

# **Guide de l'utilisateur Oracle Solaris Trusted Extensions**

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

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

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

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

#### U.S. GOVERNMENT RIGHTS

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

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

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

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

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

# Table des matières

---

<b>Préface</b> .....	11
<b>1 Présentation du logiciel Solaris Trusted Extensions</b> .....	15
Qu'est-ce que le logiciel Trusted Extensions ? .....	15
Trusted Extensions vous protège contre les intrus .....	16
L'accès à la base informatique sécurisée est limité .....	16
Le contrôle d'accès obligatoire protège les informations .....	17
Les périphériques sont protégés .....	17
Les programmes qui usurpent l'identité des utilisateurs sont bloqués .....	17
Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire .....	18
Contrôle d'accès discrétionnaire .....	18
Contrôle d'accès obligatoire .....	18
Responsabilités des utilisateurs concernant la protection des données .....	26
Trusted Extensions sépare les informations en fonction des étiquettes .....	26
Sessions à niveau unique ou multiniveau .....	26
Exemple de sélection de session .....	27
Espaces de travail étiquetés .....	28
Application du MAC pour les transactions par e-mail .....	29
Suppression des données d'objets avant la réutilisation des objets .....	29
Trusted Extensions active l'administration sécurisée .....	29
Accès aux applications dans Trusted Extensions .....	30
Administration par rôle dans Trusted Extensions .....	30
<b>2 Connexion à Trusted Extensions (tâches)</b> .....	33
Bureaux et connexions dans Trusted Extensions .....	33
Processus de connexion à Trusted Extensions .....	34
Choix du bureau avant la connexion .....	35

Identification et authentification lors de la connexion .....	35
Vérification des attributs de sécurité lors de la connexion .....	35
Connexion à Trusted Extensions .....	36
▼ Choix d'un bureau sécurisé .....	36
▼ Identification et authentification auprès du système .....	36
▼ Consultation des messages et sélection du type de session .....	37
▼ Résolution des problèmes de connexion .....	39
Connexion à distance à Trusted Extensions .....	40
▼ Connexion à un bureau Trusted Extensions distant .....	40
<b>3 Utilisation de Trusted Extensions (tâches) .....</b>	<b>43</b>
Sécurité visible du bureau dans Trusted Extensions .....	43
Processus de déconnexion de Trusted Extensions .....	44
Travail sur un système étiqueté .....	44
▼ Verrouillage et déverrouillage de l'écran .....	44
▼ Déconnexion de Trusted Extensions .....	46
▼ Procédure d'arrêt du système .....	47
▼ Procédure d'affichage de vos fichiers dans un espace de travail étiqueté .....	48
▼ Procédure d'accès aux pages de manuel Trusted Extensions .....	50
▼ Procédure d'accès à l'aide en ligne de Trusted Extensions .....	50
▼ Procédure de personnalisation du menu Workspace de CDE .....	51
▼ Procédure d'accès aux fichiers d'initialisation de chaque étiquette .....	53
▼ Procédure d'affichage interactif d'une étiquette de fenêtre .....	54
▼ Exécution de certaines tâches de bureau courantes dans Trusted Extensions .....	55
Réalisation d'actions sécurisées .....	57
▼ Procédure de modification du mot de passe dans Trusted Extensions .....	57
▼ Procédure de connexion à une étiquette différente .....	58
▼ Procédure d'allocation d'un périphérique dans Trusted Extensions .....	59
▼ Procédure de libération d'un périphérique dans Trusted Extensions .....	63
▼ Procédure d'adoption d'un rôle dans Trusted Extensions .....	63
▼ Procédure de modification de l'étiquette d'un espace de travail .....	64
▼ Procédure d'ajout d'un espace de travail possédant une étiquette particulière .....	65
▼ Procédure de basculement vers un espace de travail possédant une étiquette différente ....	66
▼ Procédure de déplacement d'une fenêtre vers un autre espace de travail .....	67
▼ Procédure de détermination de l'étiquette d'un fichier .....	68

---

▼ Procédure de déplacement de données entre les étiquettes .....	69
▼ Procédure de déplacement de fichiers entre les étiquettes dans Trusted CDE .....	73
<b>4 Éléments de Trusted Extensions (Référence) .....</b>	<b>77</b>
Caractéristiques visibles de Trusted Extensions .....	77
Étiquettes sur les bureaux Trusted Extensions .....	79
Bande de confiance .....	79
Sécurité des périphériques dans Trusted Extensions .....	81
Fichiers et applications dans Trusted Extensions .....	81
Fichier .copy_files .....	82
Fichier .link_files .....	82
Sécurité du mot de passe dans le SE Solaris .....	82
Sécurité du tableau de bord (Trusted CDE) .....	83
Zone de commutation de l'espace de travail .....	84
Menu Trusted Path .....	84
Sécurité de l'horloge .....	85
Sécurité du calendrier .....	85
Sécurité du gestionnaire de fichiers .....	85
Sécurité de l'éditeur de texte .....	86
Sous-panneau d'applications personnelles .....	86
Sécurité du logiciel de messagerie .....	86
Sécurité des imprimantes .....	86
Sécurité du gestionnaire de style .....	87
Sécurité du gestionnaire d'applications .....	88
Sécurité de la corbeille .....	88
Sécurité de l'espace de travail (Trusted JDS) .....	88
<b>Glossaire .....</b>	<b>91</b>
<b>Index .....</b>	<b>101</b>



# Liste des figures

---

FIGURE 1-1	Logo Trusted Extensions dans CDE .....	16
FIGURE 1-2	Symbole de confiance .....	18
FIGURE 1-3	Étiquettes de sensibilité classiques dans l'industrie .....	19
FIGURE 1-4	Session Trusted CDE classique .....	21
FIGURE 1-5	Session Trusted JDS classique .....	22
FIGURE 1-6	Affichage d'informations publiques à partir d'une zone d'étiquette supérieure .....	23
FIGURE 1-7	Zone de commutation de l'espace de travail .....	28
FIGURE 1-8	Panneaux étiquetés .....	28
FIGURE 2-1	Boîte de dialogue de dernière connexion .....	38
FIGURE 2-2	Générateur d'étiquettes .....	39
FIGURE 3-1	Zone de commutation du tableau de bord .....	45
FIGURE 3-2	Sélection du verrouillage de l'écran .....	45
FIGURE 3-3	Gestionnaire de fichiers étiqueté .....	49
FIGURE 3-4	Aide en ligne de Trusted Extensions .....	51
FIGURE 3-5	Opération de requête d'étiquette de fenêtre .....	55
FIGURE 3-6	Menu Trusted Path .....	58
FIGURE 3-7	Icône d'allocation de périphériques dans Trusted CDE .....	59
FIGURE 3-8	Gestionnaire d'allocation de périphériques .....	60
FIGURE 3-9	Instructions relatives à l'utilisation d'un microphone .....	61
FIGURE 3-10	Tableau de bord avec les commutateurs affichant les différentes étiquettes .....	66
FIGURE 3-11	Menu Occupy Workspace dans Trusted CDE .....	67
FIGURE 3-12	Fenêtres possédant des étiquettes différentes dans un seul espace de travail .....	68
FIGURE 3-13	Applications possédant des étiquettes différentes dans un même espace de travail .....	70
FIGURE 3-14	Boîte de dialogue de confirmation du gestionnaire de sélection dans Trusted JDS .....	71
FIGURE 3-15	Boîte de dialogue de confirmation du gestionnaire de sélection dans Trusted CDE .....	72

FIGURE 3-16	Gestionnaires de fichiers possédant des étiquettes différentes dans un même espace de travail .....	74
FIGURE 3-17	Déplacement d'un fichier entre des gestionnaires de fichiers possédant des étiquettes différentes .....	75
FIGURE 3-18	Boîte de dialogue de confirmation du gestionnaire de fichiers .....	76
FIGURE 4-1	Bureau Trusted CDE multiniveau .....	78
FIGURE 4-2	Panneaux indiquant des espaces de travail possédant des étiquette différentes dans Trusted JDS .....	79
FIGURE 4-3	Étiquette de fenêtre PUBLIC dans la bande de confiance .....	80
FIGURE 4-4	Bande de confiance sur le bureau Trusted JDS .....	80
FIGURE 4-5	Indicateur Trusted Path dans la bande de confiance .....	81
FIGURE 4-6	Menu Trusted Path - Base .....	84
FIGURE 4-7	Menu Trusted Path - Version de l'espace de travail <i>Name</i> .....	85
FIGURE 4-8	Page de garde standard pour un travail d'impression étiqueté .....	87

# Liste des tableaux

---

TABLEAU 1-1	Exemples de relations d'étiquettes dans Trusted Extensions .....	25
TABLEAU 1-2	Effet de la sélection initiale de l'étiquette sur les étiquettes disponibles au cours de la session .....	27



# Préface

---

Le *Guide de l'utilisateur Oracle Solaris Trusted Extensions* est un guide d'utilisation du système d'exploitation Solaris (SE Solaris) avec Solaris Trusted Extensions installé.

## Utilisateurs de ce guide

Ce guide est destiné à tous les utilisateurs de Trusted Extensions. Vous devez être familiarisé avec l'utilisation du SE Solaris et de l'un des bureaux suivants :

- CDE (Common Desktop Environment)
- Bureau GNOME Open Source
- Sun Java Desktop System

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

## Organisation des guides Solaris Trusted Extensions

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

Titre du guide	Sujets	Public visé
<i>Solaris Trusted Extensions Transition Guide</i>	Obsolète. Fournit un aperçu des différences entre les logiciels Trusted Solaris 8, Solaris10 et Solaris Trusted Extensions.  Pour cette version, le document <i>Nouveautés</i> pour le SE Solaris fournit un aperçu des modifications apportées à Trusted Extensions.	Tous
<i>Solaris Trusted Extensions Reference Manual</i>	Obsolète. Fournit les pages de manuel Solaris 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 comprises parmi les pages de manuel Solaris.	Tous

Titre du guide	Sujets	Public visé
<i>Guide de l'utilisateur Oracle Solaris Trusted Extensions</i>	Décrit les fonctions de base de Solaris Trusted Extensions. Ce guide contient un glossaire.	Utilisateurs, administrateurs, développeurs
<i>Solaris Trusted Extensions Installation and Configuration for Solaris 10 11/06 and Solaris 10 8/07 Releases</i>	Obsolète. Décrit la planification, l'installation et la configuration de Solaris Trusted Extensions pour les versions Solaris 10 11/06 et Solaris 10 8/07 de Trusted Extensions.	Administrateurs, développeurs
<i>Guide de configuration d'Oracle Solaris Trusted Extensions</i>	Depuis la version Solaris 10 5/08, décrit l'activation et la configuration initiale de Solaris Trusted Extensions. Remplace <i>Solaris Trusted Extensions Installation and Configuration for the Solaris 10 11/06 and Solaris 10 8/07 Releases</i> .	Administrateurs, développeurs
<i>Procédures de l'administrateur Oracle Solaris Trusted Extensions</i>	Indique comment effectuer des tâches d'administration spécifiques.	Administrateurs, développeurs
<i>Oracle Solaris Trusted Extensions Developer's Guide</i>	Explique le développement d'applications avec Trusted Extensions.	Développeurs, administrateurs
<i>Oracle Solaris Trusted Extensions Label Administration</i>	Fournit des informations sur la spécification des composants d'étiquettes dans le fichier label_encodings.	Administrateurs
<i>Compartmented Mode Workstation Labeling: Encodings Format</i>	Décrit la syntaxe utilisée dans le fichier label_encodings. La syntaxe met en œuvre les différentes règles permettant de créer des étiquettes correctes pour un système.	Administrateurs

## Organisation de ce guide

Le [Chapitre 1, “Présentation du logiciel Solaris Trusted Extensions”](#) décrit les concepts de base mis en œuvre sur un système Solaris configuré avec Trusted Extensions.

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

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

Le [Chapitre 4, “Éléments de Trusted Extensions \(Référence\)”](#) présente les éléments clés d'un système configuré avec Trusted Extensions.

Le [Glossaire](#) décrit les termes relatifs à la sécurité utilisés dans Trusted Extensions.

## Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, rendez-vous sur le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou sur le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

## 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 <code>.login</code> . Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers. <code>nom_machine%</code> Vous avez reçu du courrier.
<b>AaBbCc123</b>	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	<code>nom_machine%</code> <b>su</b> Mot de passe :
<i>aabbcc123</i>	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est <code>rm nom_fichier</code> .
<i>AaBbCc123</i>	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du <i>Guide de l'utilisateur</i> . Un <i>cache</i> est une copie des éléments stockés localement. <i>N'enregistrez pas</i> le fichier. <b>Remarque</b> : 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#

# Présentation du logiciel Solaris Trusted Extensions

---

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

- “Qu'est-ce que le logiciel Trusted Extensions ?” à la page 15
- “Trusted Extensions vous protège contre les intrus” à la page 16
- “Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire” à la page 18
- “Trusted Extensions sépare les informations en fonction des étiquettes” à la page 26
- “Trusted Extensions active l'administration sécurisée” à la page 29

## Qu'est-ce que le logiciel Trusted Extensions ?

Comme le nom et le logo suivants l'indiquent, Trusted Extensions étend les capacités du SE Solaris.

FIGURE 1-1 Logo Trusted Extensions dans CDE



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

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

## Trusted Extensions vous protège contre les intrus

Le logiciel Trusted Extensions ajoute au SE Solaris des fonctionnalités qui vous protègent contre les intrusions. Trusted Extensions s'appuie également sur certaines fonctionnalités de Solaris telles que la protection par mot de passe. Trusted Extensions ajoute une interface graphique de changement de mot de passe pour les rôles. Le contrôle est activé par défaut.

### L'accès à la base informatique sécurisée est limité

Le terme *base informatique sécurisée* (TCB, *Trusted Computing Base*) fait référence à la partie du logiciel Trusted Extensions qui gère les événements liés à la sécurité. La TCB englobe les logiciels, le matériel, les microprogrammes, la documentation et les procédures administratives. Les utilitaires et programmes d'application pouvant accéder aux fichiers relatifs à la sécurité font tous partie de la TCB. Votre administrateur définit les limites de toutes les interactions

potentielles que vous pouvez avoir avec la TCB. Ces interactions incluent les programmes dont vous avez besoin pour effectuer votre travail, les fichiers auxquels vous êtes autorisé à accéder et les utilitaires qui peuvent compromettre la sécurité.

## Le contrôle d'accès obligatoire protège les informations

Si un intrus parvient à se connecter au système, d'autres d'obstacles l'empêchent d'accéder aux informations. Les fichiers et autres ressources sont protégés par le contrôle d'accès. Comme dans le SE Solaris, le contrôle d'accès peut être défini par le propriétaire des informations. Dans Trusted Extensions, l'accès est également contrôlé par le système. Pour plus d'informations, reportez-vous à la section [“Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire”](#) à la page 18.

## Les périphériques sont protégés

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

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

## Les programmes qui usurpent l'identité des utilisateurs sont bloqués

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

FIGURE 1-2 Symbole de confiance



Ce symbole s'affiche à chaque fois que vous interagissez avec la base informatique sécurisée (TCB). La présence du symbole garantit la sécurité des transactions. L'absence de symbole indique une faille de sécurité potentielle. Le symbole de confiance est représenté à la figure ci-dessus.

## Trusted Extensions fournit des contrôles d'accès discrétionnaire et obligatoire

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

### Contrôle d'accès discrétionnaire

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

Les bits d'autorisation permettent au propriétaire de définir la protection en lecture, écriture et exécution en fonction du statut de l'utilisateur : propriétaire, groupe et autres utilisateurs. Sur les systèmes UNIX classiques, le superutilisateur ou l'utilisateur root peut passer outre à la protection DAC. Avec Trusted Extensions, les administrateurs et les utilisateurs autorisés peuvent passer outre au DAC. Les listes de contrôle d'accès (ACL) fournissent une granularité plus fine du contrôle d'accès. Les ACL permettent aux propriétaires de spécifier des autorisations distinctes pour des utilisateurs et des groupes spécifiques. Pour plus d'informations, reportez-vous au [Chapitre 6, "Controlling Access to Files \(Tasks\)"](#) du *System Administration Guide: Security Services*.

### Contrôle d'accès obligatoire

Le contrôle d'accès obligatoire (MAC) est un mécanisme de contrôle d'accès appliqué par le système et basé sur les relations entre les étiquettes. Le système associe une étiquette de sensibilité à tous les processus créés pour exécuter des programmes. La stratégie MAC utilise cette étiquette dans les décisions de contrôle d'accès. En général, les processus ne peuvent pas stocker d'informations ni communiquer avec d'autres processus, sauf si l'étiquette de la destination est égale à l'étiquette du processus. La stratégie MAC autorise les processus à lire des

données d'objets de même niveau d'étiquette ou d'un niveau inférieur. Toutefois, l'administrateur peut créer un environnement étiqueté dans lequel peu d'objets de niveau inférieur, voire aucun, ne sont disponibles.

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

## Étiquettes de sensibilité et autorisations

Une étiquette possède les deux composants suivants :

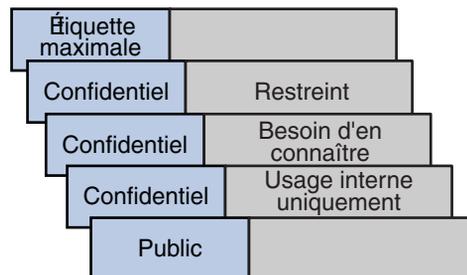
- Classification, également appelée *niveau*

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

Au sein du gouvernement américain, les classifications sont TOP SECRET, SECRET, CONFIDENTIAL et UNCLASSIFIED. Les classifications industrielles ne sont pas normalisées. Une entreprise peut établir des classifications uniques. Pour en voir un exemple, reportez-vous à la [Figure 1-3](#). Les termes figurant sur la gauche sont les classifications. Les termes figurant sur la droite sont les compartiments.
- Compartiments, également appelés *catégories*

Un compartiment représente un groupement, tel qu'un groupe de travail, un service, un projet ou un sujet. Une classification n'a pas besoin d'avoir de compartiment. Dans la [Figure 1-3](#), la classification *Confidentiel* possède trois compartiments exclusifs. Les classifications *Public* et *Étiquette maximale* n'ont aucun compartiment. Comme le montre cette figure, cinq étiquettes sont définies par cette organisation.

FIGURE 1-3 Étiquettes de sensibilité classiques dans l'industrie



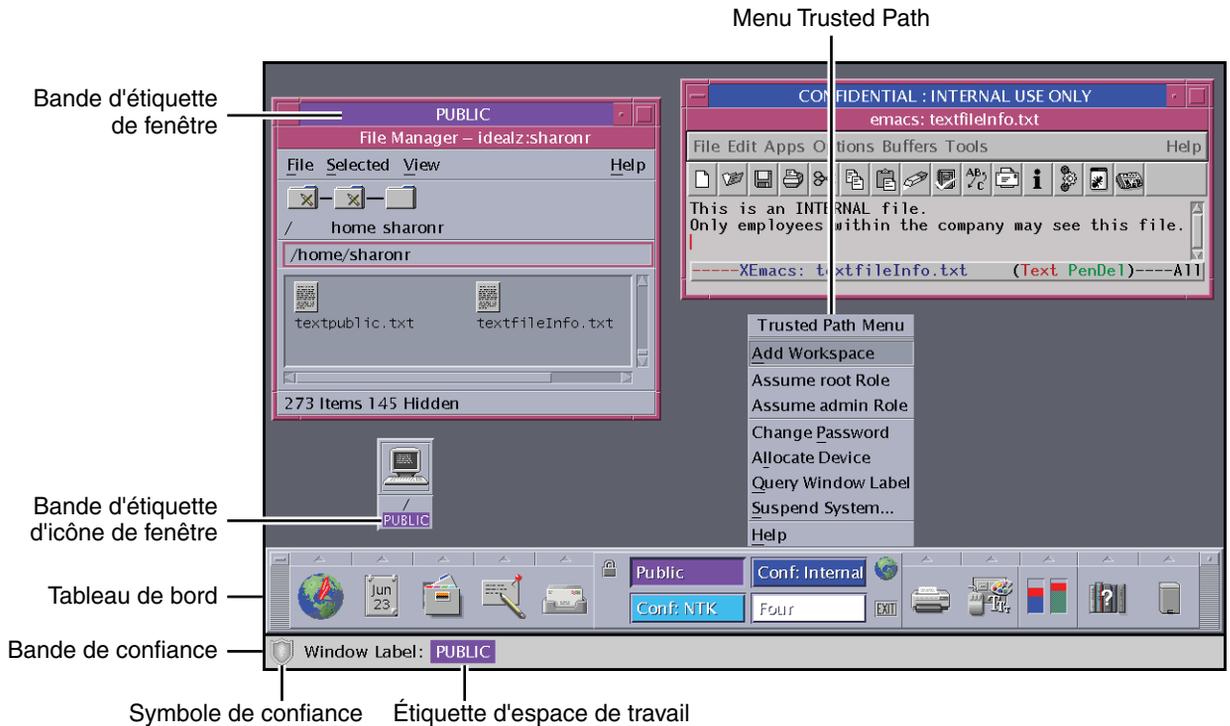
Trusted Extensions gère deux types d'étiquettes : les *étiquettes de sensibilité* et les *autorisations*. Un utilisateur peut être autorisé à travailler sur une ou plusieurs étiquettes de sensibilité. Une étiquette spéciale, appelée *autorisation de l'utilisateur*, détermine le plus haut niveau d'étiquette sur laquelle un utilisateur est autorisé à travailler. En outre, chaque utilisateur possède une

étiquette de sensibilité minimum. Cette étiquette est utilisée par défaut lors de la connexion à une session de bureau multiniveau. Après la connexion, l'utilisateur peut choisir de travailler sur d'autres étiquettes dans cette plage. Un utilisateur peut posséder l'étiquette de sensibilité minimum `Public` et l'autorisation `Confidential : Need to Know`. À la première connexion, les espaces de travail du bureau se trouvent au niveau d'étiquette `Public`. Au cours de la session, l'utilisateur peut créer des espaces de travail possédant les étiquettes `Confidential : Internal Use Only` et `Confidential : Need to Know`.

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

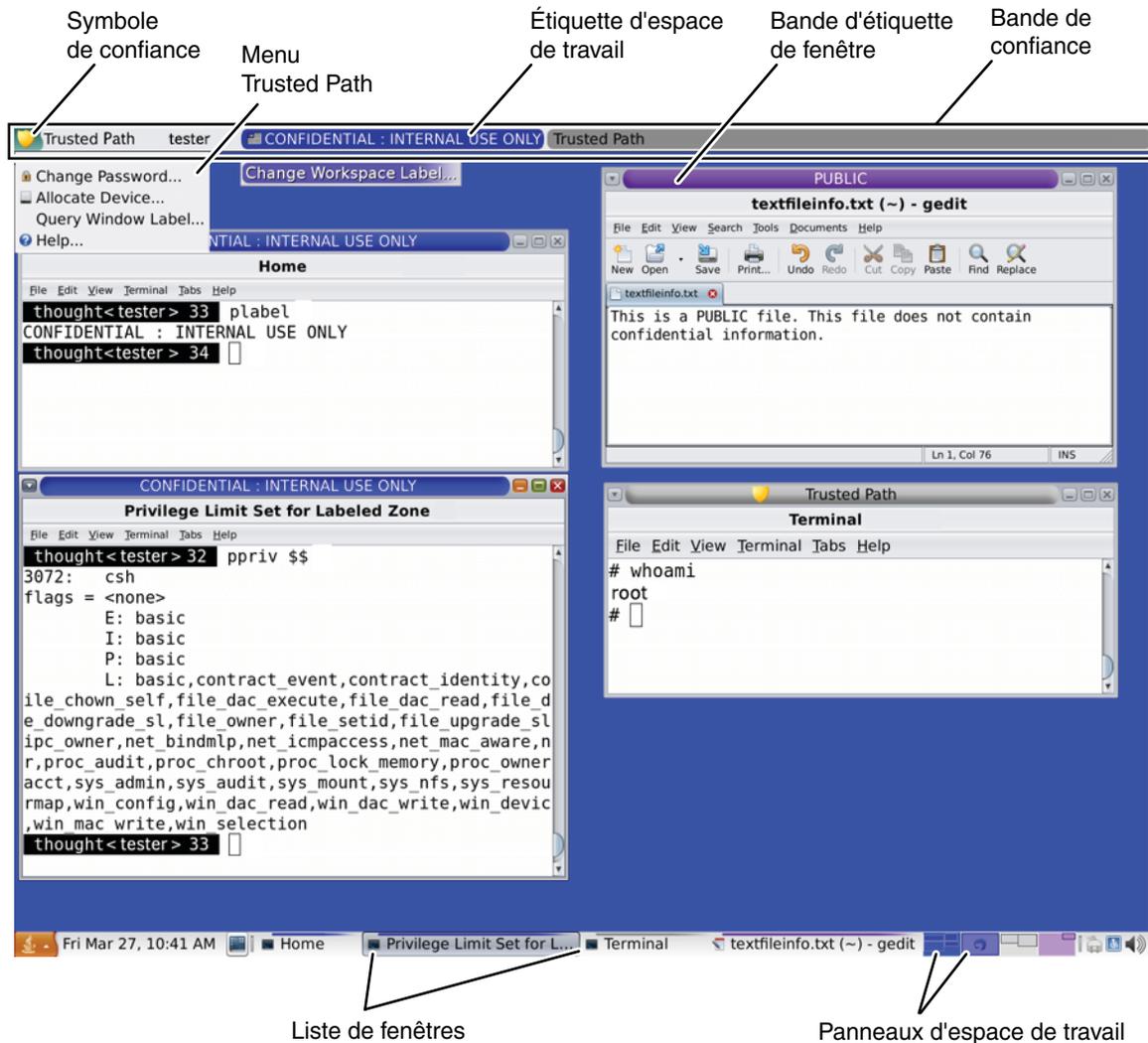
Les étiquettes peuvent être affichées dans la barre de titre des fenêtres et dans la *bande de confiance*, laquelle est une bande spéciale représentée à l'écran. La [Figure 1-4](#) présente une session Trusted Extensions multiniveau classique dans Trusted CDE. Les étiquettes et la bande de confiance sont indiquées.

FIGURE 1-4 Session Trusted CDE classique



La Figure 1-5 présente une session multiniveau classique de Trusted Extensions sur un système Trusted JDS. La bande de confiance se trouve en haut. Le menu Trusted Path (Chemin de confiance) est appelé à partir de la bande de confiance. Pour assumer un rôle, cliquez sur le nom d'utilisateur pour afficher le menu des rôles. Les commutateurs de l'espace de travail du panneau inférieur affichent la couleur de l'étiquette de l'espace de travail. Les icônes des fenêtres dans la liste des fenêtres du panneau inférieur affichent la couleur de l'étiquette de chaque fenêtre.

FIGURE 1-5 Session Trusted JDS classique



## Conteneurs et étiquettes

Trusted Extensions utilise des conteneurs pour l'étiquetage. Les conteneurs sont également appelés *zones*. La *zone globale* est une zone d'administration et n'est pas disponible pour les utilisateurs. Les zones non globales sont appelées *zones étiquetées*. Les zones étiquetées sont utilisées par les utilisateurs. La zone globale partage certains systèmes de fichiers avec des utilisateurs. Lorsque ces fichiers sont visibles dans une zone étiquetée, l'étiquette de ces fichiers est ADMIN\_LOW.

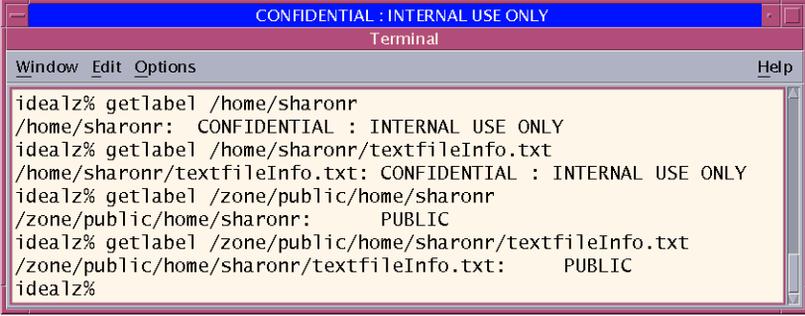
La communication réseau est limitée par étiquette. Par défaut, les zones ne peuvent pas communiquer les unes avec les autres car leurs étiquettes sont différentes. Par conséquent, une zone ne peut pas écrire dans une autre zone.

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

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

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

FIGURE 1-6 Affichage d'informations publiques à partir d'une zone d'étiquette supérieure



```
CONFIDENTIAL : INTERNAL USE ONLY
Terminal
Window Edit Options Help
idealz% getlabel /home/sharonr
/home/sharonr: CONFIDENTIAL : INTERNAL USE ONLY
idealz% getlabel /home/sharonr/textfileInfo.txt
/home/sharonr/textfileInfo.txt: CONFIDENTIAL : INTERNAL USE ONLY
idealz% getlabel /zone/public/home/sharonr
/zone/public/home/sharonr: PUBLIC
idealz% getlabel /zone/public/home/sharonr/textfileInfo.txt
/zone/public/home/sharonr/textfileInfo.txt: PUBLIC
idealz%
```

## Étiquettes et transactions

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

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

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

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

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

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

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

Considérez par exemple la figure suivante.

Classification	Compartiments
Top secret	A   B

Quatre étiquettes peuvent être créées à partir de ces composants :

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

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

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

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

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

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

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

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

Lorsque vous transférez des informations entre des fichiers possédant des étiquettes différentes, Trusted Extensions affiche une boîte de dialogue de confirmation vous demandant si vous êtes autorisé à modifier l'étiquette du fichier. Si vous n'êtes pas autorisé à le faire, Trusted Extensions n'autorise pas la transaction. L'administrateur de sécurité peut vous autoriser à augmenter ou réduire le niveau de sécurité d'informations. Pour plus d'informations, reportez-vous à la section [“Réalisation d'actions sécurisées”](#) à la page 57.

## Responsabilités des utilisateurs concernant la protection des données

En tant qu'utilisateur, il vous incombe de définir les droits d'accès destinés à protéger vos fichiers et répertoires. Les actions que vous pouvez effectuer pour définir les droits d'accès utilisent un mécanisme appelé contrôle d'accès discrétionnaire (DAC). Vous pouvez vérifier les droits d'accès à vos fichiers et répertoires à l'aide de la commande `ls -l` ou à l'aide du gestionnaire de fichiers (File Manager), comme décrit au [Chapitre 3, "Utilisation de Trusted Extensions \(tâches\)"](#).

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

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

## Trusted Extensions sépare les informations en fonction des étiquettes

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

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

## Sessions à niveau unique ou multiniveau

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

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

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

## Exemple de sélection de session

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

Les trois colonnes de gauche montrent la session de chaque utilisateur au moment de la connexion. Notez que les utilisateurs définissent une *étiquette de session* pour les sessions à niveau unique et une *autorisation de session* pour les sessions multiniveau. Le système affiche le [générateur d'étiquettes](#) approprié en fonction de votre sélection. Pour voir un générateur d'étiquettes pour une session multiniveau, reportez-vous à la [Figure 2-2](#).

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

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

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

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

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

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

## Espaces de travail étiquetés

Dans Solaris Trusted Extensions (CDE), ou Trusted CDE, les espaces de travail de Trusted Extensions sont accessibles via des boutons situés au centre du tableau de bord, comme dans le SE Solaris. Toutefois, avec Trusted Extensions, vous pouvez consacrer un espace de travail entier à une seule étiquette. Cette configuration est très pratique lorsque vous êtes dans une session multiniveau et ne souhaitez pas confondre les informations des différentes étiquettes. L'illustration suivante présente la zone de commutation de l'espace de travail avec quatre commutateurs. Chaque commutateur ouvre un espace de travail possédant une étiquette différente. Vous pouvez également assigner un ou plusieurs espaces de travail à la même étiquette.

FIGURE 1-7 Zone de commutation de l'espace de travail



Dans Solaris Trusted Extensions (JDS), ou Trusted JDS, les espaces de travail sont accessibles à l'aide des boutons situés à droite du panneau inférieur, comme le montre l'illustration suivante. Chaque espace de travail possède une étiquette.

FIGURE 1-8 Panneaux étiquetés



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

## Application du MAC pour les transactions par e-mail

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

## Suppression des données d'objets avant la réutilisation des objets

Trusted Extensions empêche la révélation involontaire d'informations sensibles en supprimant automatiquement les informations obsolètes des objets accessibles aux utilisateurs avant leur réutilisation. Par exemple, la mémoire et l'espace disque sont vidés avant d'être réutilisés. Si vous n'effacez pas les données sensibles avant la réutilisation d'un objet, les données risquent d'être révélées à des utilisateurs inappropriés. Par le biais de la libération de périphériques, Trusted Extensions efface tous les objets accessibles aux utilisateurs avant d'allouer les lecteurs à des processus. Notez cependant que vous devez effacer tous les supports de stockage amovibles tels que les DVD et disques JAZ avant d'autoriser un autre utilisateur à accéder au lecteur.

## Trusted Extensions active l'administration sécurisée

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

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

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

## Accès aux applications dans Trusted Extensions

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

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

L'utilisation de profils de droits contenant des programmes auxquels sont associés des attributs de sécurité permet d'éviter aux utilisateurs de faire un mauvais usage des données et d'endommager les données sur le système. Si vous avez besoin d'effectuer des tâches qui contournent la stratégie de sécurité, l'administrateur peut vous attribuer un profil de droits contenant les attributs de sécurité nécessaires. S'il vous est impossible d'exécuter une tâche en particulier, renseignez-vous auprès de votre administrateur. Il est possible que vous ne disposiez pas des attributs de sécurité requis.

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

---

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

---

## Administration par rôle dans Trusted Extensions

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

- Rôle root : principalement utilisé pour empêcher une connexion directe par un superutilisateur.
- Rôle d'administrateur principal : effectue toutes les tâches qui requièrent des privilèges allant au-delà des capacités des autres rôles.

- Rôle d'administrateur de sécurité : effectue les tâches liées à la sécurité, telles que l'autorisation de l'allocation de périphériques, l'attribution des profils de droits et l'évaluation des programmes logiciels.
- Rôle d'administrateur système : effectue des tâches courantes de gestion du système, telles que la mise en place des répertoires personnels et l'installation des logiciels.
- Rôle d'opérateur : effectue les sauvegardes système, gère les imprimantes et monte les supports amovibles.



## Connexion à Trusted Extensions (tâches)

---

Ce chapitre décrit les deux bureaux et le processus de connexion à un système configuré avec Solaris Trusted Extensions. Ce chapitre comprend les sections suivantes :

- “Bureaux et connexions dans Trusted Extensions” à la page 33
- “Processus de connexion à Trusted Extensions” à la page 34
- “Connexion à Trusted Extensions” à la page 36
- “Connexion à distance à Trusted Extensions” à la page 40

### Bureaux et connexions dans Trusted Extensions

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

Les bureaux sont des versions sécurisées de CDE (Common Desktop Environment) et de Sun Java Desktop System :

- Solaris Trusted Extensions (CDE) : version sécurisée de CDE. Ce bureau est utile pour les sessions à niveau unique ou multiniveau. Utilisez le bureau Trusted CDE si vous êtes familiarisé avec CDE ou si la stratégie du site exige que vous utilisiez ce bureau.
- Solaris Trusted Extensions (JDS) : version sécurisée de Java Desktop System, version *number*. Ce bureau est utile pour les sessions à niveau unique ou multiniveau. Trusted JDS inclut les fonctions d'accessibilité, par exemple un agrandisseur d'écran. Utilisez ce bureau si vous êtes familiarisé avec GNOME ou Java Desktop System, ou si la stratégie du site exige que vous utilisiez ce bureau. N'utilisez pas ce bureau si vous êtes autorisé à modifier l'étiquette des fichiers et si vous avez l'intention de glisser-déposer des fichiers pour modifier leur étiquette. Utilisez le bureau Trusted CDE pour glisser-déposer des fichiers afin de modifier leur étiquette.

L'écran de connexion n'est pas étiqueté. Le processus de connexion impose que vous établissiez une étiquette pour votre session. Une fois que vous avez choisi une étiquette, le bureau, ses

fenêtres et toutes les applications sont étiquetés. En outre, les applications qui affectent la sécurité sont visiblement protégées par un indicateur de chemin sécurisé.

## Processus de connexion à Trusted Extensions

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

1. **Choix du bureau** : comme dans le SE Solaris, vous choisissez le bureau à utiliser. Dans Trusted Extensions, vous devez choisir l'un des deux bureaux sécurisés.
2. **Identification** : comme dans le SE Solaris, vous tapez votre nom d'utilisateur dans le champ Username (Nom d'utilisateur).
3. **Authentification** : comme dans le SE Solaris, vous tapez votre mot de passe dans le champ Password (Mot de passe).  
La réussite de l'identification et de l'authentification confirme que vous êtes autorisé à utiliser le système.
4. **Vérification des messages et sélection du type de session** : examinez les informations dans la boîte de dialogue Last Login (Dernière connexion). Cette boîte de dialogue affiche l'heure de votre dernière connexion, les éventuels messages de l'administrateur et les attributs de sécurité de votre session. Si vous êtes autorisé à travailler sur plusieurs étiquettes, vous pouvez spécifier le type de session, à niveau unique ou multiniveau.

---

**Remarque** – Si votre compte vous empêche de travailler sur une étiquette, vous ne pouvez pas spécifier le type de session. Cette restriction est appelée configuration à *niveau unique* ou *étiquette unique*. Pour voir un exemple, reportez-vous à la section “[Exemple de sélection de session](#)” à la page 27.

---

5. **Sélection d'étiquette** : dans le [générateur d'étiquettes](#), choisissez le niveau de sécurité le plus élevé auquel vous avez l'intention de travailler pendant votre session.

---

**Remarque** – Par défaut, la connexion à distance n'est pas prise en charge pour les utilisateurs standard dans Trusted Extensions. Si la connexion à distance est prise en charge par votre site, contactez votre administrateur pour connaître la procédure. À partir de la version Solaris 10 5/09, un VNC (Virtual Network Computing) peut être utilisé pour afficher un bureau multiniveau à distance. Pour connaître la procédure, reportez-vous à la section “[Connexion à distance à Trusted Extensions](#)” à la page 40.

---

## Choix du bureau avant la connexion

Lorsqu'aucune session n'est en cours sur une station de travail Solaris, l'écran de connexion s'affiche. L'écran de connexion de Trusted Extensions est similaire à celui de Solaris. Comme dans l'écran de connexion de Solaris, vous pouvez choisir un bureau dans le menu Options.

## Identification et authentification lors de la connexion

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

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

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

## Vérification des attributs de sécurité lors de la connexion

L'examen des attributs de sécurité est géré par Trusted Extensions, et non par le SE Solaris. Avant la connexion, Trusted Extensions affiche la boîte de dialogue Last Login (Dernière connexion). Cette boîte de dialogue fournit des informations relatives au statut que vous pouvez examiner. Vous pouvez passer en revue ces informations passées, par exemple l'heure de votre dernière utilisation du système. Vous pouvez également consulter les attributs de sécurité en vigueur pour la prochaine session. Si votre compte est configuré pour fonctionner sous plusieurs étiquettes, vous pouvez sélectionner une session à niveau unique ou multiniveau.

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

## Connexion à Trusted Extensions

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

### ▼ Choix d'un bureau sécurisé

- 1 Dans l'écran de connexion, choisissez un bureau à partir du menu Options --> Sessions.
  - Pour Trusted CDE, choisissez Solaris Trusted Extensions (CDE).
  - Pour Trusted JDS, choisissez Solaris Trusted Extensions (JDS).
- 2 Passez à la section [“Identification et authentification auprès du système”](#) à la page 36.

### ▼ Identification et authentification auprès du système

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

Veillez à saisir le nom d'utilisateur exact que votre administrateur vous a attribué. Soyez particulièrement attentif à l'orthographe et aux majuscules.
- 2 Si vous avez fait une erreur, recommencez.
  - Pour saisir de nouveau votre nom d'utilisateur, cliquez sur Start Over (Recommencer).
  - Pour redémarrer entièrement le système de multifenêtrage, cliquez sur Reset Login (Réinitialiser la connexion) dans le menu Options.

Après le redémarrage, passez à la section [“Choix d'un bureau sécurisé”](#) à la page 36.
- 3 Validez votre saisie.

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



---

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

---

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

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

**Erreurs  
fréquentes**

Si le mot de passe que vous avez fourni est incorrect, une boîte de dialogue apparaît et affiche le message :

Login incorrect; please try again.

Cliquez sur OK pour fermer la boîte de dialogue. Ensuite, saisissez le mot de passe correct.

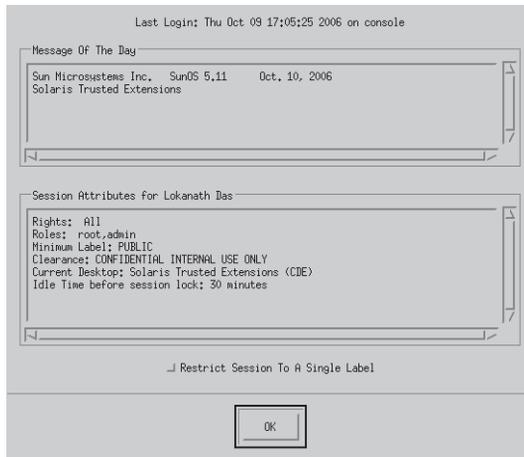
## ▼ Consultation des messages et sélection du type de session

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

**1 Dans la boîte de dialogue Last Login (Dernière connexion), vérifiez que l'heure de votre dernière session est exacte.**

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

FIGURE 2-1 Boîte de dialogue de dernière connexion



**2 Vérifiez la présence d'éventuels messages de l'administrateur.**

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

**3 Examinez les attributs de sécurité de votre session.**

Comme le montre la [Figure 2-1](#), la boîte de dialogue de dernière connexion indique les rôles que vous pouvez assumer, votre étiquette minimale et d'autres caractéristiques de sécurité.

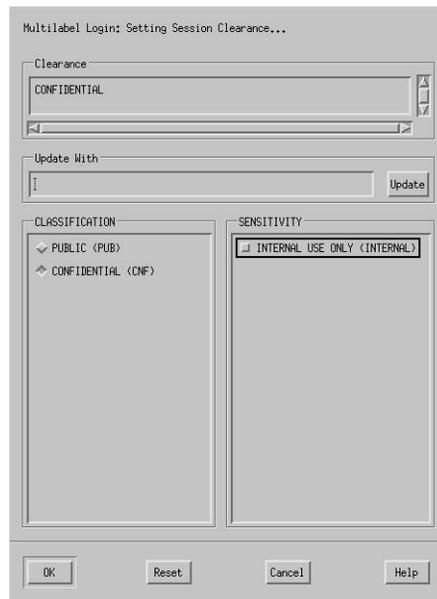
**4 (Facultatif) Si vous êtes autorisé à vous connecter à une session multiniveau, décidez si vous souhaitez une session à étiquette unique.**

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

Un générateur d'étiquettes apparaît. Si vous ouvrez une session à étiquette unique, le générateur d'étiquettes décrit votre étiquette de session. Dans un système multiniveau, le générateur d'étiquettes vous permet de choisir votre autorisation de session.

**5 Confirmez votre choix d'étiquette.**

FIGURE 2–2 Générateur d'étiquettes



- **Acceptez la valeur par défaut, sauf si vous avez une raison de ne pas le faire.**
  - **Pour une session multiniveau, sélectionnez une autorisation.**
    - Désélectionnez l'autorisation active et cliquez sur une classification et un niveau de sensibilité.
    - Ou, dans le champ Clearance (Autorisation), saisissez une autorisation.
    - Ou, dans le champ Update With (Mettre à jour avec), saisissez une étiquette.
  - **Pour une session à niveau unique, sélectionnez une étiquette.**
    - Désélectionnez l'étiquette active et cliquez sur une autre classification.
    - Ou, dans le champ Update With (Mettre à jour avec), saisissez une étiquette.
- 6 Cliquez sur OK.**
- Le bureau sécurisé que vous avez choisi, Trusted CDE ou Trusted JDS, s'affiche.

## ▼ Résolution des problèmes de connexion

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

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

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

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

- **Contactez votre administrateur système pour résoudre le problème.**

- **Si vous pouvez devenir l'utilisateur root, ouvrez une session de secours.**

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

Dans Trusted Extensions, la connexion de secours est protégée. Seul le superutilisateur peut accéder à la connexion de secours.

- a. **Comme dans le SE Solaris, choisissez Options -> Failsafe Session (Session de secours) dans l'écran de connexion.**

- b. **Lorsque vous y êtes invité, saisissez votre nom d'utilisateur et votre mot de passe.**

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

## Connexion à distance à Trusted Extensions

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

### ▼ Connexion à un bureau Trusted Extensions distant

**Avant de commencer**

Votre administrateur a exécuté les tâches de la section "Procédure d'utilisation de Xvnc afin d'accéder à distance à un système Trusted Extensions" du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

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

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

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

**2 Ouvrez une session.**

Suivez les procédures de la section [“Connexion à Trusted Extensions”](#) à la page 36.

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



## Utilisation de Trusted Extensions (tâches)

---

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

- “Sécurité visible du bureau dans Trusted Extensions” à la page 43
- “Processus de déconnexion de Trusted Extensions” à la page 44
- “Travail sur un système étiqueté” à la page 44
- “Réalisation d'actions sécurisées” à la page 57

### Sécurité visible du bureau dans Trusted Extensions

Trusted Extensions propose deux bureaux étiquetés : Solaris Trusted Extensions (CDE) et Solaris Trusted Extensions (JDS).

- Le bureau Solaris Trusted Extensions (CDE) s'affiche comme dans la [Figure 1-4](#).
- Le bureau Solaris Trusted Extensions (JDS) s'affiche comme dans la [Figure 1-5](#).

Un système configuré avec Trusted Extensions affiche la bande de confiance, sauf lors de l'ouverture de la session et du verrouillage de l'écran. Dans tous les autres cas, la bande de confiance est visible. Dans Trusted CDE, la bande apparaît en bas de l'écran. Dans Trusted JDS, la bande apparaît en haut de l'écran. Le symbole de confiance apparaît sur la bande de confiance lorsque vous interagissez avec la base informatique sécurisée. Lorsque vous modifiez votre mot de passe, par exemple, vous pouvez interagir avec la TCB.

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



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

Contactez immédiatement votre administrateur de sécurité. Pour déterminer quelle est la bande de confiance correcte, reportez-vous à la section “[Reprise du contrôle du focus actuel du bureau](#)” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

---

Pour plus d'informations sur les applications, les menus, les étiquettes et les caractéristiques du bureau, reportez-vous au [Chapitre 4, “Éléments de Trusted Extensions \(Référence\)”](#).

## Processus de déconnexion de Trusted Extensions

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

## Travail sur un système étiqueté



**Attention** – Si la bande de confiance est absente de votre espace de travail, contactez l'[administrateur de sécurité](#). Le problème de votre système pourrait être grave.

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

---

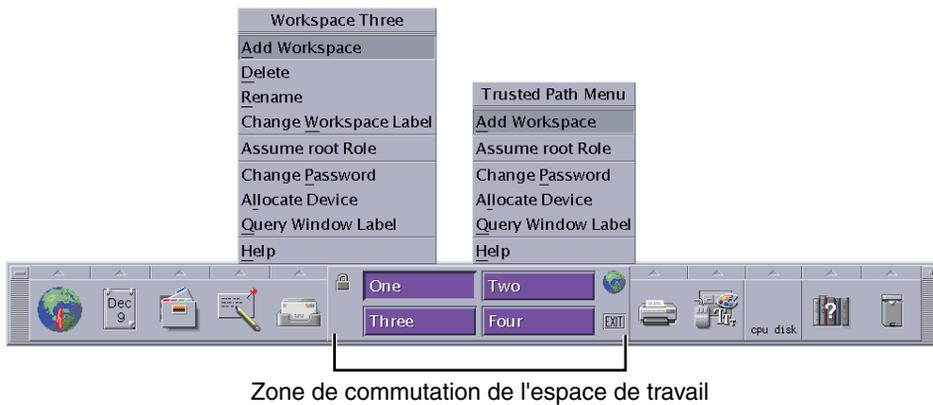
### ▼ Verrouillage et déverrouillage de l'écran

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

#### 1 Pour verrouiller votre écran, procédez de l'une des manières suivantes :

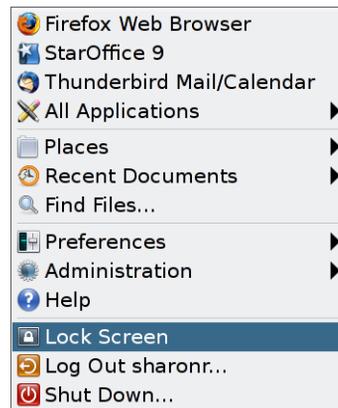
- Dans Trusted CDE, cliquez sur l'icône de verrouillage de l'écran dans la zone de commutation de l'espace de travail du tableau de bord.

FIGURE 3-1 Zone de commutation du tableau de bord



- Dans Trusted JDS, choisissez Lock Screen (Verrouillage de l'écran) dans le menu principal.

FIGURE 3-2 Sélection du verrouillage de l'écran



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

---

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

---

**2 Pour déverrouiller votre écran, procédez comme suit :**

- a. Déplacez le curseur de la souris jusqu'à ce que la boîte de dialogue Lock Screen (Verrouillage de l'écran) soit visible.**

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

- b. Saisissez votre mot de passe.**

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

## ▼ Déconnexion de Trusted Extensions

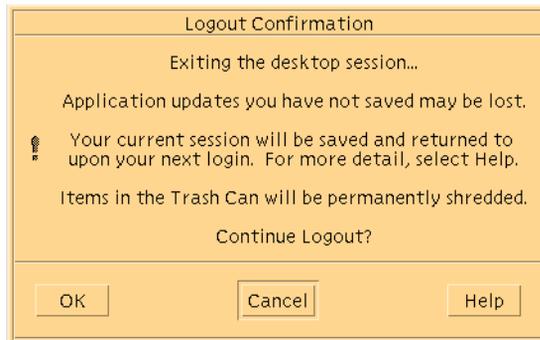
Sur la plupart des sites, l'écran se verrouille automatiquement après une période de veille spécifiée. Si vous prévoyez d'être absent plus longtemps ou si vous pensez qu'une autre personne va travailler sur votre poste, déconnectez-vous.

**1 Pour vous déconnecter, procédez de l'une des manières suivantes :**

- **Dans Trusted CDE, cliquez sur l'icône EXIT dans la zone de commutation de l'espace de travail du tableau de bord.**

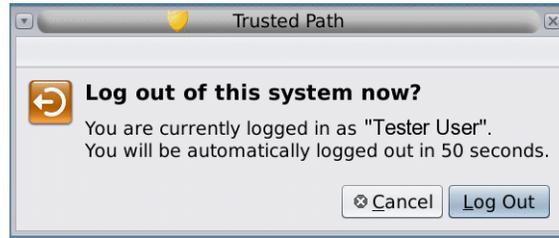
Pour voir une illustration du tableau de bord, reportez-vous à la [Figure 3-1](#).

La boîte de dialogue de confirmation de déconnexion (Logout Confirmation) s'affiche.



- Dans **Trusted JDS**, choisissez **Log Out** *vosre nom* dans le menu principal.

La boîte de dialogue de confirmation de déconnexion (Logout Confirmation) s'affiche.



- 2 Confirmez la déconnexion ou cliquez sur Annuler.

## ▼ Procédure d'arrêt du système

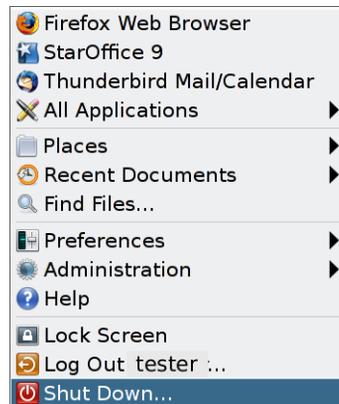
La déconnexion est la manière habituelle de mettre fin à une session Trusted Extensions. Utilisez la procédure suivante pour arrêter votre station de travail.

---

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

---

- Pour arrêter le système, procédez de l'une des manières suivantes :
  - Dans **Trusted JDS**, choisissez **Shut Down (Arrêt)** dans le menu principal. Confirmez l'arrêt.



- Dans Trusted CDE, choisissez **Suspend System (Interrompre le système)** dans le menu de l'espace de travail.

Cliquez avec le bouton 3 de la souris sur l'arrière-plan pour ouvrir le menu.

a. **Confirmez ce que vous voulez faire.**

- Cliquez sur **Shutdown (Arrêter)** pour arrêter le système.
- Cliquez sur **Suspend (Interrompre)** pour mettre votre système en mode d'économie d'énergie.
- Dans le cas contraire, cliquez sur **Annuler**.

---

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

---

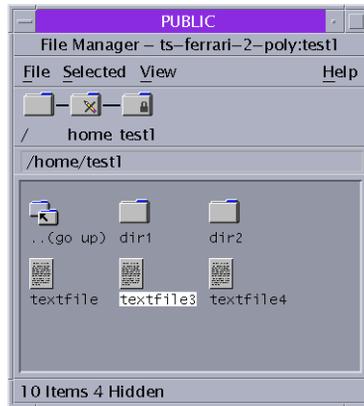
## ▼ **Procédure d'affichage de vos fichiers dans un espace de travail étiqueté**

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

- 1 **Dans un espace de travail Trusted CDE, ouvrez une fenêtre de terminal ou le gestionnaire de fichiers.**
  - **Ouvrez une fenêtre de terminal et répertoriez le contenu de votre répertoire personnel.**

Cliquez avec le bouton 3 de la souris sur l'arrière-plan. Dans le menu de l'espace de travail, sélectionnez **Programs -> Terminal (Programmes -> Terminal)**.
  - **Dans le tableau de bord, cliquez sur File Manager (Gestionnaire de fichiers).**

FIGURE 3-3 Gestionnaire de fichiers étiqueté



Le gestionnaire de fichiers s'affiche avec le contenu de votre répertoire personnel correspondant à cette étiquette.

Le gestionnaire de fichiers reprend l'étiquette de l'espace de travail actif. L'application permet d'accéder uniquement aux fichiers qui possèdent la même étiquette. Pour plus de détails sur l'affichage de fichiers de différentes étiquettes, reportez-vous à la section [“Conteneurs et étiquettes”](#) à la page 22.

- 2 Dans un espace de travail Trusted JDS, ouvrez une fenêtre de terminal ou le navigateur de fichiers.
  - **Ouvrez une fenêtre de terminal et répertoriez le contenu de votre répertoire personnel.**  
Cliquez avec le bouton 3 de la souris sur l'arrière-plan. Dans le menu, choisissez Open Terminal (Ouvrir un terminal).
  - **Double-cliquez sur le dossier Documents ou sur le dossier This Computer (Poste de travail) sur votre bureau.**  
Ces dossiers s'ouvrent dans un navigateur de fichiers. Le navigateur de fichiers s'ouvre avec la même étiquette que l'espace de travail actif. L'application permet d'accéder uniquement aux fichiers qui possèdent la même étiquette. Pour plus de détails sur l'affichage de fichiers de différentes étiquettes, reportez-vous à la section [“Conteneurs et étiquettes”](#) à la page 22.

## ▼ Procédure d'accès aux pages de manuel Trusted Extensions

- 1 Dans les versions Solaris 10 11/06 et Solaris 10 8/07 de Solaris Trusted Extensions, consultez la page de manuel [Intro\(3TSOL\)](#).

- a. Ouvrez une fenêtre de terminal.

- Dans Trusted CDE, cliquez avec le bouton 3 de la souris sur l'arrière-plan. Sélectionnez ensuite Programs -> Terminal (Programmes -> Terminal).
- Dans Trusted JDS, cliquez avec le bouton 3 de la souris sur l'arrière-plan. Choisissez ensuite Open Terminal (Ouvrir un terminal).

- b. Ouvrez la page de manuel d'introduction à Trusted Extensions.

```
% man -s 3tsol intro
```

Pour obtenir la liste des commandes utilisateur spécifiques à Trusted Extensions, reportez-vous à l'Annexe B, “Liste des pages de manuel Trusted Extensions” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

Les pages de manuel sont également disponibles à partir du site [Web de documentation](http://www.oracle.com/technetwork/indexes/documentation/index.html) (<http://www.oracle.com/technetwork/indexes/documentation/index.html>) d'Oracle.

- 2 Depuis la version Solaris 10 5/08, ouvrez la page de manuel [trusted\\_extensions\(5\)](#) dans une fenêtre de terminal.

```
% man trusted_extensions
```

Pour obtenir la liste des commandes utilisateur spécifiques à Trusted Extensions, reportez-vous à l'Annexe B, “Liste des pages de manuel Trusted Extensions” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*.

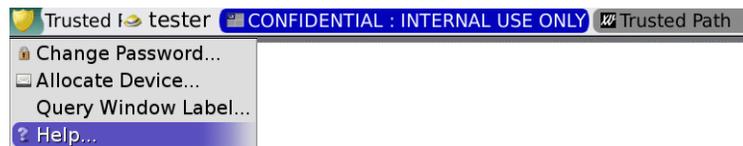
## ▼ Procédure d'accès à l'aide en ligne de Trusted Extensions

- 1 Dans Trusted CDE, cliquez sur l'icône d'aide du tableau de bord.

FIGURE 3-4 Aide en ligne de Trusted Extensions



- a. Cliquez sur le bouton Index.
  - b. Dans l'index, recherchez dans le mot `Trusted` dans All Volumes (Tous les volumes).
  - c. Cliquez sur les liens afin de trouver l'aide spécifique à Trusted Extensions.
- 2 Dans Trusted JDS, cliquez sur Help (Aide) dans le menu Trusted Path (Chemin de confiance).
    - Pour ouvrir le menu Trusted Path, cliquez sur le symbole de confiance à gauche de la bande de confiance.



- Pour trouver une aide spécifique à une tâche, cliquez sur le bouton d'aide dans l'application sécurisée que vous utilisez actuellement, par exemple le gestionnaire de périphériques.

## ▼ Procédure de personnalisation du menu Workspace de CDE

Dans Trusted CDE, les utilisateurs et les rôles peuvent personnaliser le menu Workspace (Espace de travail) pour chaque étiquette.

- 1 **Dans votre espace de travail actif, commencez à personnaliser le menu Workspace (Espace de travail).**
  - **Pour ajouter une ou plusieurs options au menu, choisissez l'option Add Item to Menu (Ajouter l'option au menu).**

Une boîte de dialogue contenant un bouton Browse (Parcourir) s'affiche.
  - **Pour modifier le menu ou les propriétés du menu, choisissez l'option Customize Menu (Personnaliser le menu).**

Un gestionnaire de fichiers s'affiche.
- 2 **Pour ajouter des options au menu Workspace, procédez comme suit :**
  - a. **Pour chaque programme, recherchez le programme et ajoutez-le.**

Cliquez sur le bouton Browse (Parcourir) pour afficher les fichiers disponibles pour cet espace de travail avec cette étiquette.
  - b. **Sélectionnez le programme.**
  - c. **Fermez la fenêtre.**

Les options sont ajoutées en haut du menu Workspace.
- 3 **Pour modifier le menu Workspace, procédez comme suit :**
  - **Pour supprimer une option de menu, cliquez avec le bouton 3 de la souris sur l'option, puis cliquez sur Put in Trash (Mettre à la corbeille).**
  - **Pour modifier les propriétés telles que les autorisations, cliquez avec le bouton 3 de la souris sur l'élément, puis cliquez sur Properties (Propriétés).**

Vous pouvez modifier les autorisations ici. Vous pouvez également consulter les informations relatives au fichier et à l'étiquette de sensibilité du fichier.
- 4 **Confirmez les modifications apportées au menu ou annulez.**
  - **Pour confirmer les modifications, choisissez File -> Update Workspace Menu (Fichier -> Mettre à jour le menu espace de travail).**

Le menu Workspace reflète vos modifications.
  - **Pour annuler vos modifications, choisissez File -> Close (Fichier -> Fermer).**

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

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

### Avant de commencer

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

Consultez votre administrateur lorsque vous modifiez ces fichiers.

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

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

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

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

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

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

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

### Exemple 3-1 Création d'un fichier `.copy_files`

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

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

### Exemple 3-2 Création d'un fichier .link\_files

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

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

#### Erreurs fréquentes

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

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

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

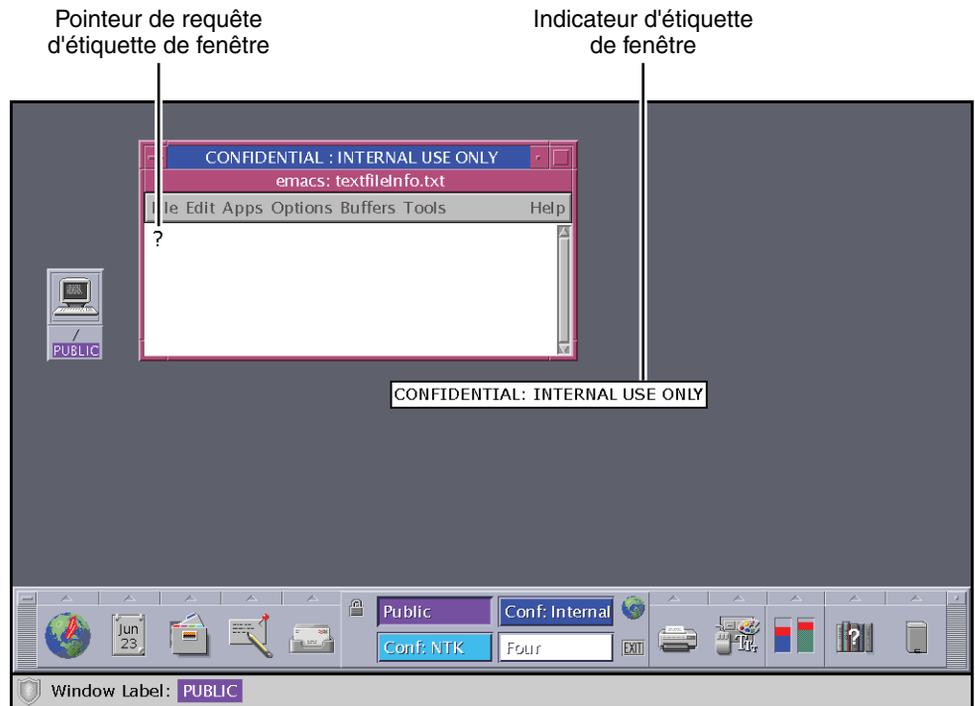
### 1 Choisissez Query Window Label (Requête d'étiquette de fenêtre) dans le menu Trusted Path.

Le pointeur se transforme en un point d'interrogation.

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

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

FIGURE 3-5 Opération de requête d'étiquette de fenêtre



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

## ▼ Exécution de certaines tâches de bureau courantes dans Trusted Extensions

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

- Vidage de la corbeille
- Recherche d'événements du calendrier
- Dans Trusted CDE, restauration du tableau de bord et utilisation du gestionnaire de style

## 1 Videz la corbeille.

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

### ■ Dans Trusted CDE, ouvrez la corbeille sur le tableau de bord.

Choisissez File -> Select All (Fichier -> Tout sélectionner), puis File -> Shred (Fichier -> Broyer). Ensuite, confirmez.

### ■ Dans Trusted JDS, cliquez avec le bouton 3 de la souris sur l'icône de la corbeille sur le bureau.

Choisissez Empty Trash (Vider la Corbeille), puis confirmez.

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

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

### ■ Dans une session multiniveau, ouvrez votre calendrier à partir d'un espace de travail possédant une étiquette différente.

### ■ Dans une session à niveau unique, déconnectez-vous. Ensuite, connectez-vous à une étiquette différente pour afficher les événements du calendrier de cette étiquette.

## 3 Dans Trusted CDE, restaurez le tableau de bord en cliquant sur la bande de confiance.

Le tableau de bord réduit est restauré.

## 4 Sur les deux bureaux, enregistrez un bureau personnalisé pour chaque étiquette.

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

### a. Configurez le bureau.

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

---

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

---

### b. Enregistrez l'espace de travail actif.

#### ■ Dans Trusted CDE, ouvrez le gestionnaire de style (Style Manager). Choisissez vos paramètres dans l'icône de démarrage.

---

**Remarque** – Le gestionnaire de style requiert le chemin de confiance. Exécutez le gestionnaire de style à partir du tableau de bord ou du menu Workspace (Espace de travail), dans lequel le gestionnaire de style possède le chemin de confiance.

---

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

- **Dans Trusted JDS, lorsque vous vous déconnectez, choisissez d'enregistrer la configuration active.**

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

- **Dans Trusted JDS, cliquez sur le menu principal.**

- i. Cliquez sur **Preferences > Sessions (Préférences > Sessions)**.

- ii. Cliquez sur le bouton **Session Options (Options de session)**.

- iii. Cliquez sur **Remember currently running (Mémoire des applications en cours d'exécution)**, puis fermez la boîte de dialogue.

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

## Réalisation d'actions sécurisées

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




---

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

---

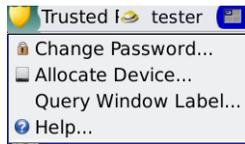
### ▼ Procédure de modification du mot de passe dans Trusted Extensions

Contrairement au SE Solaris, Trusted Extensions fournit une interface graphique pour modifier votre mot de passe. L'interface graphique prend le contrôle du pointeur jusqu'à ce que l'opération sur le mot de passe soit terminée. Pour arrêter un processus qui a saisi le pointeur de la souris, reportez-vous à la section “[Reprise du contrôle du focus actuel du bureau](#)” du [Procédures de l'administrateur Oracle Solaris Trusted Extensions](#).

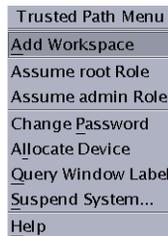
## 1 Choisissez l'option Change Password (Modifier le mot de passe) dans le menu Trusted Path.

- Dans Trusted JDS, cliquez sur Trusted Path dans la bande de confiance.

FIGURE 3-6 Menu Trusted Path



- Dans Trusted CDE, ouvrez le menu Trusted Path à partir du centre du tableau de bord.



## 2 Saisissez votre mot de passe actuel.

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



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

## 3 Saisissez le nouveau mot de passe.

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

## ▼ Procédure de connexion à une étiquette différente

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

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

**Avant de commencer**

Vous devez être connecté à une session multiniveau.

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

Pour plus d'informations, reportez-vous à la section “[Procédure d'ajout d'un espace de travail possédant une étiquette particulière](#)” à la page 65.

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

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

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

Pour plus d'informations, reportez-vous à la section “[Exécution de certaines tâches de bureau courantes dans Trusted Extensions](#)” à la page 55.

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

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

**Avant de commencer**

Vous devez être autorisé pour allouer un périphérique.

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

Ou, dans Trusted CDE, ouvrez le gestionnaire d'allocation de périphériques (Device Allocation Manager) à partir du sous-panneau Tools (Outils) du tableau de bord.

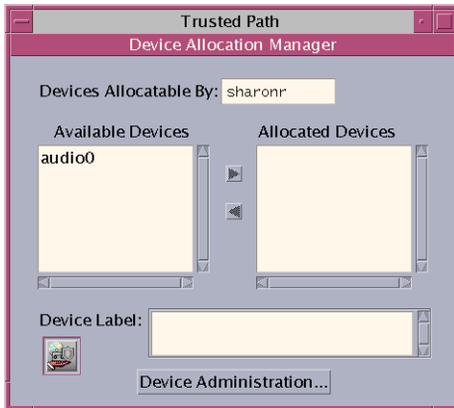
FIGURE 3-7 Icône d'allocation de périphériques dans Trusted CDE

Allocation  
de périphériques



Le gestionnaire d'allocation de périphériques s'affiche. Dans Solaris Trusted Extensions (JDS), cette interface graphique est appelée gestionnaire de périphériques (Device Manager).

FIGURE 3-8 Gestionnaire d'allocation de périphériques



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

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

- `audio0` : indique un microphone et un haut-parleur
- `cdrom0` : indique un lecteur de CD-ROM
- `floppy0` : indique un lecteur de disquette
- `mag_tapen` : indique un lecteur de bande (transmission en continu)
- `rmdiskn` : indique un disque amovible, tel qu'un disque ZIP, JAZ ou un support USB enfichable à chaud

## 3 Sélectionnez le périphérique.

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

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

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

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

#### 4 Suivez les instructions.

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

FIGURE 3-9 Instructions relatives à l'utilisation d'un microphone



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

#### Exemple 3-3 Chargement des supports amovibles pour lire un système de fichiers

Dans cet exemple, un utilisateur souhaite charger des informations sur son système à partir d'un CD-ROM étiqueté SECRET. Il est autorisé à allouer le CD-ROM.

Tout d'abord, il crée un espace de travail possédant l'étiquette SECRET. Dans cet espace de travail, il ouvre le gestionnaire d'allocation de périphériques et alloue le lecteur de CD-ROM. Il insère ensuite le CD et répond yes (oui) à la requête de montage.

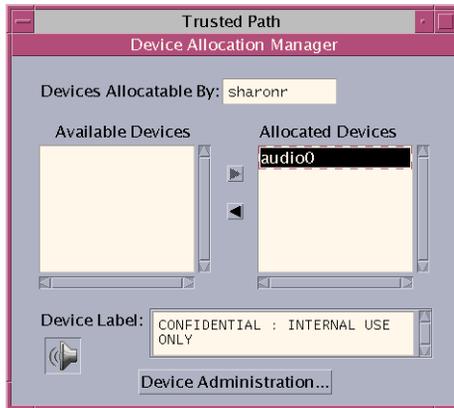
Le logiciel monte le CD et le gestionnaire de fichiers s'affiche. Le répertoire actif est défini sur le point de montage.

#### Exemple 3-4 Allocation d'un périphérique audio

Dans cet exemple, un utilisateur alloue le périphérique audio sur son système. Lorsqu'il déplace le périphérique audio vers la liste des périphériques alloués, le message suivant s'affiche :



Le périphérique est alloué à l'étiquette Confidential : Internal Use Only. L'utilisateur visualise l'étiquette lorsqu'il sélectionne le périphérique dans la liste des périphériques alloués.



Une fois que l'utilisateur a terminé d'utiliser le périphérique audio, il le libère. Le système lui rappelle de désactiver le microphone.



### Erreurs fréquentes

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

Si vous passez à l'espace de travail d'un rôle différent ou à un espace de travail d'étiquette différente, le périphérique alloué ne peut pas fonctionner. Pour utiliser le périphérique avec la nouvelle étiquette, vous devez libérer le périphérique au niveau de l'étiquette initiale, puis l'allouer à la nouvelle étiquette. Dans Trusted CDE, lorsque vous utilisez la commande Occupy Workspace (Occuper l'espace de travail) dans le menu de la fenêtre pour déplacer le gestionnaire d'allocation de périphériques vers le nouvel espace de travail, les listes de périphériques disponibles et de périphériques alloués changent pour refléter le contexte correct. Le gestionnaire de périphériques dans Trusted JDS fonctionne de la même manière lorsque vous déplacez l'interface graphique vers un espace de travail possédant une autre étiquette.

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

## ▼ Procédure de libération d'un périphérique dans Trusted Extensions

- 1 Libérez le périphérique.
  - a. Accédez à l'espace de travail dans lequel le gestionnaire d'allocation de périphériques est affiché.
  - b. Déplacez le périphérique à libérer de la liste des périphériques alloués.
- 2 Retirez le support.
- 3 Cliquez sur OK dans la boîte de dialogue Deallocation (Libération).

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

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

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

- 1 Ouvrez le menu Trusted Path (Chemin de confiance).
  - Dans Solaris Trusted Extensions (CDE), cliquez au centre du tableau de bord.

Si un rôle vous a été affecté par l'administrateur de sécurité, le menu Trusted Path inclut une option de menu permettant d'adopter un rôle (Assume *nom\_du\_rôle* Role).

Sélectionnez Assume *nom\_du\_rôle* Role (Assumer le rôle *nom\_du\_rôle*).
  - Dans Solaris Trusted Extensions (JDS), cliquez sur votre nom d'utilisateur à droite du symbole de confiance.

Choisissez le nom du rôle dans le menu.
- 2 Tapez le mot de passe du rôle et appuyez sur la touche Entrée.

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



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

Une fois le mot de passe du rôle accepté, le logiciel vous place dans un espace de travail du rôle. Dans Trusted JDS, l'espace de travail actif devient l'espace de travail du rôle. Dans Trusted CDE, un nouvel espace de travail est créé pour le rôle. Vous êtes dans la zone globale. Vous pouvez effectuer les tâches autorisées par les profils de droits de votre rôle.

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

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

Utilisez la procédure décrite ci-dessous pour travailler avec une étiquette différente dans le même espace de travail. Pour créer un espace de travail possédant une étiquette différente, reportez-vous à la section “[Procédure d'ajout d'un espace de travail possédant une étiquette particulière](#)” à la page 65.

### Avant de commencer

Vous devez être connecté à une session multiniveau.

#### 1 Modifiez l'étiquette de votre espace de travail actif.

- **Dans Trusted CDE, cliquez avec le bouton 3 de la souris sur le bouton de l'espace de travail.**

Dans le menu, choisissez Change Workspace Label (Modifier l'étiquette de l'espace de travail).

- **Dans Trusted JDS, cliquez sur l'étiquette de la fenêtre dans la bande de confiance.**

Cliquez sur Change Workspace Label.



#### 2 Sélectionnez une étiquette dans le générateur d'étiquettes.

L'étiquette de l'espace de travail est remplacée par la nouvelle étiquette. Les fenêtres et les applications qui ont été appelées avant la modification de l'étiquette continuent de s'exécuter avec l'étiquette précédente. La bande de confiance renseigne sur la nouvelle étiquette. Dans un

système dans lequel les étiquettes sont assorties d'une couleur, les nouvelles fenêtres sont représentées à l'aide de la nouvelle couleur. Dans Trusted CDE, le bouton de l'espace de travail utilise un affichage coloré. Dans Trusted JDS, le panneau utilise un affichage coloré.

## ▼ Procédure d'ajout d'un espace de travail possédant une étiquette particulière

La possibilité de définir les étiquettes des espaces de travail dans Trusted Extensions offre un moyen pratique de travailler avec différentes étiquettes au cours d'une même session. Sur les deux bureaux, vous pouvez ajouter un espace de travail possédant votre étiquette minimum. Dans Trusted CDE, vous pouvez ajouter un espace de travail possédant la même étiquette qu'un espace de travail existant.

---

**Astuce** – Dans Trusted CDE, renommez chaque bouton d'espace de travail afin d'y faire figurer l'étiquette de l'espace de travail concerné.

---

Pour modifier l'étiquette de l'espace de travail actif, reportez-vous à la section [“Procédure de modification de l'étiquette d'un espace de travail”](#) à la page 64.

### Avant de commencer

Vous devez être connecté à une session multiniveau.

- 1 **Dans Trusted JDS, pour créer un espace de travail possédant votre étiquette minimum, effectuez les opérations suivantes :**
  - a. Cliquez avec le bouton 3 de la souris sur un panneau de l'espace de travail.
  - b. Dans le menu, choisissez Preferences (Préférences).
  - c. Augmentez le numéro figurant dans le champ Number of Workspaces (Nombre d'espaces de travail).

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

---

**Remarque** – Dans Trusted JDS, pour ajouter un espace de travail possédant une étiquette différente, sélectionnez un panneau d'espace de travail et modifiez son étiquette. Pour plus d'informations, reportez-vous à la section [“Procédure de modification de l'étiquette d'un espace de travail”](#) à la page 64.

---

- 2 Dans Trusted CDE, pour créer un espace de travail possédant votre étiquette minimum, effectuez les opérations suivantes :
  - a. Cliquez avec le bouton 3 de la souris sur la zone de commutation de l'espace de travail.
  - b. Dans le menu, choisissez Add Workspace (Ajouter un espace de travail).  
L'espace de travail est créé avec votre étiquette minimum.
  - c. (Facultatif) Renommez l'espace de travail.
- 3 Dans Trusted CDE, pour créer un espace de travail possédant la même étiquette qu'un espace de travail existant, procédez comme suit :
  - a. Cliquez avec le bouton 3 de la souris sur le bouton de l'espace de travail souhaité.
  - b. Dans le menu, choisissez Add Workspace (Ajouter un espace de travail).  
L'espace de travail créé possède la même étiquette que le bouton de l'espace de travail.

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

- Pour passer à un espace de travail existant, procédez de l'une des manières suivantes :
  - Dans Trusted CDE, cliquez sur le commutateur de l'espace de travail possédant cette étiquette.

FIGURE 3–10 Tableau de bord avec les commutateurs affichant les différentes étiquettes



- Dans Trusted JDS, cliquez sur le panneau de l'espace de travail dans l'affichage des panneaux.



Vous vous trouvez à présent dans cet espace de travail étiqueté.

**Erreurs fréquentes**

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

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

Les fenêtres qui sont déplacées vers un autre espace de travail conservent leur étiquette d'origine. Les actions effectuées dans ces fenêtres sont réalisées au niveau de l'étiquette de la fenêtre et non au niveau de l'étiquette de l'espace de travail. Le déplacement d'une fenêtre est utile pour comparer des informations. Vous pouvez aussi vouloir utiliser des applications à différents niveaux d'étiquette sans avoir à changer d'espace de travail.

- Pour déplacer une fenêtre vers un espace de travail différent, effectuez l'une des opérations suivantes :
  - Dans Trusted CDE, utilisez le menu **Occupy Workspace (Occuper l'espace de travail)**.
    - a. Depuis le menu de la fenêtre de l'application, choisissez **Occupy Workspace**.

FIGURE 3-11 Menu Occupy Workspace dans Trusted CDE

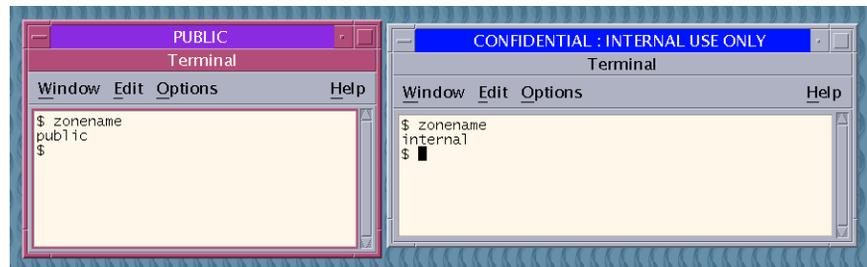


- b. Choisissez un espace de travail possédant une étiquette différente, puis cliquez sur **OK**.

Cette action déplace l'application vers un espace de travail possédant une étiquette différente. Notez que la boîte de dialogue **Occupy Workspace** possède l'étiquette **Trusted Path** (Chemin de confiance). Cette étiquette indique que l'occupation d'un espace de travail affecte la base informatique sécurisée.

La figure suivante illustre deux fenêtres de terminal possédant des étiquettes différentes dans un même espace de travail.

FIGURE 3–12 Fenêtres possédant des étiquettes différentes dans un seul espace de travail



- Dans Trusted JDS, dans l'affichage des panneaux, faites glisser la fenêtre à partir du panneau de son espace de travail d'origine vers un autre panneau.

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

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

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

- 1 Dans Trusted CDE, utilisez le gestionnaire de fichiers (File Manager) pour déterminer l'étiquette du fichier.
  - Dans le gestionnaire de fichiers, sélectionnez le fichier, puis choisissez l'option de menu File -> Properties (Fichier -> Propriétés).  
Lisez la valeur de la propriété Sensitivity Label (Étiquette de sensibilité) du fichier.
  - Vous pouvez également faire glisser le fichier du gestionnaire de fichiers qui le contient vers le bureau.  
L'icône du fichier affiche l'étiquette du fichier.
- 2 Dans Trusted JDS, utilisez le navigateur de fichiers (File Browser).

---

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

---

## ▼ Procédure de déplacement de données entre les étiquettes

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

### Avant de commencer

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

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

- “Procédure d’octroi de l’autorisation de modifier l’étiquette de fichiers à un utilisateur” du *Procédures de l’administrateur Oracle Solaris Trusted Extensions*
- “Procédure d’octroi de l’autorisation de modifier le niveau de sécurité de données à un utilisateur” du *Procédures de l’administrateur Oracle Solaris Trusted Extensions*

Vous devez être connecté à une session multiniveau.

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

Pour plus d'informations, reportez-vous à la section “[Procédure d'ajout d'un espace de travail possédant une étiquette particulière](#)” à la page 65.

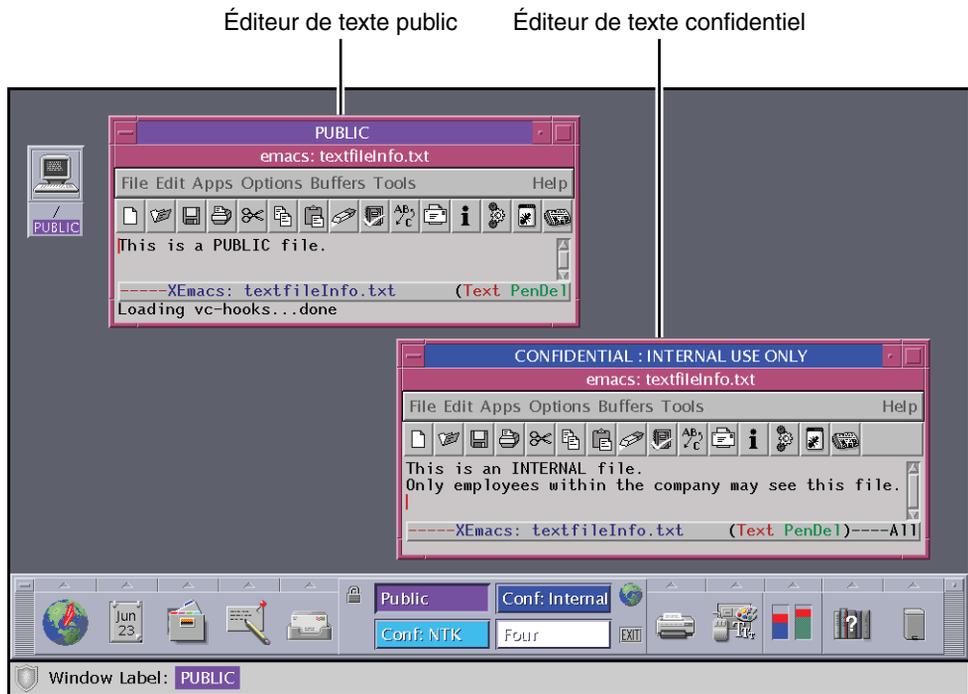
### 2 Confirmez l'étiquette du fichier source.

Pour plus d'informations, reportez-vous à la section “[Procédure de détermination de l'étiquette d'un fichier](#)” à la page 68.

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

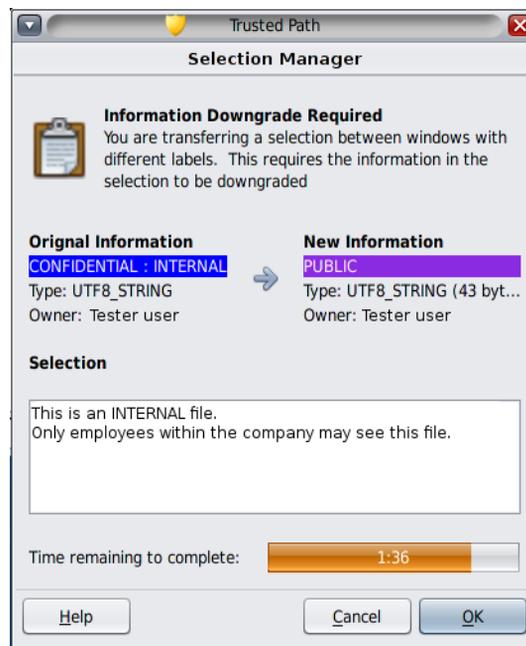
Pour plus d'informations, reportez-vous à la section “[Procédure de déplacement d'une fenêtre vers un autre espace de travail](#)” à la page 67. La figure suivante représente deux éditeurs possédant des étiquettes différentes dans le même espace de travail.

FIGURE 3-13 Applications possédant des étiquettes différentes dans un même espace de travail



- 4 Mettez en surbrillance les informations à déplacer et collez la sélection dans la fenêtre cible. La boîte de dialogue de confirmation du gestionnaire de sélection s'affiche.

FIGURE 3-14 Boîte de dialogue de confirmation du gestionnaire de sélection dans Trusted JDS

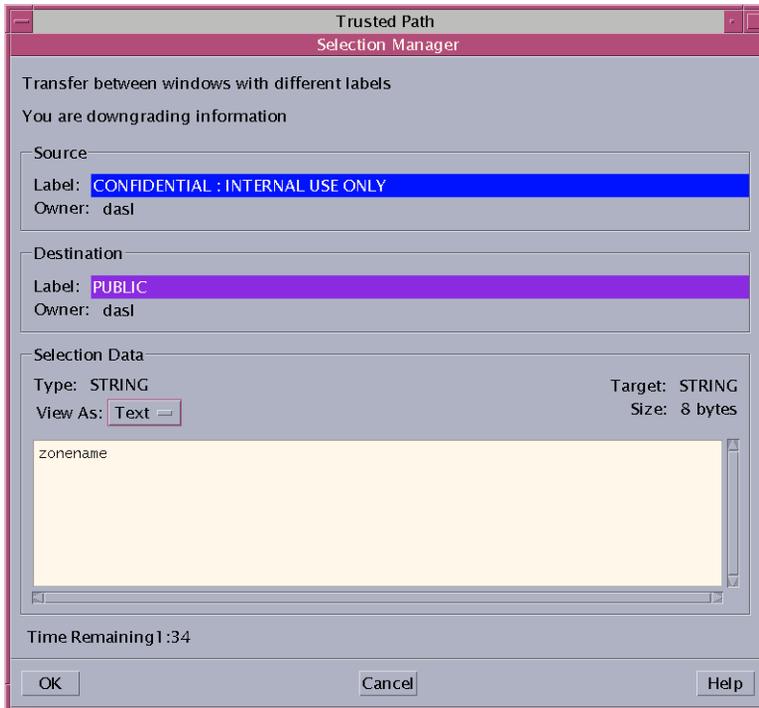


## 5 Examinez la boîte de dialogue de confirmation du gestionnaire de sélection.

Cette boîte de dialogue :

- explique pourquoi la confirmation de la transaction est nécessaire ;
- identifie l'étiquette et le propriétaire du fichier source ;
- identifie l'étiquette et le propriétaire du fichier cible ;
- identifie le type de données sélectionnées pour le transfert, le type du fichier cible et la taille des données en octets. Par défaut, les données sélectionnées sont visibles sous forme de texte ;
- indique le temps restant jusqu'à l'achèvement de la transaction. La durée et l'utilisation du chronomètre dépendent de la configuration de votre site.

FIGURE 3-15 Boîte de dialogue de confirmation du gestionnaire de sélection dans Trusted CDE



- 6 (Facultatif) Dans le menu **View As** (Afficher comme), choisissez la façon dont vous souhaitez afficher les informations source.
  - Choisissez hexadécimal pour visualiser les données au format hexadécimal.
  - Choisissez **None** (Aucun) pour masquer entièrement les données.  
En modifiant le paramétrage du menu **View As**, vous modifiez l'affichage des transferts suivants. Choisissez **None** pour les sélections qui se composent de données illisibles.
- 7 Confirmez que vous souhaitez modifier l'étiquette des données.
  - Cliquez sur **Annuler** pour arrêter la transaction.
  - Sinon, cliquez sur **OK**.

## ▼ Procédure de déplacement de fichiers entre les étiquettes dans Trusted CDE

Comme sur un système Solaris standard, vous pouvez déplacer les fichiers dans Trusted Extensions. Lorsque vous déplacez un fichier vers une autre étiquette, vous augmentez ou réduisez la sensibilité des informations contenues dans le fichier.

### Avant de commencer

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

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

- “Procédure d'octroi de l'autorisation de modifier l'étiquette de fichiers à un utilisateur” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*
- “Procédure d'octroi de l'autorisation de modifier le niveau de sécurité de données à un utilisateur” du *Procédures de l'administrateur Oracle Solaris Trusted Extensions*

Vous devez être connecté à une session multiniveau dans Trusted CDE. Le fichier que vous souhaitez déplacer doit être fermé. Vérifiez que personne d'autre n'utilise ce fichier.

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

Pour plus d'informations, reportez-vous à la section “[Procédure d'ajout d'un espace de travail possédant une étiquette particulière](#)” à la page 65.

#### 2 Ouvrez deux gestionnaires de fichiers possédant chacun l'une des étiquettes.

Pour plus d'informations, reportez-vous à la section “[Procédure d'affichage de vos fichiers dans un espace de travail étiqueté](#)” à la page 48.

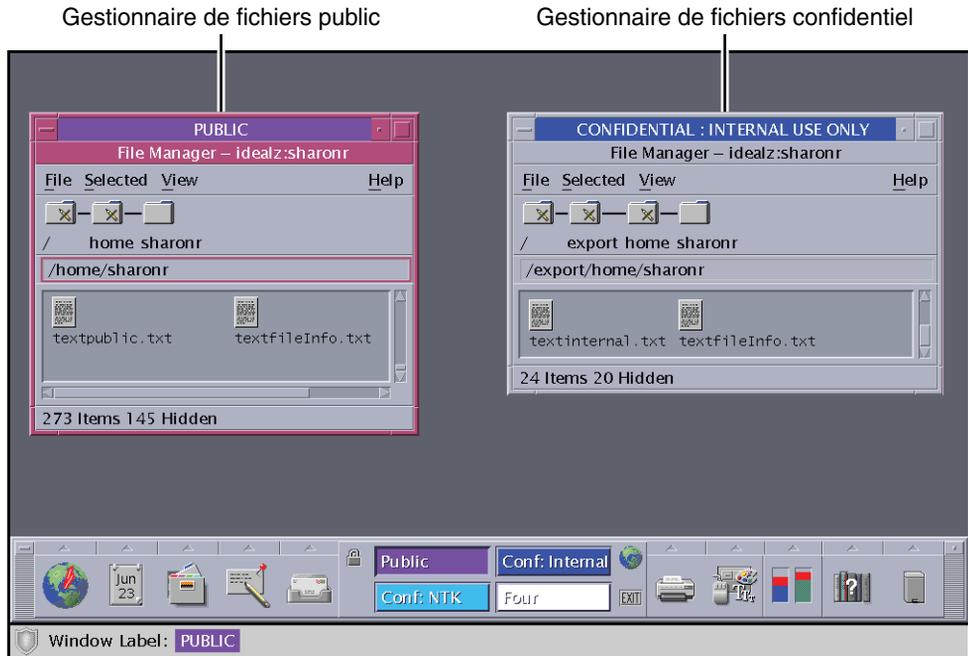
#### 3 Dans le gestionnaire de fichiers source, accédez au fichier dont vous souhaitez modifier l'étiquette.

#### 4 Dans le gestionnaire de fichiers cible, accédez au nouveau répertoire du fichier.

#### 5 Déplacez les gestionnaires de fichiers dans le même espace de travail.

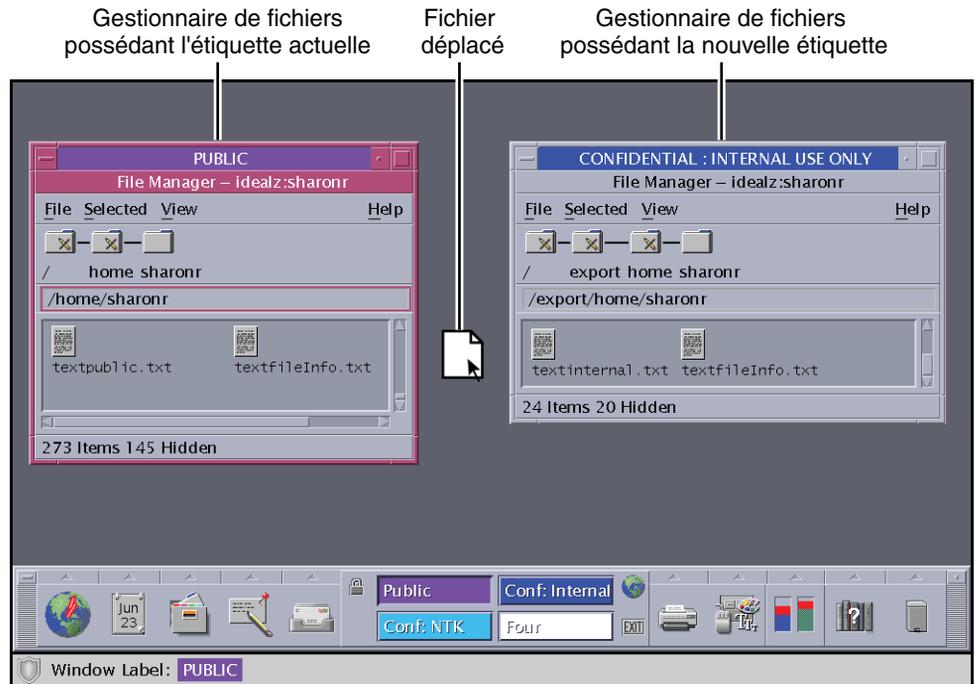
Pour plus d'informations, reportez-vous à la section “[Procédure de déplacement d'une fenêtre vers un autre espace de travail](#)” à la page 67.

FIGURE 3-16 Gestionnaires de fichiers possédant des étiquettes différentes dans un même espace de travail



- 6 Faites glisser le fichier vers le répertoire cible et déposez-le.

FIGURE 3-17 Déplacement d'un fichier entre des gestionnaires de fichiers possédant des étiquettes différentes

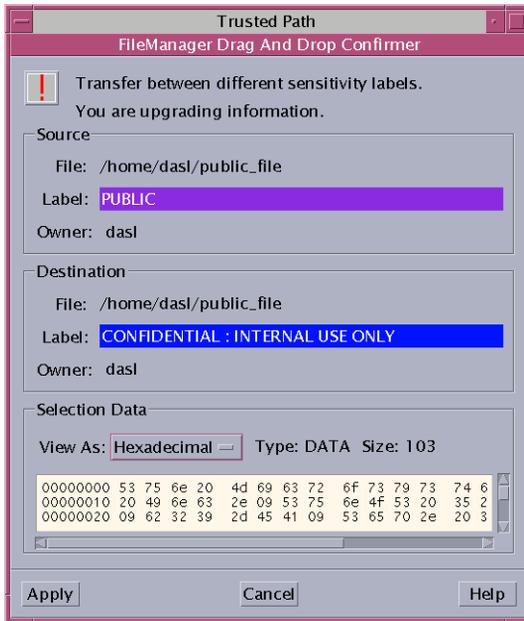


La boîte de dialogue de confirmation du gestionnaire de fichiers s'affiche, comme illustré à la Figure 3-18.

Cette boîte de dialogue est similaire à la boîte de dialogue de confirmation du gestionnaire de sélection, mais ne contient pas de chronomètre. Cette boîte de dialogue :

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

FIGURE 3-18 Boîte de dialogue de confirmation du gestionnaire de fichiers



## 7 Confirmez que vous souhaitez modifier l'étiquette du fichier.

- Cliquez sur Annuler pour arrêter la transaction.
- Cliquez sur Apply (Appliquer) pour déplacer le fichier vers la nouvelle étiquette.

### Exemple 3-5 Liaison d'un fichier à une étiquette différente

Lier un fichier à une étiquette différente permet de consulter un fichier possédant une étiquette de niveau inférieur depuis une étiquette de niveau plus élevé. Le fichier est uniquement accessible en écriture au niveau de l'étiquette inférieure.

Pour lier un fichier, l'utilisateur appuie sur les touches Maj+Ctrl tout en faisant glisser l'icône du fichier du gestionnaire de fichiers source vers le gestionnaire de fichiers cible. Ensuite, l'utilisateur confirme le lien ou annule l'opération.

#### Erreurs fréquentes

Si votre système n'est pas configuré pour autoriser le surclassement ou le déclassement d'étiquettes, une boîte de dialogue indiquant que le transfert n'est pas autorisé s'affiche. Contactez votre administrateur de sécurité.

## Éléments de Trusted Extensions (Référence)

---

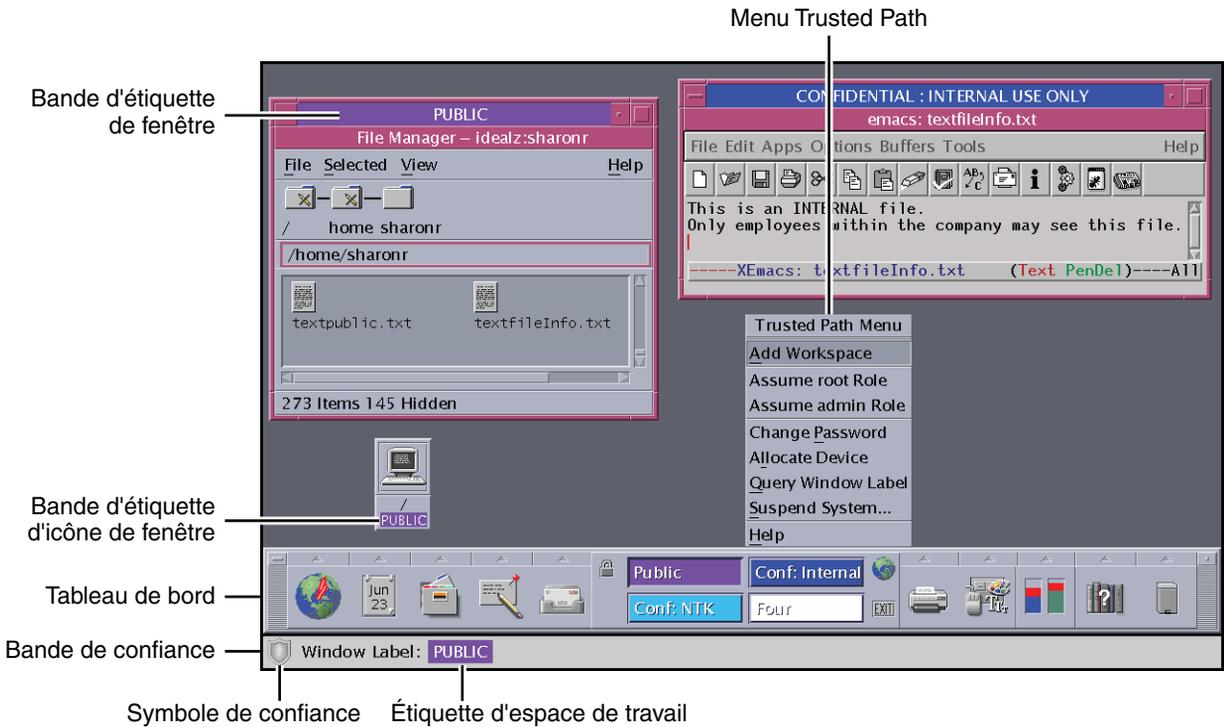
Ce chapitre décrit les éléments clés de Solaris Trusted Extensions. Ce chapitre comprend les sections suivantes :

- “Caractéristiques visibles de Trusted Extensions” à la page 77
- “Sécurité des périphériques dans Trusted Extensions” à la page 81
- “Fichiers et applications dans Trusted Extensions” à la page 81
- “Sécurité du mot de passe dans le SE Solaris” à la page 82
- “Sécurité du tableau de bord (Trusted CDE)” à la page 83

### Caractéristiques visibles de Trusted Extensions

Une fois connecté selon la procédure indiquée au [Chapitre 2, “Connexion à Trusted Extensions \(tâches\)”](#), vous pouvez travailler dans Trusted Extensions. Votre travail est soumis à certaines restrictions de sécurité. Les restrictions spécifiques à Trusted Extensions sont la plage d’étiquettes du système, vos autorisations et votre choix de session à niveau unique ou multiniveau. Comme illustré dans la figure suivante, quatre fonctions distinguent un système configuré avec Trusted Extensions d’un système Solaris. Pour afficher les fonctions sur un bureau Trusted JDS, reportez-vous à la [Figure 1-5](#).

FIGURE 4-1 Bureau Trusted CDE multiniveau



- **Affichages des étiquettes** : toutes les fenêtres, les espaces de travail, les fichiers et les applications ont une étiquette. Le bureau fournit des bandes d'étiquettes et d'autres indicateurs permettant d'afficher l'étiquette d'une entité.
- **Bande de confiance** : cette bande est un mécanisme de sécurité graphique particulier. Dans Solaris Trusted Extensions (CDE), la bande de confiance est toujours affichée au bas de l'écran. Dans Solaris Trusted Extensions (JDS), la bande s'affiche en haut de l'écran.
- **Accès limité à des applications à partir de l'espace de travail** : l'espace de travail vous permet uniquement d'accéder à des applications autorisées dans votre compte.
- **Menu Trusted Path (Chemin de confiance)** : dans Trusted CDE, la zone de commutation sur le tableau de bord permet d'accéder au menu Trusted Path, utilisé pour effectuer les tâches liées à la sécurité. Dans Trusted JDS, le symbole de confiance permet d'accéder au menu.

## Étiquettes sur les bureaux Trusted Extensions

Comme expliqué à la section “[Contrôle d'accès obligatoire](#)” à la page 18, toutes les applications et les fichiers Trusted Extensions portent des étiquettes. Trusted Extensions affiche les étiquettes aux emplacements suivants :

- Bandes d'étiquette de la fenêtre au-dessus de la barre de titre de la fenêtre
- Bandes d'étiquette de l'icône de la fenêtre sous la fenêtre réduite
- Indicateur d'étiquette de la fenêtre dans la bande de confiance
- Indicateur de requête d'étiquette de fenêtre dans le menu Trusted Path qui affiche l'étiquette ou l'icône de la fenêtre spécifiée par l'emplacement du pointeur
- Dans Trusted JDS, la couleur des panneaux indique l'étiquette de l'espace de travail.

FIGURE 4-2 Panneaux indiquant des espaces de travail possédant des étiquettes différentes dans Trusted JDS



La [Figure 4-1](#) présente l'affichage des étiquettes sur un bureau Trusted CDE. La [Figure 1-5](#) présente l'affichage des étiquettes sur un bureau Trusted JDS. L'option de menu Query Window Label (Requête d'étiquette de fenêtre) peut être utilisée pour afficher l'étiquette d'une fenêtre. Pour obtenir un exemple, reportez-vous à la [Figure 3-5](#).

## Bande de confiance

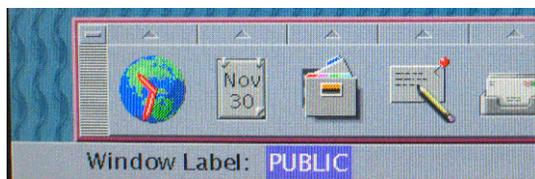
Dans Trusted CDE, la bande de confiance s'affiche dans une zone réservée au bas de l'écran au cours de toutes les sessions Trusted Extensions. Dans Trusted JDS, la bande de confiance s'affiche en haut de l'écran.

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

Dans Trusted CDE, la bande de confiance comporte deux éléments :

- **Le symbole de confiance** : s'affiche lorsque l'élément affiché à l'écran relève de la sécurité.
- **L'étiquette de la fenêtre** : facultatif. Affiche l'étiquette de la fenêtre active.

FIGURE 4-3 Étiquette de fenêtre PUBLIC dans la bande de confiance



Dans Trusted JDS, la bande de confiance comporte deux éléments supplémentaires :

- **Le nom de compte actif** : à droite du symbole de confiance, affiche le nom du propriétaire du nouveau processus dans l'espace de travail. Si le compte est un compte doté d'un rôle, une icône représentant un chapeau précède le nom du rôle.
- **Fenêtres étiquetées** : affiche les étiquettes de toutes les fenêtres de l'espace de travail.

FIGURE 4-4 Bande de confiance sur le bureau Trusted JDS



## Symbole de confiance

Chaque fois que vous accédez à une partie de la TCB, le symbole de confiance apparaît à gauche de la zone de la bande de confiance. Dans Trusted CDE, le symbole apparaît à gauche du tableau de bord. Dans Trusted JDS, le symbole apparaît à gauche de la bande de confiance.



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



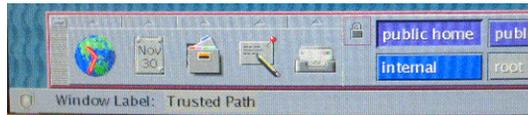
**Attention** – Si la bande de confiance n'apparaît pas dans votre espace de travail, contactez l'[administrateur de sécurité](#). Votre système pourrait avoir un problème sérieux.

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

## Indicateur d'étiquette de fenêtre

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

FIGURE 4-5 Indicateur Trusted Path dans la bande de confiance



## Sécurité des périphériques dans Trusted Extensions

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

Pour utiliser un périphérique, reportez-vous à la section [“Procédure d'allocation d'un périphérique dans Trusted Extensions”](#) à la page 59.

## Fichiers et applications dans Trusted Extensions

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

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

Certaines applications utilisent les fichiers d'initialisation pour configurer l'environnement de l'utilisateur. Deux fichiers spéciaux dans votre répertoire personnel vous permettent d'accéder

aux fichiers d'initialisation de chaque niveau d'étiquette. Ces fichiers permettent à une application correspondant à une étiquette d'utiliser un fichier d'initialisation provenant d'un répertoire dont l'étiquette est différente. Ces deux fichiers spéciaux sont `.copy_files` et `.link_files`.

## Fichier `.copy_files`

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

## Fichier `.link_files`

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

# Sécurité du mot de passe dans le SE Solaris

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

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

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

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

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

Vous pouvez modifier votre mot de passe à l'aide de l'option de menu Change Password (Modifier le mot de passe) à partir du menu Trusted Path. Pour connaître la procédure à suivre, reportez-vous à la section [“Réalisation d'actions sécurisées”](#) à la page 57.

## Sécurité du tableau de bord (Trusted CDE)

Le tableau de bord de Solaris Trusted Extensions (CDE) est très similaire à celui du CDE standard. Le tableau de bord de Trusted Extensions vous permet d'accéder uniquement aux applications, fichiers et utilitaires que vous êtes autorisé à utiliser. Si vous cliquez avec le bouton de souris 3 n'importe où dans la zone de commutation de l'espace de travail, le menu [menu Trusted Path \(Chemin de confiance\)](#) (menu Chemin de confiance) apparaît.

Pour pouvoir accéder à un périphérique via le gestionnaire de support amovible (Removable Media Manager), ce périphérique doit être alloué à l'aide du gestionnaire d'allocation de périphériques (Device Allocation Manager). Le gestionnaire de support amovible est accessible via le sous-panneau Tools (Outils), lequel est placé au-dessus de l'icône Style Manager (Gestionnaire de style) sur le tableau de bord.

---

**Astuce** – Si vous réduisez le tableau de bord, vous pouvez le rétablir en cliquant n'importe où dans la bande de confiance.

---

Dans Trusted Extensions, les sites de dépôt de l'icône d'installation (Install) sont limités aux applications et fichiers que vous êtes autorisé à utiliser au niveau de l'étiquette de l'espace de travail actif.

Pour plus d'informations sur le CDE standard, reportez-vous au *Common Desktop Environment User's Guide*.

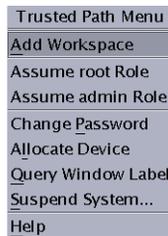
## Zone de commutation de l'espace de travail

Dans Trusted Extensions, les boutons de l'espace de travail définissent non seulement des espaces de travail distincts, mais exigent également que vous travailliez à des niveaux d'étiquette précis. Lorsque vous ouvrez une session multiniveau, chaque espace de travail possède l'étiquette la plus basse que vous pouvez utiliser. Si votre administrateur a utilisé des codes de couleur pour les étiquettes sur votre site, les boutons de l'espace de travail s'affichent dans la couleur de l'étiquette qui leur est associée. Le menu Trusted Path (Chemin de confiance) est disponible à partir de la zone de commutation de l'espace de travail.

## Menu Trusted Path

Le menu Trusted Path contient les options de menu qui touchent à la sécurité, comme illustré dans la figure suivante.

FIGURE 4-6 Menu Trusted Path - Base



Ce menu vous permet par exemple de modifier votre mot de passe ou d'allouer des périphériques. Pour plus d'informations, reportez-vous à la section "[Réalisation d'actions sécurisées](#)" à la page 57.

Dans Trusted CDE, le menu Trusted Path comporte une deuxième version. La version de l'espace de travail *Name* inclut d'autres options de l'espace de travail. Les sélections qui s'affichent dans votre menu dépendent de la façon dont l'administrateur a configuré votre compte.

FIGURE 4-7 Menu Trusted Path - Version de l'espace de travail *Name*

## Sécurité de l'horloge

Dans Trusted Extensions, seul un administrateur peut modifier la date et l'heure définies pour votre station de travail.

## Sécurité du calendrier

Le calendrier affiche vos rendez-vous correspondant à l'étiquette de votre espace de travail actif uniquement. Pour voir les rendez-vous correspondant à une autre étiquette, vous devez ouvrir un calendrier sous l'étiquette concernée.

## Sécurité du gestionnaire de fichiers

Dans Trusted Extensions, le gestionnaire de fichiers (File Manager) affiche les fichiers possédant l'étiquette de l'espace de travail actif. Pour afficher simultanément des fichiers correspondant à plusieurs étiquettes, exécutez le gestionnaire de fichiers à partir d'espaces de travail possédant des étiquettes différentes. Utilisez ensuite la commande `Occupy Workspace` (Occuper l'espace de travail) pour afficher les différentes fenêtres du gestionnaire de fichiers dans le même espace de travail.

Le gestionnaire de fichiers vous permet de modifier les autorisations de base et la liste de contrôle d'accès (ACL) pour un fichier ou un dossier. Si vous y êtes autorisé, vous pouvez également déplacer ou lier des fichiers entre des gestionnaires de fichiers possédant différentes étiquettes. Pour plus d'informations sur l'utilisation des gestionnaires de fichiers, reportez-vous aux sections [“Procédure d'affichage de vos fichiers dans un espace de travail étiqueté”](#) à la page 48 et [“Réalisation d'actions sécurisées”](#) à la page 57.

## Sécurité de l'éditeur de texte

Un éditeur de texte peut être utilisé pour modifier des fichiers correspondant à l'étiquette de l'espace de travail actif uniquement. Si vous y êtes autorisé, vous pouvez copier des informations entre les éditeurs de texte de différentes étiquettes.

## Sous-panneau d'applications personnelles

Les applications par défaut dans le sous-panneau d'applications personnelles fonctionnent de la même manière que l'environnement CDE standard. L'icône Terminal ouvre le shell par défaut qui vous a été attribué par votre administrateur. Pour accéder à un serveur Web, l'étiquette de votre navigateur doit être la même que celle du serveur Web.

## Sécurité du logiciel de messagerie

Dans Trusted Extensions, tous les messages sont étiquetés. Lorsque vous envoyez un message, il est envoyé avec l'étiquette de votre application de messagerie électronique. Seuls les utilisateurs et les hôtes qui sont autorisés à accéder à cette étiquette reçoivent le message. Seuls les utilisateurs qui travaillent au niveau de cette étiquette peuvent visualiser le message.

Si vous devez utiliser le message d'absence dans votre application de messagerie électronique, vous devez explicitement activer les réponses aux messages automatiques pour chaque étiquette au niveau de laquelle vous avez l'habitude de recevoir du courrier électronique. Adressez-vous à votre administrateur de sécurité pour connaître la stratégie de sécurité appliquée sur votre site au sujet des messages de réponse automatique.

## Sécurité des imprimantes

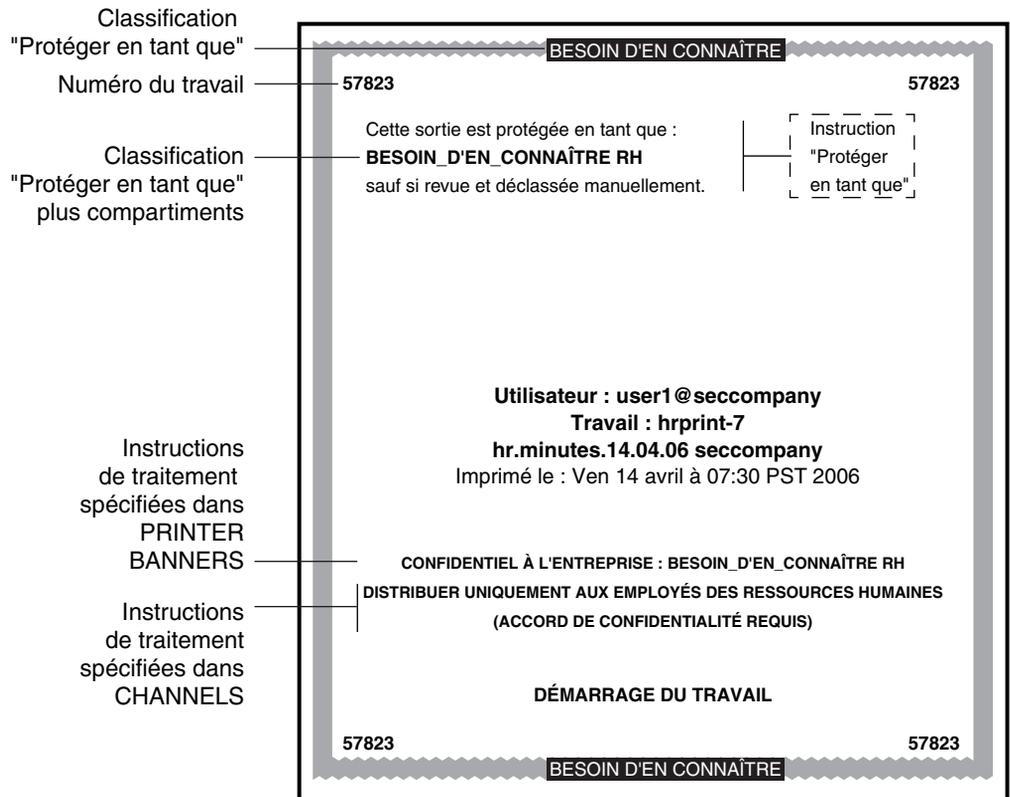
Le gestionnaire d'impression dans le panneau Personal Printers (Imprimantes personnelles) affiche des icônes de toutes les imprimantes qui sont accréditées jusqu'à votre niveau d'autorisation. Toutefois, vous ne pouvez utiliser que les imprimantes autorisées à imprimer des documents au niveau de l'étiquette de l'espace de travail actif.

Un travail d'impression typique dans Trusted Extensions inclut les étiquettes et différentes pages supplémentaires :

- Une page de garde au début de la tâche d'impression identifie le travail d'impression, fournit des instructions de traitement et précise une étiquette adaptée au site.
- Les pages du corps du texte sont étiquetées au niveau de l'en-tête et du pied de page.
- Une page de fin signale la fin du travail d'impression.

Une page de garde étiquetée standard est illustrée dans la figure suivante. Les mots DÉMARRAGE DU TRAVAIL identifient la page de garde.

FIGURE 4-8 Page de garde standard pour un travail d'impression étiqueté



Pour obtenir des informations de sécurité précises concernant l'impression sur votre site, contactez votre administrateur.

## Sécurité du gestionnaire de style

À trois exceptions près, le gestionnaire de style fonctionne de la même manière que sur un système Solaris.

- Le gestionnaire de style ne peut pas être exécuté à partir du gestionnaire d'applications lorsque Trusted Extensions est configuré car le gestionnaire de style requiert le chemin de confiance. Exécutez le gestionnaire de style à partir du tableau de bord et du menu de l'espace de travail, où le gestionnaire de style dispose du chemin de confiance.

- Les options d'économiseur d'écran et de verrouillage de l'écran sont limitées. L'administrateur spécifie la durée maximale pendant laquelle votre système peut rester inactif avant d'être verrouillé. Vous pouvez réduire le temps d'inactivité. Vous ne pouvez pas augmenter la durée d'inactivité au-delà du maximum. Vous avez toujours la possibilité de choisir un motif pour les moments où l'écran est verrouillé. Contactez votre administrateur si vous n'êtes pas familiarisé avec la stratégie en vigueur sur votre site.
- Le contrôle du démarrage définit les paramètres de la session au démarrage en fonction de l'étiquette ou des droits que vous spécifiez lors de la connexion. Par conséquent, vous pouvez enregistrer une configuration d'espace de travail différente pour chaque étiquette dans la plage d'étiquettes de votre compte.

## Sécurité du gestionnaire d'applications

Le gestionnaire d'applications vous permet d'accéder uniquement aux applications et utilitaires que votre administrateur vous a affectés. Dans un rôle, vous avez accès à un autre ensemble d'applications et de fonctionnalités. N'oubliez pas que l'effectivité d'une fonction sur un fichier dépend de l'étiquette de l'espace de travail actif.

De même, bien que vous puissiez ajouter des applications au sous-panneau d'applications personnelles en faisant glisser des icônes dans le site de dépôt de l'icône d'installation, vous pouvez uniquement exécuter une application si votre administrateur vous l'a attribuée.

## Sécurité de la corbeille

Dans Trusted Extensions, la corbeille peut stocker les fichiers à supprimer par étiquettes. Vous pouvez envoyer des fichiers possédant n'importe quelle étiquette dans la corbeille, mais la corbeille affichera uniquement les fichiers possédant l'étiquette active. Vous devez supprimer les informations sensibles dès qu'elles sont dans la corbeille.

## Sécurité de l'espace de travail (Trusted JDS)

Dans Trusted Extensions, Trusted JDS fournit une sécurité équivalente à celle de Trusted CDE, mais la présentation et l'apparence sont différentes. Comme dans Trusted CDE, les applications de bureau sont sensibles à l'étiquette. Les applications s'exécutent au niveau de l'étiquette de l'espace de travail actif et affichent uniquement des informations de même étiquette que la procédure qui a ouvert l'application.

L'emplacement des fonctionnalités de sécurité dans Trusted JDS est différent de leur emplacement dans Trusted CDE. Leur comportement peut également être différent.

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



# Glossaire

---

<b>action</b>	Application accessible à partir de l'interface graphique de CDE (Common Desktop Environment). Une action est représentée par une icône. L'action est constituée d'une ou de plusieurs commandes et d'invites utilisateur facultatives. Dans Trusted Extensions, une action n'est disponible pour un utilisateur que si l' <b>administrateur de sécurité</b> a inclus l'action dans un <b>profil de droits</b> affecté au compte de l'utilisateur. De même, certaines fonctions de l'action peuvent n'être disponibles que si l'administrateur de sécurité a affecté les autorisations et privilèges appropriés dans ce profil de droits.
<b>administrateur de sécurité</b>	Sur un système configuré avec Trusted Extensions, <b>rôle</b> qui est affecté à l'utilisateur ou aux utilisateurs chargé(s) de définir et d'appliquer la stratégie de sécurité. L'administrateur de sécurité peut travailler au niveau de n'importe quelle étiquette dans la <b>plage d'accréditations du système</b> , et peut éventuellement accéder à toutes les informations du site. L'administrateur de sécurité configure les attributs de sécurité pour tous les utilisateurs et équipements. Voir également <b>fichier de codage des étiquettes</b> .
<b>administrateur système</b>	Fonction de sécurité du SE Oracle Solaris. Le <b>rôle</b> d'administrateur système peut être affecté à l'utilisateur ou aux utilisateurs chargé(s) de réaliser des tâches standard d'administration du système telles que la configuration des éléments non liés à la sécurité des comptes utilisateur. Voir également <b>administrateur de sécurité</b> .
<b>affichage des étiquettes</b>	Fonction de sécurité qui affiche les <b>étiquettes d'administration</b> ou les remplace par des éléments de substitution non classifiés. Par exemple, si la stratégie de sécurité interdit d'exposer les étiquettes ADMIN_HIGH et ADMIN_LOW, les étiquettes RESTRICTED et PUBLIC peuvent leur être substituées.
<b>allocation de périphériques</b>	Fonction de sécurité du SE Oracle Solaris. L'allocation de périphériques est un mécanisme destiné à protéger les informations d'un <b>périphérique affectable</b> en empêchant toute personne autre que l'utilisateur qui affecte le périphérique d'y accéder. Lorsque le périphérique est libéré, des scripts de nettoyage du périphérique sont exécutés pour supprimer les informations du périphérique avant que celui-ci ne soit à nouveau accessible pour un autre utilisateur. Dans Trusted Extensions, l'allocation de périphériques est gérée par le <b>gestionnaire d'allocation de périphériques (Device Allocation Manager)</b> .
<b>application sécurisée</b>	Application qui a reçu un ou plusieurs privilèges.
<b>attributs de sécurité</b>	Fonction de sécurité du SE Oracle Solaris. Propriétés d'une entité liée à la sécurité telle qu'un processus, une zone, un utilisateur ou un périphérique. Les attributs de sécurité comprennent les valeurs d'identification comme <b>ID utilisateur (UID)</b> and <b>ID de groupe (GID)</b> . Les attributs qui sont spécifiques à Trusted Extensions incluent les étiquettes et la plage d'étiquettes. Notez que certains attributs de sécurité seulement s'appliquent à un type d'entité particulier.

<b>autorisation</b>	Fonction de sécurité du SE Oracle Solaris. Une autorisation permet à un utilisateur d'exécuter une action qui serait par ailleurs interdite par la stratégie de sécurité. L' <b>administrateur de sécurité</b> affecte les autorisations à un profil de droits. Les profils de droits sont ensuite assignés à des comptes utilisateur ou des <b>rôles</b> . Certaines commandes et actions ne fonctionnent pas parfaitement si l'utilisateur ne dispose pas des autorisations nécessaires. Voir également <b>privilège</b> .
<b>autorisation de session</b>	<b>autorisation</b> définie lors de la connexion, qui indique la limite supérieure des étiquettes pour une <b>session</b> Trusted Extensions. Si l'utilisateur est autorisé à définir l'autorisation de session, il peut spécifier toute valeur figurant dans la <b>plage d'étiquettes du compte</b> de l'utilisateur. Si le compte de l'utilisateur est configuré de manière à ne permettre que des sessions à niveau unique, l'autorisation de session est définie sur la valeur par défaut indiquée par l' <b>administrateur de sécurité</b> . Voir également <b>autorisation</b> .
<b>autorisation utilisateur</b>	Autorisation gérée par l' <b>administrateur de sécurité</b> . Une autorisation utilisateur définit la limite supérieure de la <b>plage d'étiquettes du compte</b> de l'utilisateur. L'autorisation utilisateur détermine l'étiquette la plus haute au niveau de laquelle l'utilisateur est autorisé à travailler. Voir également <b>autorisation</b> et <b>autorisation de session</b> .
<b>autorisation</b>	<b>étiquette</b> définissant la limite supérieure de la <b>plage d'étiquettes</b> . Une autorisation comprend deux composants : une <b>classification</b> et aucun, un ou plusieurs compartiments. Une autorisation n'a pas besoin d'être une <b>étiquette bien formée</b> . Une autorisation définit une limite théorique et pas nécessairement une étiquette réelle. Voir également <b>autorisation utilisateur</b> , <b>autorisation de session</b> et <b>fichier de codage des étiquettes</b> .
<b>autorisations</b>	Ensemble de codes qui indiquent quels utilisateurs sont autorisés à lire, écrire ou exécuter le fichier ou répertoire (dossier). Les utilisateurs sont classés dans les catégories suivantes : propriétaire, groupe (groupe du propriétaire) et autres (tous les autres). L'autorisation de lecture, indiquée par la lettre <i>r</i> , permet à l'utilisateur de lire le contenu d'un fichier ou, s'il s'agit d'un répertoire, d'afficher la liste des fichiers présents dans le dossier. L'autorisation d'écriture, indiquée par la lettre <i>w</i> , permet à l'utilisateur d'apporter des modifications à un fichier ou, dans le cas d'un dossier, d'ajouter ou de supprimer des fichiers. Le droit d'exécution, indiqué par la lettre <i>e</i> , permet à l'utilisateur d'exécuter le fichier s'il s'agit d'un fichier exécutable. Si le fichier est un répertoire, le droit d'exécution permet à l'utilisateur de lire les fichiers dans le répertoire ou d'y effectuer une recherche. On parle également d'autorisations UNIX ou de bits d'autorisation.
<b>bande de confiance</b>	Zone graphique rectangulaire plein écran apparaissant dans une zone réservée de l'écran. La bande de confiance s'affiche dans toutes les sessions Trusted Extensions pour confirmer qu'il s'agit de sessions Trusted Extensions valides. En fonction de la configuration du site, la bande de confiance dispose d'un ou de deux composants : (1) un <b>symbole de confiance</b> obligatoire qui indique l'interaction avec la <b>base informatique sécurisée (TCB, Trusted Computing Base)</b> et (2) une <b>étiquette</b> facultative qui indique l'étiquette active de la fenêtre ou de l'espace de travail actif.
<b>base informatique sécurisée (TCB, Trusted Computing Base)</b>	Partie d'un système configuré avec Trusted Extensions qui a une incidence sur la sécurité. La TCB englobe les logiciels, le matériel, les microprogrammes, la documentation et les procédures administratives. Les utilitaires et applications pouvant accéder aux fichiers liés à la sécurité font partie de la base informatique sécurisée.
<b>canal caché</b>	Canal de communication qui n'est normalement pas destiné à la communication de données. Un canal caché autorise un processus à transférer indirectement des informations d'une manière qui va à l'encontre de la stratégie de sécurité.

<b>chemin de confiance</b>	Fait référence au mécanisme permettant d'accéder à des actions et des commandes autorisées à interagir avec la <a href="#">base informatique sécurisée (TCB, Trusted Computing Base)</a> . Voir également <a href="#">menu Trusted Path (Chemin de confiance)</a> , <a href="#">symbole de confiance</a> et <a href="#">bande de confiance</a> .
<b>classification</b>	Composant d'une <a href="#">autorisation</a> ou d'une <a href="#">étiquette</a> . Une classification indique un niveau de sécurité hiérarchique, par exemple TOP SECRET ou UNCLASSIFIED.
<b>Common Desktop Environment (CDE)</b>	Bureau graphique étiqueté incluant un gestionnaire de sessions, un gestionnaire de fenêtres et différents outils du bureau. Trusted Extensions ajoute des applications sécurisées au bureau, par exemple le <a href="#">générateur d'étiquettes</a> , le <a href="#">gestionnaire d'allocation de périphériques (Device Allocation Manager)</a> et le <a href="#">Gestionnaire de sélection (Selection Manager)</a> . Voir également <a href="#">Trusted JDS</a> .
<b>compartiment</b>	Composant non hiérarchique d'une <a href="#">étiquette</a> utilisé avec le composant <a href="#">classification</a> pour former une <a href="#">autorisation</a> ou une <a href="#">étiquette</a> . Un compartiment représente un groupe d'utilisateurs qui pourraient avoir besoin d'accéder à des informations, par exemple un département ingénierie ou une équipe de projet pluridisciplinaire.
<b>compartmented mode workstation (CMW)</b>	Système informatique répondant aux exigences du gouvernement américain en termes de sécurité des stations de travail telles que spécifiées à la section <i>Security Requirements for System High and Compartmented Mode Workstations</i> du document DDS-2600-5502-87 de la DIA. Plus précisément, ce document définit un système d'exploitation sécurisé basé sur un système Window X pour les stations de travail UNIX.
<b>configuration à étiquette unique</b>	Compte utilisateur configuré pour être utilisé avec une <a href="#">étiquette</a> unique. Également appelée configuration à niveau unique.
<b>configuration étendue</b>	Système informatique qui n'est plus une <a href="#">configuration évaluable</a> en raison de modifications qui ont enfreint la stratégie de sécurité.
<b>configuration évaluable</b>	Système informatique répondant aux exigences de sécurité standard définies par le gouvernement. Voir également <a href="#">configuration étendue</a> .
<b>contrôle</b>	Fonction de sécurité du SE Oracle Solaris. Le contrôle est un processus permettant de capturer l'activité de l'utilisateur et d'autres événements survenant sur le système, puis de stocker ces informations dans un ensemble de fichiers appelé <i>piste d'audit</i> . Le contrôle génère des rapports d'activité du système dans le cadre de la stratégie de sécurité du site.
<b>contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</b>	Mécanisme de contrôle d'accès qui permet au propriétaire d'un fichier ou d'un répertoire d'accorder ou de refuser l'accès à d'autres utilisateurs. Le propriétaire affecte des <a href="#">autorisations</a> en lecture, écriture et exécution au propriétaire, au groupe d'utilisateurs auquel appartient le propriétaire et à une catégorie appelée autres, qui fait référence à tous les autres utilisateurs non spécifiés. Le propriétaire peut également spécifier une <a href="#">liste de contrôle d'accès (ACL, Access Control List)</a> . Une ACL permet au propriétaire d'attribuer des autorisations spécifiques à d'autres utilisateurs et à d'autres groupes. Contraire de <a href="#">contrôle d'accès obligatoire (MAC, Mandatory Access Control)</a> .

<b>contrôle d'accès obligatoire (MAC, Mandatory Access Control)</b>	Mécanisme de contrôle d'accès appliqué par le système qui utilise des autorisations et des étiquettes pour appliquer la stratégie de sécurité. Une <a href="#">autorisation</a> ou une <a href="#">étiquette</a> est un niveau de sécurité. MAC associe les programmes qu'un utilisateur exécute au niveau de sécurité auquel l'utilisateur choisit de travailler dans la session. MAC autorise uniquement l'accès aux informations, aux programmes et aux périphériques correspondant au même niveau ou à un niveau inférieur. MAC empêche également les utilisateurs d'écrire dans des fichiers de niveau inférieur. MAC ne peut pas être contourné sans une autorisation ou un privilège spécial. Contraire de <a href="#">contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</a> .
<b>domination stricte</b>	Voir également <a href="#">étiquette dominante</a> .
<b>droit d'accès</b>	Fonction de sécurité présente sur la plupart des systèmes informatiques. Les droits d'accès donnent à l'utilisateur l'autorisation de lire, d'écrire, d'exécuter ou d'afficher le nom d'un fichier ou d'un répertoire. Voir également <a href="#">contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</a> et <a href="#">contrôle d'accès obligatoire (MAC, Mandatory Access Control)</a> .
<b>espace de travail</b>	Voir <a href="#">espace de travail étiqueté</a> .
<b>espace de travail étiqueté</b>	Espace de travail Solaris Trusted Extensions (CDE) ou Solaris Trusted Extensions (JDS). Un espace de travail étiqueté étiquette chaque activité qui y est lancée avec l' <a href="#">étiquette</a> de l'espace de travail. Lorsque les utilisateurs déplacent une fenêtre dans un espace de travail correspondant à une autre étiquette, la fenêtre déplacée conserve son étiquette d'origine.
<b>étiquette</b>	Également appelée étiquette de sensibilité. Une étiquette indique le niveau de sécurité d'une entité. Une entité est un fichier, un répertoire, un processus, un périphérique ou une interface réseau. L'étiquette d'une entité permet de déterminer si l'accès doit être autorisé dans une transaction particulière. Les étiquettes comprennent deux composants : une <a href="#">classification</a> qui indique le niveau hiérarchique de sécurité et aucun, un ou plusieurs compartiments permettant de définir qui peut accéder à une entité d'une classification donnée. Voir également <a href="#">fichier de codage des étiquettes</a> .
<b>étiquette bien formée</b>	<a href="#">étiquette</a> pouvant être incluse dans une plage, car elle est autorisée par toutes les règles applicables dans le <a href="#">fichier de codage des étiquettes</a> .
<b>étiquette de sensibilité</b>	Voir <a href="#">étiquette</a> .
<b>étiquette déclassée</b>	<a href="#">étiquette</a> d'un objet qui a été modifiée et remplacée par une valeur qui n'est pas dominante par rapport à la valeur précédente de l'étiquette.
<b>étiquette disjointe</b>	Voir également <a href="#">étiquette dominante</a> .
<b>étiquette dominante</b>	Lors de la comparaison de deux étiquettes, étiquette dont le composant <a href="#">classification</a> est supérieur ou égal à la classification de la deuxième étiquette et dont les composants <a href="#">compartiment</a> comprennent tous les composants compartiment de la deuxième étiquette. Si les composants sont les mêmes, les étiquettes sont dites dominantes et sont <i>égales</i> . Si une étiquette domine l'autre et les étiquettes ne sont donc pas égales, la première étiquette est dite <i>strictement dominante</i> par rapport à l'autre. Deux étiquettes sont <i>disjointes</i> si elles ne sont pas égales et qu'aucune étiquette n'est dominante.

<b>étiquette minimum</b>	<p><b>étiquette</b> affectée à un utilisateur en tant que limite inférieure de l'ensemble d'étiquettes dans lequel cet utilisateur peut travailler. La première fois qu'un utilisateur ouvre une session Trusted Extensions, l'étiquette minimum est l'étiquette par défaut de l'utilisateur. Au moment de la connexion, l'utilisateur peut choisir une autre étiquette comme étiquette initiale.</p> <p>Désigne aussi l'étiquette la plus basse autorisée pour tout utilisateur non administratif. L'étiquette minimum est affectée par l'<b>administrateur de sécurité</b> et définit la limite inférieure de la <b>plage d'accréditations de l'utilisateur</b>.</p>
<b>étiquette surclassée</b>	<p><b>étiquette</b> d'un objet ayant été modifiée et remplacée par une valeur qui est dominante par rapport à la valeur précédente de l'étiquette.</p>
<b>étiquettes d'administration</b>	<p>Deux étiquettes spéciales prévues pour les fichiers d'administration uniquement : ADMIN_LOW et ADMIN_HIGH. ADMIN_LOW est l'étiquette la plus basse dans le système sans catégories. Cette étiquette est strictement dominée par toutes les étiquettes du système. Les informations de niveau ADMIN_LOW sont lisibles par tous, mais peuvent uniquement être écrites par un utilisateur occupant un <b>rôle</b> qui travaille au niveau de l'étiquette ADMIN_LOW. ADMIN_HIGH est l'étiquette la plus haute dans le système sans catégories. Cette étiquette domine strictement toutes les étiquettes du système. Les informations de niveau ADMIN_HIGH ne sont lisibles que par les utilisateurs occupant un rôle opérant au niveau ADMIN_HIGH. Les étiquettes d'administration sont utilisées comme des étiquettes ou des autorisations pour les rôles et les systèmes. Voir également <b>étiquette dominante</b>.</p>
<b>fichier de codage des étiquettes</b>	<p>Fichier géré par l'<b>administrateur de sécurité</b>. Le fichier de codage contient les définitions de toutes les autorisations et étiquettes valides. Il définit également la <b>plage d'accréditations du système</b> et la <b>plage d'accréditations de l'utilisateur</b> et définit les informations de sécurité des impressions sur le site.</p>
<b>générateur d'étiquettes</b>	<p>Application sécurisée de Trusted Extensions. Cette interface graphique permet aux utilisateurs de choisir des autorisations pour la session ou une étiquette de session. L'<b>autorisation</b> ou l'<b>étiquette</b> doit être comprise dans la <b>plage d'étiquettes du compte</b> que l'<b>administrateur de sécurité</b> a affectée à l'utilisateur.</p>
<b>gestion des installations sécurisées</b>	<p>Toutes les activités associées à l'administration du système dans un système UNIX classique, plus toutes les activités d'administration nécessaires au maintien de la sécurité d'un système distribué et des données qu'il contient.</p>
<b>gestionnaire d'allocation de périphériques (Device Allocation Manager)</b>	<p>Application sécurisée de Trusted Extensions. Cette interface graphique est utilisée pour configurer, allouer et libérer des périphériques. La configuration des périphériques inclut l'ajout d'exigences relatives à l'autorisation à un périphérique.</p>
<b>Gestionnaire de sélection (Selection Manager)</b>	<p>Application sécurisée de Trusted Extensions. Cette interface graphique s'affiche lorsque des utilisateurs autorisés tentent d'augmenter ou de réduire le niveau de sécurité d'informations.</p>
<b>hôte</b>	<p>Ordinateur connecté à un réseau.</p>

<b>ID de contrôle (AUID, Audit ID)</b>	Fonction de sécurité du SE Oracle Solaris. Un ID de contrôle représente l'utilisateur connecté. L'AUID n'est plus modifié une fois que l'utilisateur assume un rôle, de sorte qu'il est utilisé pour identifier l'utilisateur à des fins de <a href="#">contrôle</a> . L'ID de contrôle représente toujours l'utilisateur objet du contrôle, même lorsque celui-ci acquiert des <a href="#">UID/GID effectifs</a> . Voir également <a href="#">ID utilisateur (UID)</a> .
<b>ID de groupe (GID)</b>	Fonction de sécurité du SE Oracle Solaris. Un ID de groupe est un nombre entier qui identifie un groupe d'utilisateurs partageant des droits d'accès communs. Voir également <a href="#">contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</a> .
<b>ID utilisateur (UID)</b>	Fonction de sécurité du SE Oracle Solaris. Un UID identifie un utilisateur à des fins de <a href="#">contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</a> , de <a href="#">contrôle d'accès obligatoire (MAC, Mandatory Access Control)</a> et de <a href="#">contrôle</a> . Voir également <a href="#">droit d'accès</a> .
<b>lecture</b>	Aptitude d'un <a href="#">sujet</a> à visualiser un <a href="#">objet</a> dont l' <a href="#">étiquette</a> est dominée par le sujet. La stratégie de sécurité autorise généralement la lecture. Par exemple, un éditeur de texte qui s'exécute en tant que <code>Sec ret</code> peut lire les données <code>Unc lass ified</code> . Voir également <a href="#">contrôle d'accès obligatoire (MAC, Mandatory Access Control)</a> .
<b>liste de contrôle d'accès (ACL, Access Control List)</b>	Fonction de sécurité du SE Oracle Solaris. Une ACL étend le <a href="#">contrôle d'accès discrétionnaire (DAC, Discretionary Access Control)</a> à l'utilisation d'une liste de spécifications d'autorisation (entrées ACL) qui s'appliquent à des utilisateurs et des groupes spécifiques. Une ACL permet un contrôle plus précis que celui que fourni par les <a href="#">autorisations</a> UNIX standard.
<b>mécanisme de secours</b>	Méthode de raccourci permettant de spécifier des adresse IP dans la base de données <code>tnrhtp</code> . Pour les adresses IPv4, le mécanisme de secours reconnaît le <code>0</code> comme un caractère générique pour un sous-réseau.
<b>menu Trusted Path (Chemin de confiance)</b>	Menu des opérations Trusted Extensions qui s'affiche lorsque vous maintenez le bouton 3 de la souris enfoncé sur la zone de commutation du tableau de bord. Les sélections de menu se répartissent en trois catégories : sélections orientées espace de travail, sélections d'adoption de <a href="#">rôle</a> et tâches liées à la sécurité.
<b>modèle d'hôte</b>	Enregistrement dans la base de données <code>tnrhtp</code> qui définit les attributs de sécurité d'une classe d'hôtes pouvant accéder au réseau Trusted Extensions.
<b>moins privilège</b>	Voir <a href="#">principe du moins privilège</a> .
<b>objet</b>	Entité passive contenant ou recevant des données, par exemple un fichier de données, un répertoire, une imprimante ou un autre périphérique. Un objet fait généralement l'objet d'interventions de la part de sujets. Dans certains cas, un <a href="#">processus</a> peut être un objet, par exemple lorsque vous envoyez un signal à un processus.
<b>opérateur</b>	<a href="#">rôle</a> pouvant être affecté à l'utilisateur ou aux utilisateurs chargés de la sauvegarde des systèmes.
<b>passerelle</b>	Hôte qui possède plusieurs interfaces réseau. Un tel hôte peut être utilisé pour relier deux ou plusieurs réseaux. Lorsque la passerelle est un hôte Trusted Extensions, elle peut restreindre le trafic à une étiquette donnée.
<b>périphérique</b>	Voir <a href="#">périphérique affectable</a> .

<b>périphérique affectable</b>	Fonction de sécurité du SE Oracle Solaris. Un périphérique affectable peut être utilisé par un seul utilisateur à la fois et est en mesure d'importer ou d'exporter des données à partir du système. L' <a href="#">administrateur de sécurité</a> détermine les utilisateurs autorisés à accéder à des périphériques affectables précis. Les périphériques affectables incluent les lecteurs de bande, les lecteurs de disquette, les périphériques audio et les lecteurs de CD-ROM. Voir également <a href="#">allocation de périphériques</a> .
<b>périphérique libéré</b>	Fonction de sécurité du SE Oracle Solaris. Un périphérique libéré n'est plus alloué exclusivement à un utilisateur. Voir également <a href="#">allocation de périphériques</a> .
<b>plage d'accréditations</b>	Ensemble d'étiquettes approuvées pour une classe d'utilisateurs ou de ressources. Voir également <a href="#">plage d'accréditations du système</a> , <a href="#">plage d'accréditations de l'utilisateur</a> , <a href="#">fichier de codage des étiquettes</a> et <a href="#">plage d'accréditations réseau</a> .
<b>plage d'accréditations de l'utilisateur</b>	Plus vaste ensemble d'étiquettes que l' <a href="#">administrateur de sécurité</a> puisse potentiellement affecter à un utilisateur d'un site spécifique. La plage d'accréditations de l'utilisateur exclut les <a href="#">étiquettes d'administration</a> et toute combinaison d'étiquettes uniquement disponible aux administrateurs. La plage d'accréditations de l'utilisateur est définie dans le <a href="#">fichier de codage des étiquettes</a> .
<b>plage d'accréditations du système</b>	Ensemble de toutes les étiquettes valides pour un site. Cet ensemble comprend les <a href="#">étiquettes d'administration</a> disponibles pour l' <a href="#">administrateur de sécurité</a> et l' <a href="#">administrateur système</a> du site. La plage d'accréditations du système est définie dans le <a href="#">fichier de codage des étiquettes</a> .
<b>plage d'accréditations réseau</b>	Ensemble d'étiquettes au sein duquel les hôtes Trusted Extensions sont autorisés à communiquer sur un réseau. Cet ensemble peut être une liste de quatre étiquettes discrètes.
<b>plage d'étiquettes</b>	N'importe quel ensemble d'étiquettes limité au niveau supérieur par une <a href="#">autorisation</a> ou étiquette maximale, au niveau inférieur par une étiquette minimale et se composant d'étiquettes bien formées. Les plages d'étiquettes sont utilisées pour appliquer le <a href="#">contrôle d'accès obligatoire (MAC, Mandatory Access Control)</a> . Voir également <a href="#">fichier de codage des étiquettes</a> , <a href="#">plage d'étiquettes du compte</a> , <a href="#">plage d'accréditations</a> , <a href="#">plage d'accréditations réseau</a> , <a href="#">plage de session</a> , <a href="#">plage d'accréditations du système</a> et <a href="#">plage d'accréditations de l'utilisateur</a> .
<b>plage d'étiquettes du compte</b>	Ensemble d'étiquettes affecté par l'administrateur de sécurité à un utilisateur ou un <a href="#">rôle</a> pour travailler sur un système configuré avec Trusted Extensions. Une plage d'étiquettes est définie au niveau supérieur par l' <a href="#">autorisation utilisateur</a> et au niveau inférieur par l' <a href="#">étiquette minimum</a> de l'utilisateur. Chaque étiquette de l'ensemble doit être bien formée.
<b>plage de session</b>	Ensemble des étiquettes disponibles pour un utilisateur pendant une session Trusted Extensions. La plage de session est limitée au niveau supérieur par l' <a href="#">autorisation de session</a> de l'utilisateur et au niveau inférieur par l' <a href="#">étiquette minimum</a> .
<b>principe du moindre privilège</b>	Principe de sécurité qui limite les utilisateurs aux seules fonctions nécessaires à leur travail. Ce principe est appliqué dans le système d'exploitation Solaris en mettant les privilèges à la disposition des programmes en fonction des besoins. Les privilèges sont disponibles en fonction des besoins, à des fins spécifiques uniquement.
<b>privilege</b>	Fonction de sécurité du SE Oracle Solaris. Un privilege est une autorisation accordée à un programme par l' <a href="#">administrateur de sécurité</a> . Un privilege peut être requis pour passer outre à certains aspects de la stratégie de sécurité. Voir également <a href="#">autorisation</a> .

<b>processus</b>	Programme en cours d'exécution. Les processus Trusted Extensions disposent d'attributs de sécurité Solaris, tels que l' <b>ID utilisateur (UID)</b> , l' <b>ID de groupe (GID)</b> , l' <b>ID de contrôle (AUID, Audit ID)</b> de l'utilisateur et des privilèges. Trusted Extensions ajoute une <b>étiquette</b> à chaque processus.
<b>processus privilégié</b>	Fonction de sécurité du SE Oracle Solaris. Un <b>processus</b> privilégié est exécuté par un utilisateur disposant de privilèges.
<b>profil</b>	Voir <b>profil de droits</b> .
<b>profil de droits</b>	Fonction de sécurité du SE Oracle Solaris. Un profil de droits permet à l' <b>administrateur de sécurité</b> d'un site de regrouper les commandes et les actions CDE avec les attributs de sécurité. Les attributs, tels que les autorisations et les privilèges de l'utilisateur, permettent aux commandes et aux actions d'aboutir. Un profil de droits contient généralement des tâches connexes. Un profil peut être affecté à des utilisateurs et à des rôles.
<b>rôle</b>	Fonction de sécurité du SE Oracle Solaris. Un rôle est un compte spécial qui donne à l'utilisateur qui assume le rôle accès à certaines applications avec les attributs de sécurité nécessaires à l'exécution de tâches spécifiques.
<b>session</b>	Intervalle de temps qui s'écoule entre la connexion à l'hôte Trusted Extensions et la déconnexion de l'hôte. La <b>bande de confiance</b> apparaît lors de toutes les sessions Trusted Extensions pour confirmer que les utilisateurs ne sont pas victimes d'une usurpation par un système contrefait.
<b>shell de profil</b>	Fonction de sécurité du SE Oracle Solaris. Une version du shell Bourne qui permet à un utilisateur d'exécuter des programmes avec des attributs de sécurité.
<b>stratégie de sécurité</b>	Ensemble des règles DAC, MAC et d'étiquettes qui définissent la manière dont les informations peuvent être consultées et par qui. Sur le site d'un client, ensemble de règles qui définit la sensibilité des informations traitées au niveau de ce site. La stratégie comprend les mesures utilisées pour protéger les informations contre tout accès non autorisé.
<b>sujet</b>	Entité active, généralement un <b>processus</b> qui s'exécute au nom d'un utilisateur ou d'un <b>rôle</b> . Un sujet fait circuler les informations entre les objets ou modifie l'état du système.
<b>symbole de confiance</b>	Symbole qui s'affiche à gauche de la zone <b>bande de confiance</b> . Le symbole s'affiche chaque fois que l'utilisateur accède à une partie de la <b>base informatique sécurisée (TCB, Trusted Computing Base)</b> .
<b>Trusted JDS</b>	Bureau graphique étiqueté incluant un gestionnaire de sessions, un gestionnaire de fenêtres et différents outils du bureau. Trusted JDS est un bureau entièrement accessible.
<b>type d'hôte</b>	Classification d'un <b>hôte</b> . La classification est utilisée pour les communications réseau. Les définitions des types d'hôtes sont stockées dans la base de données tnrtcp. Le type d'hôte détermine si le protocole réseau CIPSO est utilisé pour communiquer avec d'autres hôtes sur le réseau. L'expression <i>protocole réseau se</i> rapporte aux règles d'empaquetage des informations de communication.

<b>UID/GID effectif</b>	Fonction de sécurité du SE Oracle Solaris. Les ID effectifs remplacent le véritable ID lorsque cela est nécessaire pour exécuter un programme particulier ou une option d'un programme. L' <a href="#">administrateur de sécurité</a> affecte un UID effectif à une commande ou une action ou dans un <a href="#">profil de droits</a> lorsque cette commande ou action doit être exécutée par un utilisateur spécifique, le plus souvent lorsque la commande doit être exécutée en tant que root. Les ID de groupe effectifs sont utilisés de la même manière. Notez que l'utilisation de la commande <code>setuid</code> comme dans les systèmes UNIX classiques risque de ne pas fonctionner en raison des privilèges nécessaires.
<b>usurpation</b>	Acte consistant à contrefaire un programme logiciel afin d'accéder de manière illicite aux informations présentes sur un système.
<b>utilisateur standard</b>	Utilisateur qui ne détient aucune autorisation spéciale permettant des exceptions par rapport aux stratégies de sécurité standard du système. En général, un utilisateur standard ne peut pas assumer de <a href="#">rôle</a> d'administration.



# Index

---

## A

### Accès

- Bureau multiniveau distant, 40–41
- Écriture, 24
- Fichier d'initialisation de chaque étiquette, 53–54
- Lecture et écriture, 25
- Lecture seule, 24
- Pages du manuel dans Trusted Extensions, 50
- Répertoire personnel de niveau inférieur, 23

Accès en écriture, Dans un environnement étiqueté, 24

Accès en lecture, Dans un environnement étiqueté, 24

Accessibilité, Fournie par Trusted JDS, 33

Administration système, Sur Trusted

Extensions, 29–31

Adoption d'un rôle, 63–64

Aide dans Trusted Extensions

Aide en ligne, 50–51

Pages de manuel, 50

Ajout

Espace de travail, 65–66

Espace de travail étiqueté, 65–66

Allocation, Support amovible, 61

Allocation d'un périphérique, 59–62

Dépannage, 62

Application de confiance, Tableau de bord, 83

Application sécurisée, À l'aide de profils de droits, 30

Arrêt d'un poste de travail, 47–48

Aucun indicateur de confiance, Dépannage, 80

Augmentation du niveau de sécurité

d'informations, 25

Autorisation

Allocation de périphériques, 17

Autorisation (*Suite*)

De session, 39

Définition à la connexion, 26–27, 39

Modification d'étiquettes, 25

Nécessaire pour modifier l'étiquette de données, 69–72

Type d'étiquette, 19

Autorisation de l'utilisateur, Définition, 19

Autorisation de session, Définition, 26–27

## B

Bande de confiance

Absente dans l'écran de verrouillage, 45

Description, 79

Emplacement à l'écran, 20, 21

Emplacement dans CDE, 78

Emplacement dans Trusted JDS, 78

Procédure en cas d'absence de la bande, 44

Système multiécran, 43

Basculement vers un espace de travail possédant une étiquette différente, 66–67

Base informatique sécurisée (TCB, Trusted Computing Base)

Définition, 16

Procédures qui interagissent avec la TCB, 57–76

Symbole d'interaction, 17, 80

Bureau

Connexion à distance, 40–41

Focus du clavier, 57–58

Tâches courantes, 55–57

Bureaux, Dans Trusted Extensions, 33–34

## C

CDE, Application de confiance sur le tableau de bord, 83

Choix

Bureau, 35, 36

Étiquette ou autorisation au cours de la connexion, 38

Combinaisons de touches, Vérification de la fiabilité de la préhension, 57–58

Composant de classification de l'étiquette, Définition, 19

Composant de compartiment de l'étiquette, Définition, 19

Connexion

À un bureau multiniveau à distance, 40–41

Choix d'un bureau, 35, 36

Choix d'une étiquette ou d'une autorisation, 38

Cinq étapes, 34

Dépannage, 37, 39–40

Étiquette différente, 58

Examen des paramètres de sécurité, 37–39

Secours, 39–40

Connexion à distance, Bureau multiniveau, 40–41

Connexion à niveau unique, Trusted CDE ou Trusted JDS, 36

Connexion de secours, 39–40

Connexion multiniveau

À distance, 40–41

Trusted CDE ou Trusted JDS, 36

Conteneur, *Voir* Zone

Contrôle d'accès

Bits d'autorisation, 18

Contrôle d'accès discrétionnaire (DAC, Discretionary Access Control), 18

Contrôle d'accès obligatoire (MAC, Mandatory Access Control), 18–25

Liste de contrôle d'accès (ACL, Access Control List), 18

Contrôle d'accès discrétionnaire (DAC, Discretionary Access Control), Définition, 18

Contrôle d'accès obligatoire (MAC, Mandatory Access Control)

Appliqué pour les e-mails, 29

Définition, 18–25

Copier-coller, Effet sur les étiquettes, 25

.copy\_files, fichier

Création, 53–54

Dépannage, 54

Description, 82

Création

\$HOME/.copy\_files, fichier, 53–54

\$HOME/.link\_files, fichier, 53–54

## D

Déconnexion

Procédure, 46–47

Responsabilités de l'utilisateur, 44

Dépannage

\$HOME/.copy\_files, fichier, 54

\$HOME/.link\_files, fichier, 54

Allocation de périphérique, 62

Attribution d'une nouvelle étiquette à d<sup>2</sup>es fichiers, 76

Bande de confiance absente, 44

Connexion, 39–40

Gestionnaire de fichiers absent, 62

Indicateur de confiance manquant, 80

Messages d'erreur de la ligne de commande, 30

Mot de passe incorrect, 37

Tableau de bord réduit, 83

Déplacement

Données vers une étiquette différente, 69–72

Fenêtre vers un espace de travail possédant une étiquette différente, 67–68

Fichier vers une étiquette différente, 73–76

Détermination

Étiquette d'un fichier, 68–69

Étiquette de fenêtre, 54–55

Domination entre étiquettes, 23–25

Données

Détermination de l'étiquette, 68–69

Modification de l'étiquette, 69–72

Protection par MAC, 18–25

## Droits d'accès

- À la discrétion du propriétaire du fichier, 18
- Responsabilités de l'utilisateur, 26

**E**

E-mail, Application des étiquettes, 29

## Écran sans étiquette

- Écran de connexion, 33
- Verrouillage de l'écran, 45

Élément de menu Arrêt, 47–48

Élément de menu Suspendre le système, 47–48

## Espace de travail

- Définition de l'étiquette par défaut, 58
- Étiqueté, 28

## Étiquette

*Voir aussi* Autorisation

- Affichage dans Trusted Extensions, 79
- Affichée sur le bureau, 20, 21
- Composants, 19–21
- Définition à la connexion, 39
- Définition des autorisations à la connexion, 26–27
- Définition des étiquettes de session, 39
- Détermination par requête de fenêtre, 54–55
- Domination, 23–25
- Exemples d'étiquettes de l'industrie, 19
- Exemples d'étiquettes du gouvernement, 24
- Exemples de relations entre étiquettes, 25
- Modification de l'étiquette d'informations, 25
- Modification de l'étiquette d'un fichier, 73–76
- Modification de l'étiquette de données, 69–72
- Moyens de protéger les données, 26–29
- Plage, 19
- Relations, 23–25
- Type, 19
- Visible sur le bureau, 43
- Zone étiquetée, 22–23

## Étiquette de sensibilité

- Voir* Étiquette
- Type d'étiquette, 19

Examen des paramètres de sécurité, Procédure au cours de la connexion, 37–39

**F**

## Fichier

- \$HOME/.copy\_files, 53–54, 82
  - \$HOME/.link\_files, 53–54, 82
  - Accès aux fichiers d'initialisation de chaque étiquette, 53–54
  - Affichage dans un espace de travail, 48–49
  - Déplacement entre gestionnaires de fichiers, 73–76
  - Liaison entre gestionnaires de fichiers possédant différentes étiquettes, 76
  - Modification de l'étiquette, 73–76
- Fichiers d'initialisation
- Accès à chaque étiquette, 53–54
  - Dépannage lorsqu'ils sont personnalisés, 40

**G**

Gestionnaire d'allocation de périphériques (Device Allocation Manager), Libération de périphériques, 63

## Gestionnaire de fichiers

- Affichage du contenu, 48
- Dépannage en cas d'absence, 62
- Modification de l'étiquette, 73–76
- Modification de l'étiquette de fichiers, 76
- Sécurité dans Trusted Extensions, 85

## Gestionnaire de sélection, 70

## Gestionnaire de style

- Chemin de confiance requis, 57
  - Limites dans Solaris Trusted Extensions (CDE), 87–88
  - Modification des caractéristiques de session, 58
- Glisser-déposer, Effet sur les étiquettes, 25

**I**

Impression, Page de garde étiquetée standard, 86

Indicateur d'étiquette de fenêtre, 81

Indicateur de confiance, Manquant, 80

Informations, *Voir* Données

Instructions relatives aux e-mails, Responsabilités de l'utilisateur, 26

**L**

- Liaison de fichiers possédant différentes étiquettes, 76
  - À l'aide de `.link_files`, 53–54
- Libération de périphériques, Procédure de base, 63
- `.link_files`, fichier
  - Création, 53–54
  - Dépannage, 54
- `.link_files` Fichier, Description, 82
- Liste de contrôle d'accès (ACL, Access Control List), 18

**M**

- Menu Espace de travail, Suspendre le système, 47–48
- Menu principal, Arrêt, 47–48
- Menu Trusted Path
  - Adoption d'un rôle, 63–64
  - Allocate Device (Allouer le périphérique), 59–62
  - Change Workspace Label (Modifier l'étiquette d'un espace de travail), 64–65
  - Emplacement, 78
  - Modification du mot de passe, 57–58
- Menu Trusted Path (Chemin de confiance)
  - Description, 84
  - Query Window Label (Requête d'étiquette de fenêtre), 54–55
  - Utilisation, 51
- Menu Workspace (Espace de travail),
  - Personnalisation, 51–52
- Modification
  - De l'étiquette par des utilisateurs autorisés, 73–76
  - Étiquette d'un espace de travail, 64–65
  - Mot de passe, 57–58
  - Niveau de sécurité de données, 69–72, 73–76
- Modification d'étiquettes, Dépannage, 76
- Montage, Support amovible, 61
- Mot de passe, Responsabilités de l'utilisateur, 82–83

**N**

- Navigateur de fichiers
  - Affichage de l'étiquette d'un fichier, 68
  - Affichage du contenu, 49
  - Dépannage en cas d'absence, 62

- Not Found, message d'erreur, 30
- Not in Profile, message d'erreur, 30

**O**

- Objet
  - Définition, 20
  - Réutilisation, 29
- Option de menu Allocate Device (Allouer le périphérique), 59–62
- Option de menu Assume Rolerolename (Assumer le rôle `nom_du_rôle`), 63–64
- Option de menu Change Password (Modifier le mot de passe), 57–58
- Option de menu Change Workspace Label (Modifier l'étiquette d'un espace de travail), 64–65
- Option de menu Query Window Label (Requête d'étiquette de fenêtre), 54–55

**P**

- Pages de manuel dans Trusted Extensions, 50
- Pas de bande de confiance, Dépannage, 44
- Périphérique
  - Voir* Périphérique
  - Allocation, 59–62
  - Autorisation avant réutilisation, 29
  - Dépannage, 62
  - Protection, 17
  - Sécurité selon les exigences d'affectation, 81
  - Utilisation, 59–62
- Personnalisation
  - Bureau, 56
  - Menu Workspace (Espace de travail), 51–52
- `pfsh`, commande, *Voir* Shell du profil
- Plage d'étiquettes
  - Dépannage d'une station de travail avec une plage limitée, 40
  - Description, 19
- Pratiques de sécurité, Définition, 16
- Préhension sécurisée, Combinaison de touches, 57–58
- Procédures, *Voir* Utilisateur
- Processus de connexion, *Voir* Connexion

- Profil, *Voir* Profil de droits
  - Profil de droits, Définition, 30
  - Protection des fichiers
    - Basée sur les étiquettes, 26–29
    - DAC, 18
    - MAC, 18–25
    - Responsabilités de l'utilisateur, 26
- R**
- Raccourci clavier, Reprise de contrôle du focus du bureau, 57–58
  - Recherche
    - Aide en ligne de Trusted Extensions, 50–51
    - Événements du calendrier de chaque étiquette, 56
    - Menu Trusted Path, 63, 78
  - Réduction du niveau de sécurité d'informations, 25
  - Répertoire
    - Modification de l'étiquette, 73–76
    - Visibilité des répertoires personnels, 23
  - Répertoire personnel, Visible depuis la zone supérieure, 23
  - Responsabilités
    - Administrateurs, 30–31
    - Utilisateur concernant la protection des données, 26
    - Utilisateur lors de la déconnexion, 46–47
    - Utilisateur pour la sécurité du mot de passe, 82–83
    - Utilisateur pour le nettoyage des supports, 29
  - Responsabilités de l'utilisateur
    - Lors du départ de la station de travail, 44
    - Protection des données, 26
    - Sécurité du mot de passe, 82–83
  - Rôle
    - Ajout d'un espace de travail étiqueté, 65–66
    - Compte utilisateur spécial, 29–31
    - Modification de l'étiquette des espaces de travail, 64–65
  - Rôle admin, *Voir* Rôle d'administrateur système
  - Rôle d'administrateur de sécurité
    - Contact à propos d'un indicateur de confiance manquant, 80
    - Contact si la bande de confiance est absente, 44
    - Responsabilités, 30–31
  - Rôle d'administrateur système, Responsabilités, 30–31
  - Rôle d'opérateur, Responsabilités, 30–31
  - Rôle oper, *Voir* Rôle d'opérateur
  - Rôle root, Responsabilités, 30–31
  - Rôle secadmin, *Voir* Rôle d'administrateur de sécurité
  - Rôles
    - Responsabilités, 30–31
    - Rôles communs, 30–31
- S**
- Sécurité de l'éditeur de texte dans Trusted Extensions, 86
  - Sécurité de l'horloge dans Trusted Extensions, 85
  - Sécurité de l'outil Printer dans Trusted Extensions, 86–87
  - Sécurité de la corbeille dans Trusted Extensions, 88
  - Sécurité des messages dans Trusted Extensions, 86
  - Sécurité du calendrier dans Trusted Extensions, 85
  - Sécurité du gestionnaire d'applications dans Trusted Extensions, 88
  - Sélection, Modification de l'étiquette, 69–72
  - Session
    - Choix des autorisations, 26–27
    - Définition du niveau, 39
    - Effet de sélection du niveau, 27–28
    - Niveau unique ou multiniveau, 26–27
  - Session à niveau unique, Définition, 26–27
  - Session multiniveau, Définition, 26–27
  - Shell de profil, Définition, 30
  - Solaris Trusted Extensions (CDE), *Voir* CDE
  - Stop-A (L1-A), combinaison de touches, 48
  - Stratégie, *Voir* Stratégie de sécurité
  - Stratégie de sécurité
    - Définition, 16, 98
  - Sujet, Définition, 20
  - Symbole de confiance
    - Description, 80
    - Icône d'inviolabilité, 17
    - Sur l'espace de travail, 43
  - Système multiécran, Bande de confiance, 43

**T**

- Tableau de bord
  - Description des applications de confiance, 83
  - Restauration après réduction, 83
- Tâches, *Voir* Utilisateur
- Trusted CDE
  - Bureau Trusted Extensions, 33
  - Choix comme bureau, 36
  - Personnalisation du bureau, 56
  - Personnalisation du menu Workspace (Espace de travail), 51–52
  - Recherche d'aide en ligne pour Trusted Extensions, 50
  - Utilisation du gestionnaire de style, 57
- Trusted Extensions
  - Fonction visible, 77–81
  - Présentation, 15–16
- Trusted JDS
  - Aide en ligne, 51
  - Bureau Trusted Extensions, 33
  - Choix comme bureau, 36
  - Personnalisation du bureau, 56
  - Sécurité de l'espace de travail, 88–89
- Type d'étiquette, 19

**U**

- Usurpation, Définition, 99
- Usurpation d'identité, Définition, 17
- Utilisateur
  - Accès aux fichiers d'initialisation de chaque étiquette, 53–54
  - Adoption d'un rôle, 63–64
  - Affichage des fichiers dans un espace de travail, 48–49
  - Aide en ligne, 50
  - Ajout d'un espace de travail étiqueté, 65–66
  - Allocation d'un périphérique, 59–62
  - Arrêt d'un poste de travail, 47–48
  - Autorisé à modifier l'étiquette d'un fichier, 73–76
  - Autorisé à modifier le niveau de sécurité de données, 69–72
  - Basculement vers un espace de travail possédant une étiquette différente, 66–67

**Utilisateur (Suite)**

- Connexion à une étiquette différente, 58
- Déconnexion, 46–47
- Déplacement d'une fenêtre vers un espace de travail possédant une étiquette différente, 67–68
- Déplacement de données entre étiquettes, 69–72
- Déplacement de fichiers entre étiquettes, 73–76
- Détermination de l'étiquette d'un fichier, 68–69
- Déverrouillage de votre écran, 46
- Liaison de fichiers possédant différentes étiquettes, 76
- Modification de l'étiquette d'un espace de travail, 64–65
- Modification du mot de passe, 57–58
- Personnalisation du menu Workspace (Espace de travail), 51–52
- Recherche d'aide en ligne pour Trusted Extensions, 50–51
- Responsabilités
  - Autorisations des périphériques, 29
  - Lors du départ de la station de travail, 46–47
  - Protection des données, 26
  - Sécurité du mot de passe, 82–83
  - Verrouillage de l'écran, 44–46
- Utilisation d'un bureau sécurisé, Niveau unique ou multiniveau, 36
- Utilisation d'un périphérique, *Voir* Allocation d'un périphérique

**V**

- Vérification des paramètres de sécurité, Boîte de dialogue de Dernière connexion, 35
- Visibilité
  - Bande de confiance, 20, 21, 44, 78
  - Étiquettes après la connexion, 33–34
  - Lecture de répertoires personnels de niveau inférieur, 23
  - Sécurité du bureau, 43–44

**Z**

## Zone

- Étiquetée, 22–23

- Visibilité du répertoire personnel, 23

## Zone de commutation de l'espace de travail

- Dans le CDE Trusted Extensions, 84

- Illustration, 28

