44

N

`No route available`, 111–113
Nom
  Spécification pour une zone, 74–76, 161–163
Nommage
  Zone, 74–76, 161–163
`nscd`, démon, Ajout à chaque zone étiquetée, 91–92

O

Options d'installation de Solaris, Configuration requise, 42–43
Ordinateur portable, Planification, 27
Outil Trusted Network Zones
  Attribution d'étiquette aux zones nommées, 75
  Attribution d'étiquettes aux zones nommées, 162
  Dépannage, 163

P

Planification
  Voir aussi Utilisation de Trusted Extensions
  Configuration d'ordinateur portable, 27
  Contrôle, 27–28
  Création de compte, 28
  Étiquette, 22–23
  Impression, 26–27
  Matériel, 23
  Réseau, 23–24
  Serveur NFS, 26–27
  Service de nommage LDAP, 27
  Stratégie d'administration, 21–22
  Stratégie de configuration de Trusted Extensions, 29–30
  Trusted Extensions, 19–32
  Zone, 24–26
Planification matérielle, 23
Pool ZFS, Création pour le clonage de zones, 58–59
Préparation de la création de zones à l'aide d'actions CDE (liste des tâches), 160–163
Prise de décision
  Configuration en tant que rôle ou superutilisateur, 48
Prise de décision *(Suite)*
  Utilisation d'un fichier de codage fourni par Sun, 47
Profil de droits, Personnalisation pour la séparation des tâches, 93–96
Publications, Sécurité et UNIX, 154–155

R

Redémarrage
  Activation de la connexion à une zone étiquetée, 104
  Activation des étiquettes, 59–61
Répertoire, Configuration du service de nommage, 129
Répertoire personnel
  Connexion et obtention, 106–107
  Création, 104–107
  Création du serveur, 105–106
Réseau, *Voir* Réseau Trusted Extensions
Réseau Trusted Extensions
  Activation d'IPv6, 56–57
  Ajout d'une interface spécifique à une zone, 85–87
  Ajout de démon `nscd` spécifique à une zone, 91–92
  Planification, 23–24
  Spécification de route par défaut pour les zones étiquetées, 87–91
  Suppression du démon `nscd` spécifique à une zone, 92
`resolv.conf`, fichier, Chargement lors de la configuration, 67–68
Rôle
  Ajout de rôle local à l'aide de `roleadd`, 98
  Connexion à distance, 141–143
  Création de l'administrateur de sécurité, 96–98
  Détermination du moment de création, 48
  Séparation des tâches, 93–96, 99
  Vérification du fonctionnement, 102–104
Rôle d'administrateur de sécurité, Création, 96–98
Rôle d'administrateur système, Limitation, 99
`roleadd`, commande, 98
Route par défaut, Spécification pour les zones étiquetées, 87–91

S

Sauvegarde, Système antérieur avant l'installation, 31–32
Sécurité
  Équipe chargée de la configuration initiale, 41
  Mot de passe root, 44
  Publications, 154–155
  Stratégie de sécurité du site, 149–155
Séparation des tâches
  Création de profil de droits, 93–96
  Planification, 29–30
  Planification pour LDAP, 129
Serveur LDAP
  Collecte d'informations, 121–122
  Configuration d'un port multiniveau, 128–129
  Configuration de proxy pour les clients Trusted Extensions, 131–132
  Configuration du service de nommage, 122–125
  Création de proxy pour les clients Trusted Extensions, 132
  Enregistrement des informations d'identification et de connexion avec Console de gestion Solaris, 133–134
  Installation dans Trusted Extensions, 122–125
  Planification de la séparation des tâches, 129
  Protection des fichiers journaux, 127–128
Serveur multiniveau, Planification, 26–27
SMF (Service Management Framework, utilitaire de gestion de services), `labeld`, service, 49
SMF (Service Management Framework, Utilitaire de gestion des services)
  `dpadm`, 124
  `dsadm`, 124
Solaris Trusted Extensions, *Voir* Trusted Extensions
Stratégie de sécurité du site
  Compréhension, 20–21
  Décisions de configuration de Trusted Extensions, 150
  Recommandations, 151
  Recommandations d'accès physique, 152
  Recommandations relatives au personnel, 153
  Tâches, 149–155
  Violations courantes, 153–154
Sun Java System Directory Server, *Voir* Serveur LDAP
Support, Copie des fichiers à partir d'un support amovible, 115
Suppression
  Démon `nscd` spécifique à une zone, 92
  Zone étiquetée, 116
Suppression de Trusted Extensions, *Voir* Désactivation
`svcs: Pattern 'labeld' doesn't match any instances`, 49
Système Solaris installé, Configuration requise pour Trusted Extensions, 43–45
Système Sun Ray
  Serveur LDAP, et, 121
  Site Web de documentation, 36

T

Tâche et liste de tâches
  Configuration d'un serveur proxy LDAP sur un hôte Trusted Extensions (liste des tâches), 120–121
  Tâches de configuration supplémentaires de Trusted Extensions, 113–117
Tâche et liste des tâches
  Association d'interfaces réseau avec des zones à l'aide d'actions CDE (liste des tâches), 157–160
  Configuration d'un serveur LDAP sur un hôte Trusted Extensions (liste des tâches), 119–120
  Configuration de l'écouteur dans Trusted Extensions (liste des tâches), 139–147
  Configuration de la Console de gestion Solaris pour LDAP (liste des tâches), 132–138
  Création de zones étiquetées, 68–84
  Création de zones étiquetées à l'aide d'actions CDE (liste des tâches), 163–172
  Préparation de la création de zones à l'aide d'actions CDE (liste des tâches), 160–163
Tâches de configuration supplémentaires de Trusted Extensions, 113–117
`tcp_listen=true`, paramètre LDAP, 134–135
Trusted Extensions
  Voir aussi Planification Trusted Extensions
  Activation, 49
  Collecte d'informations avant l'activation, 46
  Décision à prendre avant l'activation, 47–48
  Désactivation, 116–117

Trusted Extensions *(Suite)*
Différences du point de vue de l'administrateur Oracle Solaris, 32–33
Mémoire requise, 23
Planification, 19–32
Planification de la stratégie de configuration, 29–30
Planification de réseau, 23–24
Planification matérielle, 23
Préparation, 42–45, 46–48
Résultats avant configuration, 32–33
Séparation des tâches, 29–30
Stratégie de configuration à deux rôles, 30
`tsol_ldap.tbx`, fichier, 135–136
`txzonemgr`, script, 69–70, 112

U

`useradd`, commande, 101–102
`/usr/sbin/txzonemgr`, script, 69–70, 112, 163
Utilisateur
Ajout à partir du serveur NIS, 107–109
Ajout d'utilisateur local à l'aide de `useradd`, 101–102
Création d'utilisateurs initiaux, 99–102
Deux rôles nécessaires pour créer des utilisateurs, 99
Deux rôles nécessaires pour créer un utilisateur, 93–96

V

Vérification
État de la zone, 79–81
Fonctionnement des rôles, 102–104
`label_encodings`, fichier, 52–56

Z

`zenity`, script, 69–70
ZFS, Non pris en charge mais méthode de création de zone rapide, 26
Zone
Activation de la connexion, 104
Affichage de l'activité de la zone, 78, 82, 166
Ajout d'une interface réseau, 85–87
Ajout du démon `nscd` à chaque zone étiquetée, 91–92
Arrêt, 81, 169
Association de noms de zones aux étiquettes, 75, 162
Choix de la méthode de création, 24–26
Création, 164–167
Création de pool ZFS pour le clonage, 58–59
Démarrage, 166
Dépannage relatif à l'installation, 77
Initialisation, 78–79, 165, 166
Initialisation pour LDAP, 164–167
Installation, 77, 164–167
Isolement avec des routes par défaut, 87–91
Personnalisation, 81–82
Résolution des problèmes d'accès, 111–113
Spécification d'étiquette, 74–76, 161–163
Spécification d'une adresse IP partagée, 158–159
Spécification d'une adresse IP pour toutes les zones, 73–74, 159–160
Spécification de nom, 74–76, 161–163
Spécification de route par défaut, 87–91
Suppression, 116
Suppression du démon `nscd` des zones étiquetées, 92
`txzonemgr`, script, 112
`/usr/sbin/txzonemgr`, script, 69–70, 163
Vérification de l'état, 79–81
Zone Console (Console de zone), Sortie, 78