Guide d'administration de Solaris™ Security Toolkit 4.2

Sun Microsystems, Inc.
www.sun.com

Référence 819-3788-10
Août 2005, révision A

Communiquez vos commentaires sur ce document à : http://www.sun.com/hwdocs/feedback

Papier
recyclable

Adobe PostScript

Table des matières

Figures

Tableaux

Exemples de code

Préface

Ce manuel contient des informations de référence facilitant la compréhension et l'utilisation du logiciel Solaris™ Security Toolkit. Il est essentiellement destiné aux utilisateurs qui souhaitent sécuriser les systèmes d'exploitation (SE) Solaris™ 8, 9 et 10 à l'aide du logiciel Solaris Security Toolkit, par exemple les administrateurs, les consultants, etc., qui déploient de nouveaux systèmes Sun ou sécurisent des systèmes déployés. Les instructions s'appliquent au logiciel en mode JumpStart™ ou en mode autonome.

Avant de lire ce document

Vous devez être un administrateur système certifié Sun pour Solaris™ ou un administrateur réseau certifié Sun pour Solaris™. Vous devez maîtriser les protocoles et les topologies standard de réseau.

Étant donné que ce document s'adresse à un public varié, votre expérience et vos connaissances personnelles en matière de sécurité détermineront le type de consultation et d'utilisation que vous en ferez.

Organisation de ce document

Ce manuel est un guide de l'utilisateur. Il contient des informations, des instructions et des directives sur l'utilisation du logiciel en vue de sécuriser des systèmes. Cet ouvrage est organisé comme suit :

Le **chapitre 1** décrit la logique et l'objectif du logiciel Solaris Security Toolkit. Il couvre les composants clés, les fonctions, les avantages et les plates-formes prises en charge.

Le **chapitre 2** propose une méthode de sécurisation des systèmes. Vous pouvez appliquer le processus Solaris Security Toolkit avant de sécuriser les systèmes à l'aide du logiciel correspondant.

Le **chapitre 3** fournit des instructions sur le téléchargement, l'installation et l'exécution du logiciel Solaris Security Toolkit et d'autres logiciels de sécurité.

Le **chapitre 4** propose des informations et des procédures permettant d'annuler les modifications introduites par le logiciel Solaris Security Toolkit pendant les sécurisations.

Le **chapitre 5** décrit la configuration et la gestion des serveurs JumpStart en vue d'utiliser le logiciel Solaris Security Toolkit.

Le **chapitre 6** décrit l'audit (la validation) de la sécurité d'un système à l'aide du logiciel Solaris Security Toolkit. Utilisez les informations et les procédures figurant dans ce chapitre pour maintenir un profil de sécurité donné après la sécurisation.

Le **chapitre 7** applique à un scénario réaliste les informations contenues dans les chapitres précédents pour installer et sécuriser un nouveau système.

Utilisation des commandes UNIX

Les commandes et procédures de base UNIX®, telles que l'arrêt ou le démarrage du système, ou encore la configuration des périphériques, ne sont pas traitées dans ce document. Pour de plus amples informations à ce sujet, reportez-vous aux sources suivantes :

- la documentation accompagnant les logiciels livrés avec le système ;
- la documentation relative au système d'exploitation Solaris, à l'adresse `http://docs.sun.com.`

Invites de shell

Shell	Invite
C	*nom-ordinateur*%
superutilisateur C	*nom-ordinateur*#
Bourne et Korn	$
Superutilisateur Bourne et Korn	#

Conventions typographiques

Style*	Signification	Exemples
AaBbCc123	Noms de commandes, de fichiers et de répertoires ; sortie affichée à l'écran	Modifiez le fichier .login. Utilisez la commande ls -a pour afficher la liste de tous les fichiers. % Vous avez reçu du courrier.
AaBbCc123	Caractères saisis par l'utilisateur, par opposition à la sortie affichée à l'écran	% **su** Mot de passe :
AaBbCc123	Titres d'ouvrages, nouveaux termes ou expressions, mots à mettre en évidence. Variables de ligne de commande à remplacer par des noms ou des valeurs réels.	Lisez le chapitre 6 du *Guide de l'utilisateur*. Ces paramètres sont appelés options de *classe*. Vous *devez* vous connecter en tant que superutilisateur pour effectuer cette opération. Pour supprimer un fichier, tapez rm *nom_du_fichier*.

* Il est possible que les paramètres de votre navigateur soient différents.

Utilisation de termes génériques pour les modèles de matériel

Les systèmes haut de gamme Sun Fire™ ont pour référence les numéros de modèle suivants :

- E25K
- E20K
- 15K
- 12K

Les systèmes milieu de gamme Sun Fire™ ont pour référence les numéros de modèle suivants :

- E6900
- E4900
- 6800
- 4810
- 4800
- 3800

Les systèmes entrée de gamme Sun Fire™ ont pour référence les numéros de modèle suivants :

- E2900
- Netra 1280
- V1280
- V890
- V880
- V490
- V480

Systèmes matériels pris en charge

Le logiciel Solaris Security Toolkit 4.2 prend en charge le système SPARC® 64 bits *uniquement* et les systèmes x86/x64 exécutés sous le SE Solaris 10. Il ne reconnaît pas les systèmes SPARC 32 bits exécutés sous Solaris 8 et 9, par exemple Ultra 2 Creator 3D.

Versions du SE Solaris prises en charge

Le support Sun du logiciel Solaris Security Toolkit est disponible *uniquement* pour les systèmes d'exploitation Solaris 8, 9 et 10.

Remarque – Dans le cadre de l'utilisation du logiciel Solaris Security Toolkit 4.2, Solaris 10 peut être utilisé *uniquement* sur des domaines de systèmes haut de gamme Sun Fire et *non* sur le contrôleur système (SC).

Bien qu'il soit possible d'utiliser le logiciel sous les SE Solaris 2.5.1, 2.6 et 7, le support Sun du logiciel *n'est pas* disponible pour ces systèmes d'exploitation.

Le logiciel Solaris Security Toolkit détecte automatiquement la version du SE Solaris installée, puis exécute les tâches appropriées pour cette version.

Dans les exemples du présent document, les scripts vérifiant la version du SE recherchent les versions 5.*x* (versions de SunOS™) et non les versions 2.*x*, 7, 8, 9 ou 10 (versions du SE Solaris). Le TABLEAU P-1 indique la corrélation entre les versions de SunOS et du SE Solaris.

TABLEAU P-1 Corrélation entre les versions de SunOS et du SE Solaris

Version de SunOS	Version du SE Solaris
5.5.1	2.5.1
5.6	2.6
5.7	7
5.8	8
5.9	9
5.10	10

Versions de System Management Services (SMS) prises en charge

Si vous utilisez System Management Services (SMS) 1.4, 1.4.1 et 1.5 pour exécuter le SC sur des systèmes haut de gamme Sun Fire, le logiciel Solaris Security Toolkit 4.2 est pris en charge par tous les SE Solaris 8 et 9. Aucune version de SMS n'est reconnue sous le Solaris 10 lorsque vous utilisez le logiciel Solaris Security Toolkit 4.2.

Remarque – Dans le cadre de l'utilisation du logiciel Solaris Security Toolkit 4.2, Solaris 10 peut être utilisé *uniquement* sur des domaines et *non* sur le contrôleur système (SC).

Documentation connexe

Les documents en ligne sont disponibles à l'adresse suivante :

`http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise_computing/systems_management/sst/index.html`

Application	Titre	Référence	Format	Emplacement
Notes de version	*Notes de version de Solaris Security Toolkit 4.2*	819-3795-10	PDF HTML	En ligne
Référence	*Solaris Security Toolkit 4.2 Reference Manual*	819-1503-10	PDF HTML	En ligne
Pages Man	*Solaris Security Toolkit 4.2 Man Page Guide*	819-1505-10	PDF	En ligne

Documentation, support et formation

Fonction Sun	URL	Description
Documentation	http://www.sun.com/documentation/	Téléchargement de documents PDF et HTML ; commandes de documents imprimés
Support	http://www.sun.com/support/	Support technique et téléchargement de patchs
Formation	http://www.sun.com/training/	Formations Sun

Sites Web tiers

Sun n'assume aucune responsabilité quant à la disponibilité des sites Web tiers mentionnés dans ce document. Sun ne peut être tenu pour responsable des informations, du matériel promotionnel ou publicitaire, des produits ou autre matériel contenus sur ces sites ou accessibles à partir de ces sites ou sources. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation de tout contenu, biens ou services disponibles sur ou dans ces sites ou ressources et termes.

Vos commentaires sont les bienvenus

Nous souhaitons améliorer notre documentation. Vos commentaires et suggestions sont donc les bienvenus. Vous pouvez les envoyer à partir du site suivant :

http://www.sun.com/hwdocs/feedback

N'oubliez pas de joindre le titre et la référence du document à votre message :

Guide d'administration de Solaris Security Toolkit 4.2, référence 819-3788-10.

CHAPITRE 1

Introduction

Ce chapitre décrit la logique et l'objectif du logiciel Solaris Security Toolkit. Il couvre les composants clés, les fonctionnalités, les avantages et les plates-formes prises en charge. Ce chapitre contient des directives pour le contrôle de version des modifications et des déploiements, et fournit des informations importantes sur la personnalisation du logiciel Solaris Security Toolkit.

Ce chapitre contient les sections suivantes :

Sécurisation de systèmes à l'aide du logiciel Solaris Security Toolkit

Le logiciel Solaris Security Toolkit, couramment appelé kit d'outils JASS (JumpStart Architecture and Security Scripts), propose un mécanisme automatisé, extensible et évolutif permettant de construire des systèmes d’exploitation Solaris et de maintenir ces derniers sécurisés. À l'aide du logiciel Solaris Security Toolkit, vous pouvez sécuriser vos systèmes et effectuer des audits de sécurité.

La liste suivante répertorie les termes de ce guide qu'il est important de maîtriser :

- **Sécurisation** – Modification des configurations du SE Solaris afin d’améliorer la sécurité d'un système.
- **Audit** – Processus permettant de déterminer si la configuration d'un système est conforme à un profil de sécurité prédéfini.

Remarque – Le terme *audit* désigne le processus automatisé qui permet au logiciel Solaris Security Toolkit de valider un niveau de sécurité par rapport à un profil de sécurité prédéfini. L'emploi de ce terme dans cet ouvrage *ne garantit pas* la complète sécurisation du système contrôlé après l'utilisation de l'option d'audit.

- **Score** – Nombre d'échecs détectés lors d'un audit. Lorsqu'aucun échec, quel que soit le type, n'est détecté, le score est `0`. Le logiciel Solaris Security Toolkit augmente le score (également connu sous le nom de valeur de vulnérabilité) de `1` pour chaque échec détecté.

Il existe deux modes d'installation du logiciel Solaris Security Toolkit décrits brièvement dans la dernière partie de cette section :

- « Mode JumpStart » à la page 2
- « Mode autonome » à la page 3

Indépendamment du mode d'installation d'un système, vous pouvez vous servir du logiciel Solaris Security Toolkit pour sécuriser et minimiser les systèmes. Utilisez ensuite périodiquement le logiciel Solaris Security Toolkit pour vérifier que le profil de sécurité des systèmes sécurisés n'a pas été modifié par accident ou par malveillance.

Mode JumpStart

L'installation et la configuration du système doivent être automatisées autant que possible. L'idéal serait qu'elles soient automatisées à 100 %. Ces tâches comprennent l'installation et la configuration du système d'exploitation, la configuration du réseau, les comptes utilisateurs, les applications et la sécurisation. Le logiciel JumpStart est une technologie qui permet d'automatiser les installations du SE Solaris. Il fournit un mécanisme d'installation de systèmes sur un réseau sans intervention humaine ou presque. Le logiciel Solaris Security Toolkit propose une structure et des scripts permettant la mise en oeuvre et l'automatisation de la plupart des tâches associées à la sécurisation de systèmes SE Solaris dans les installations basées sur le logiciel JumpStart. Pour obtenir JumpStart Enterprise Toolkit (JET), qui facilite les installations basées sur JumpStart et inclut des modules prenant en charge la sécurisation au moyen du logiciel Solaris Security Toolkit, consultez le site de téléchargement de Sun à l'adresse suivante :

`http://www.sun.com/download/`

Pour de plus amples informations sur la technologie JumpStart, reportez-vous à l'ouvrage Sun BluePrints™ *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Mode autonome

Le logiciel Solaris Security Toolkit dispose d'un mode autonome. Ce mode donne accès à la même fonctionnalité de sécurisation que le mode JumpStart, mais sur des systèmes déployés. Dans les deux modes, les modifications de sécurité peuvent, et doivent être, personnalisées afin de remplir les conditions de sécurité requises par votre système.

Indépendamment du mode d'installation d'un système, vous pouvez utiliser le logiciel Solaris Security Toolkit pour sécuriser les systèmes. Utilisez ensuite périodiquement le logiciel Solaris Security Toolkit pour vérifier que la configuration des systèmes sécurisés n'a pas été modifiée par accident ou par malveillance.

Composants du logiciel

Cette section présente la structure des composants du logiciel Solaris Security Toolkit. Le logiciel Solaris Security Toolkit se compose d'une collection de fichiers et de répertoires. La FIGURE 1-1 illustre la structure du logiciel.

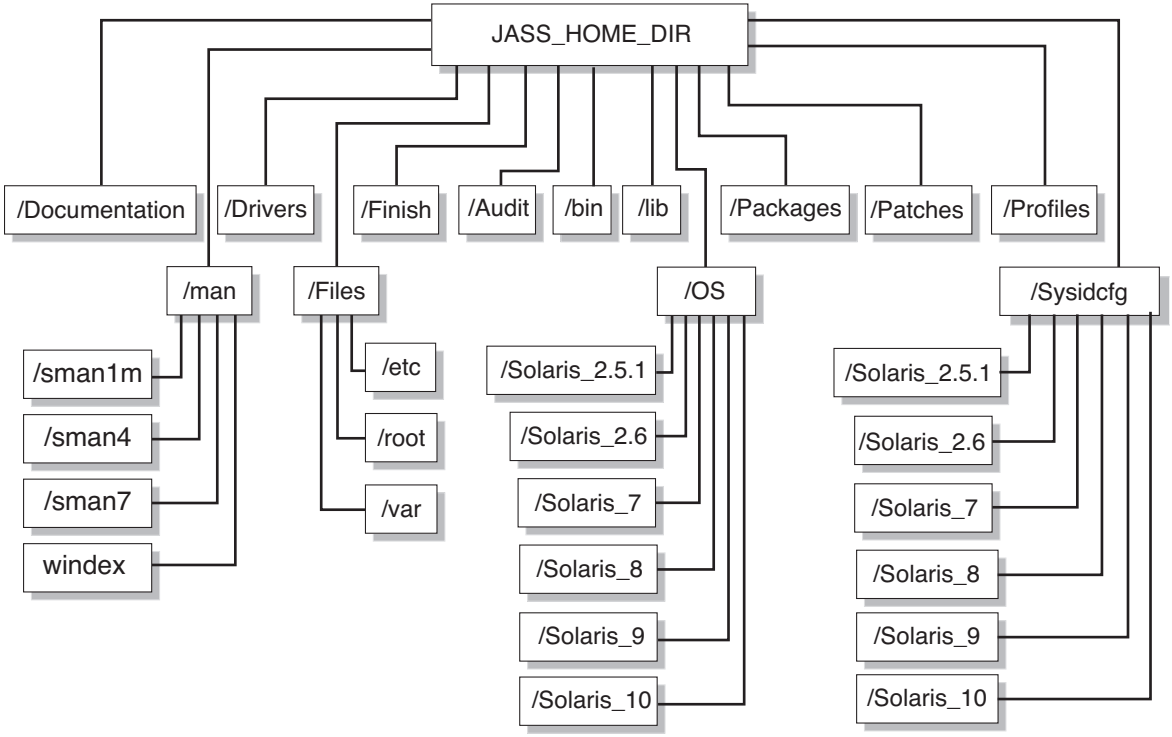

FIGURE 1-1 Structure des composants du logiciel

Les fichiers programme ou de commande suivants se trouvent dans le répertoire `/bin` :

- `add-client` – Programme auxiliaire JumpStart pour l'ajout de clients dans un environnement JumpStart
- `rm-client` – Programme auxiliaire JumpStart pour la suppression de clients d'un environnement JumpStart
- `make-jass-pkg` – Commande qui offre la possibilité de créer un package du SE Solaris à partir du contenu du répertoire Solaris Security Toolkit, pour simplifier la distribution interne d'une configuration personnalisée Solaris Security Toolkit
- `jass-check-sum` – Commande qui permet de déterminer si des fichiers modifiés par le logiciel Solaris Security Toolkit ont été changés et ce, à l'aide d'une somme de contrôle créée à chaque exécution du logiciel Solaris Security Toolkit.
- `jass-execute` – Commande qui exécute la plupart des fonctionnalités du logiciel Solaris Security Toolkit

Répertoires

Les composants de l'architecture Solaris Security Toolkit sont organisés dans les répertoires suivants :

- `/Audit`
- `/bin`
- `/Documentation`
- `/Drivers`
- `/Files`
- `/Finish`
- `/lib`
- `/man`
- `/OS`
- `/Packages`
- `/Patches`
- `/Profiles`
- `/Sysidcfg`

Chacun de ces répertoires est décrit dans cette section. Le cas échéant, chaque script, fichier de configuration ou sous-répertoire est mentionné dans la liste. Pour de plus amples informations, cette section renvoie également à d'autres chapitres.

La structure du répertoire Solaris Security Toolkit se base sur la structure illustrée dans l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Répertoire `Audit`

Ce répertoire contient les scripts audit qui permettent d'évaluer la conformité du système par rapport à un profil de sécurité ou un ensemble de scripts audit défini. Les scripts de ce répertoire sont organisés en plusieurs catégories :

- Disable
- Enable
- Install
- Minimize
- Print
- Remove
- Set
- Update

Pour une liste détaillée des scripts de chaque catégorie et une description de chaque script, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Répertoire `Documentation`

Ce répertoire contient des fichiers texte destinés à l'utilisateur, tels que les fichiers `README`, `EOL_NOTICE` et `INSTALL`.

Répertoire `man`

Ce répertoire contient des sous-répertoires correspondant aux sections des pages man de commandes, de fonctions et de pilotes. Il inclut également le fichier `windex`, index des commandes fourni à titre gracieux.

Pour de plus amples informations sur les pages man, reportez-vous à celles-ci ou au manuel *Solaris Security Toolkit 4.2 Man Page Guide*.

Répertoire `Drivers`

Ce répertoire contient des fichiers d'informations de configuration indiquant les fichiers exécutés et installés quand vous utilisez le logiciel Solaris Security Toolkit. Il inclut des pilotes, des scripts et des fichiers de configuration.

Exemple de pilotes et de scripts présents dans le répertoire `Drivers` :

- `audit_{private|public}.funcs`
- `common_{log|misc}.funcs`
- `{config|hardening|secure}.driver`
- `driver.{init|run}`
- `driver_{private|public}.funcs`

- `finish.init`
- `server-{config|hardening|secure}.driver`
- `suncluster3x-{config|hardening|secure}.driver`
- `sunfire_15k_sc-{config|hardening|secure}.driver`
- `undo.{funcs|init|run}`
- `user.init.SAMPLE`
- `user.run.SAMPLE`

Tous les pilotes inclus avec le logiciel Solaris Security Toolkit possèdent *trois fichiers* :

- *nom*`-{config|hardening|secure}.driver`

Ces trois fichiers sont placés entre parenthèses dans la liste précédente, par exemple `sunfire_15k_sc-{config|hardening|secure}.driver`. Les noms de ces fichiers sont indiqués par souci de précision. Toutefois, pour exécuter un pilote, utilisez *uniquement* `secure.driver` ou le *nom*`-secure.driver`. Ce pilote appelle *automatiquement* les pilotes associés.

L'architecture de Solaris Security Toolkit comprend des informations de configuration pour que vous puissiez utiliser les scripts driver, finish et audit dans différents environnements, *sans* avoir à les modifier. Toutes les variables utilisées dans les scripts finish et audit sont conservées dans un ensemble de fichiers de configuration. Ces fichiers de configuration sont importés par les pilotes, afin que les scripts finish et audit puissent disposer de ces variables quand elles sont appelées par les pilotes.

Le logiciel Solaris Security Toolkit contient quatre fichiers principaux de configuration, qui se trouvent tous dans le répertoire `Drivers` :

- `driver.init`
- `finish.init`
- `user.init`
- `user.run`

Le fichier `user.run` est le fichier dans lequel vous écrivez les versions améliorées ou de remplacement des fonctions de Solaris Security Toolkit, qui, le cas échéant, sont automatiquement utilisées.

Attention – Modifiez les définitions de variable dans le fichier de configuration `user.init` *uniquement*, *jamais* dans les fichiers de configuration `driver.init` et `finish.init`.

Les scripts finish appelés par les pilotes se trouvent dans le répertoire `Finish`. Les scripts audit appelés par les pilotes se trouvent dans le répertoire `Audit`. Les fichiers installés par les pilotes sont lus à partir du répertoire `Files`. Pour de plus amples informations sur les scripts finish, reportez-vous au chapitre 4 du manuel *Solaris Security Toolkit 4.2 Reference Manual*. Pour de plus amples informations sur les scripts audit, reportez-vous au chapitre 5 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

La FIGURE 1-2 représente un organigramme du flux de contrôle du pilote.

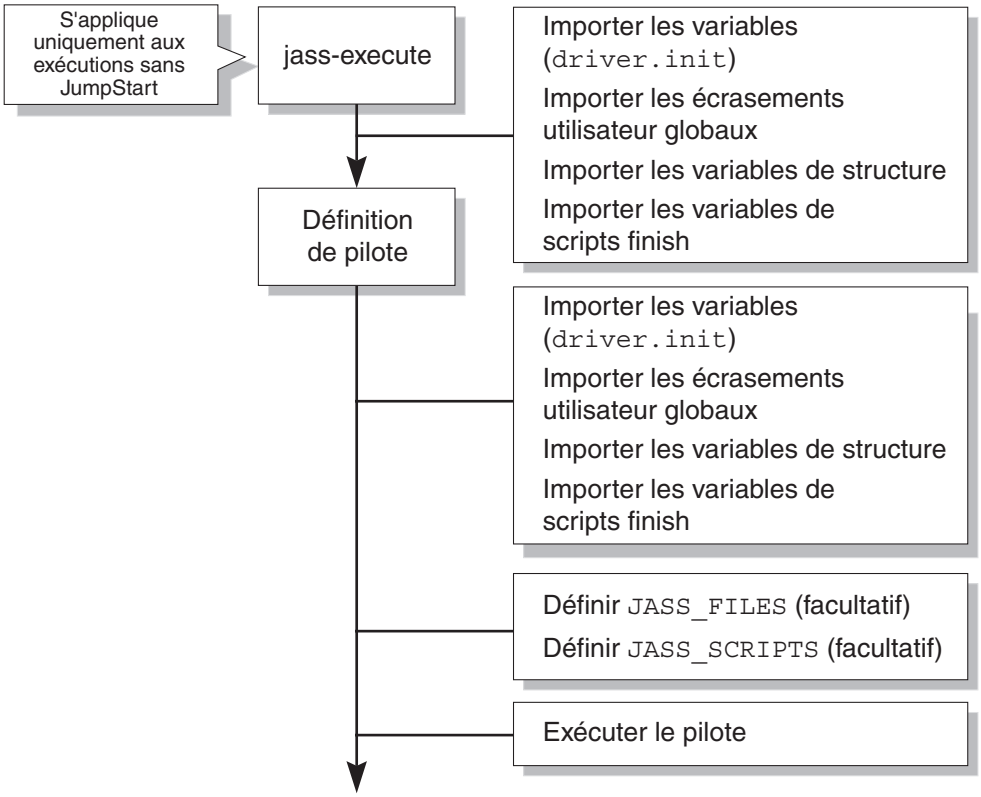

FIGURE 1-2 Flux de contrôle du pilote

1. Lorsque JumpStart *n'est pas* utilisé, le pilote exécute la commande jass-execute. JumpStart appelle directement le pilote et non la commande `jass-execute`.
2. Le pilote risque de définir explicitement les variables.
3. Le pilote importe toutes les variables d'environnement des différents fichiers `.init`.
4. Il définit les variables d'environnement `JASS_FILES` et `JASS_SCRIPTS`. Ces définitions sont facultatives ; il est possible de définir un seul environnement, les deux ou aucun.

   Pour de plus amples informations sur la définition des variables d'environnement `JASS_FILES` et `JASS_SCRIPTS`, reportez-vous au chapitre 7 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

5. Le pilote appelle `driver.run` pour l'exécution des tâches définies par les variables d'environnement `JASS_FILE` et `JASS_SCRIPTS`.

6. (*Facultatif*) Le pilote définit un comportement de pilote spécifique qui peut être utilisé pour ignorer les valeurs système par défaut de `finish.init` ou`user.init`. Dans l'EXEMPLE DE CODE 1-1, le pilote définit explicitement la variable `JASS_PASS_HISTORY` sur `4`.

L'EXEMPLE DE CODE 1-1 illustre le code de flux de contrôle du pilote.

EXEMPLE DE CODE 1-1 Code de flux de contrôle du pilote

```
DIR="`/bin/dirname $0`"
JASS_PASS_HISTORY="4"
export DIR
. ${DIR}/driver.init

JASS_FILES="
                          /etc/cron.d/cron.allow
                          /etc/default/ftpd
                          /etc/default/telnetd
"

JASS_SCRIPTS="
                          install-at-allow.fin
                          remove-unneeded-accounts.fin
"
. ${DIR}/driver.run
```

1. Cet exemple de code définit et exporte la variable d'environnement `DIR` de sorte que les pilotes reconnaissent le répertoire de départ.

2. Le pilote définit explicitement la variable `JASS_PASS_HISTORY` sur `4`.

3. Il lit les différents fichiers `.init` (en commençant par le fichier `driver.init`).

4. La variable d'environnement `JASS_FILES` est définie comme contenant les fichiers copiés du répertoire `JASS_HOME_DIR/Files` sur le client.

5. La variable d'environnement `JASS_SCRIPTS` est alors définie avec les scripts finish exécutés par le logiciel Solaris Security Toolkit.

6. L'exécution de la sécurisation commence par l'appel du pilote `driver.run`. Le pilote `driver.run` copie les fichiers spécifiés par`JASS_FILES` et exécute les scripts spécifiés par `JASS_SCRIPTS`.

Répertoire `Files`

Ce répertoire est utilisé par la variable d'environnement `JASS_FILES` et le script `driver.run` pour stocker les fichiers copiés sur le client JumpStart.

Ce répertoire contient les fichiers suivants :

- `/.cshrc`
- `/.profile`
- `/etc/default/sendmail`
- `/etc/dt/config/Xaccess`
- `/ftpd/banner.msg`
- `/etc/hosts.allow`
- `/etc/hosts.allow-15k_sc`
- `/etc/hosts.allow-server`
- `/etc/hosts.allow-suncluster`
- `/etc/hosts.deny`
- `/etc/init.d/klmmod`
- `/etc/init.d/nddconfig`
- `/etc/init.d/set-tmp-permissions`
- `/etc/init.d/sms_arpconfig`
- `/etc/init.d/swapadd`
- `/etc/issue`
- `/etc/motd`
- `/etc/opt/ipf/ipf.conf`
- `/etc/opt/ipf/ipf.conf-15k_sc`
- `/etc/opt/ipf/ipf.conf-server`
- `/etc/security/audit_class+5.10`
- `/etc/security/audit_class+5.8`
- `/etc/security/audit_class+5.9`
- `/etc/security/audit_control`
- `/etc/security/audit_event+5.10`
- `/etc/security/audit_event+5.8`
- `/etc/security/audit_event+5.9`
- `/etc/sms_domain_arp`
- `/etc/sms_sc_arp`
- `/etc/syslog.conf`
- `/root/.cshrc`
- `/root/.profile`
- `/var/opt/SUNWjass/BART/rules`
- `/var/opt/SUNWjass/BART/rules-secure`

Répertoire `Finish`

Ce répertoire contient les scripts finish qui introduisent les modifications et les mises à jour du système lors de l'exécution. Les scripts de ce répertoire sont organisés en plusieurs catégories :

- Disable
- Enable
- Install
- Minimize
- Print
- Remove
- Set
- Update

Pour une liste détaillée des scripts de chaque catégorie et une description de chaque script, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Répertoire `OS`

Ce répertoire contient *uniquement* les images du SE Solaris. Ces images sont utilisées par le processus d'installation du logiciel JumpStart comme source du SE Solaris pour les installations client. Le script `add_client` accepte les versions du SE Solaris contenues dans ce répertoire comme arguments, à condition que les noms de répertoires respectent les conventions d'attribution de nom du SE Solaris Security Toolkit suivantes.

Pour de plus amples informations sur le chargement et la modification des images du SE Solaris, reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Les noms attribués lors de l'installation respectent les conventions indiquées ci-après.

SE Solaris

Utilisez la convention d'attribution de nom suivante pour le SE Solaris :

`Solaris_`*version du SE_année (4 chiffres)_mois (2 chiffres) de la version du CD-ROM*

Par exemple, le nom de répertoire du CD-ROM du SE Solaris 10, daté de mars 2005, est `Solaris_10_2005-03`. En séparant les mises à jour et les versions du SE Solaris, il est possible d'exercer un contrôle précis en vue des tests et des déploiements.

Plates-formes Solaris pour x86/x64

Le répertoire du SE Solaris pour les plates-formes x86/x64 doit avoir le nom suivant :

`Solaris_`*version du SE_année (4 chiffres)_mois (2 chiffres) de la version du CD-ROM*`_ia`

Par exemple, si la date de version du SE Solaris pour les plates-formes x86/x64 est mars 2005, le répertoire doit avoir le nom suivant : `Solaris_10_2005-03_ia`.

Répertoire `Packages`

Ce répertoire contient les packages qui peuvent être installés avec un script finish et vérifiés par un script audit. Par exemple, le package Open Secure Shell peut être stocké dans le répertoire `Packages` de sorte que le script finish approprié installe le logiciel, au besoin.

Plusieurs scripts finish et audit inclus dans le logiciel Solaris Security Toolkit effectuent l'installation du logiciel, des tâches de configuration de base et de vérification. Les scripts qui installent et vérifient le logiciel à partir du répertoire `Packages` comprennent les éléments suivants :

- `install-fix-modes.{fin|aud}`
- `install-jass.{fin|aud}`
- `install-md5.{fin|aud}`
- `install-openssh.{fin|aud}`

Répertoire `Patches`

Ce répertoire doit être utilisé pour le stockage de clusters de patchs recommandés et de sécurité pour le SE Solaris. Les patchs requis doivent être téléchargés et extraits dans ce répertoire.

Le stockage et l'extraction des patchs dans ce répertoire optimise l'installation. Lorsque les patchs ont été extraits dans ce répertoire, le script d'installation des patchs du logiciel Solaris Security Toolkit automatise l'installation. Ainsi, vous *n'avez pas* à extraire manuellement les clusters de patchs chaque fois que vous installez un système.

Créez des sous-répertoires pour chaque version du SE Solaris utilisée. Par exemple, le répertoire `Patches` peut contenir les répertoires `9_Recommended` et `10_Recommended`.

Le logiciel Solaris Security Toolkit prend en charge les clusters de patchs du SE Solaris pour les plates-formes x86/x64. La convention d'attribution de nom pour ces clusters de patchs est la même que celle du service SunSolve OnLine℠.

Le format est `<version>_x86_Recommended`. Le cluster de patchs du SE Solaris 10 pour les plates-formes x86/x64 se trouve dans un répertoire intitulé `10_x86_Recommended`.

Répertoire `Profiles`

Ce répertoire contient tous les profils JumpStart. Ces profils renferment des informations de configuration utilisées par le logiciel JumpStart afin de déterminer les clusters du SE Solaris nécessaires à l'installation (installation de base, d'utilisateur final, de développeur ou de distribution complète, par exemple), à l'organisation des disques et au type d'installation (autonome, par exemple).

Les profils JumpStart sont répertoriés et utilisés dans le fichier `rules` pour définir la création de systèmes spécifiques ou de groupes de systèmes.

Répertoire `Sysidcfg`

Le répertoire `Sysidcfg`, similaire au répertoire `Profiles`, contient des fichiers utilisés *uniquement* lors d'installations en mode JumpStart. Ces fichiers automatisent les installations du SE Solaris en fournissant les informations d'installation requises. Les informations spécifiques au SE Solaris sont stockées dans une arborescence de répertoires distincte.

Chaque version du SE Solaris possède son propre répertoire. Le répertoire contenant chaque version est intitulé `Solaris_`*version du SE*. Le logiciel Solaris Security Toolkit contient des fichiers échantillon `sysidcfg` pour les versions 2.5.1 à 10 du SE Solaris.

Les fichiers échantillon `sysidcfg` peuvent être étendus à d'autres types de fichiers, réseau ou hôte par exemple. Le logiciel Solaris Security Toolkit prend en charge les fichiers arbitraires `sysidcfg`.

Pour de plus amples informations sur les fichiers `sysidcfg`, reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Référentiel de données

Bien que n'appartenant pas à la structure de répertoires `JASS_HOME_DIR`, le référentiel de données, ou `JASS_REPOSITORY`, prend en charge les annulations de Solaris Security Toolkit, enregistre les données relatives à chaque exécution et les données du journal d'exécution, et maintient un fichier manifeste des fichiers modifiés par le logiciel. Ce répertoire se trouve à l'emplacement suivant : `/var/opt/SUNWjass/runs/`*horodatage*.

Maintien du contrôle de version

Il est *essentiel* de maintenir le contrôle de version de tous les fichiers et scripts utilisés par le logiciel Solaris Security Toolkit pour deux raisons.

1. L'un des objectifs de cet environnement est d'offrir la possibilité de recréer une installation du système. Cet objectif serait impossible sans un instantané de toutes les versions de fichier utilisées pendant une installation.
2. Étant donné que ces scripts remplissent des fonctions de sécurité, et constituent des processus vitaux pour de nombreuses organisations, vous devez faire preuve de *la plus grande prudence* afin que *seules* les modifications nécessaires et testées soient mises en oeuvre.

Un package de contrôle de version Source Code Control System (SCCS) est inclus dans le package du SE Solaris `SUNWsprot`. Vous pouvez utiliser un autre logiciel de contrôle de version disponible en freeware ou en vente dans le commerce pour gérer les informations de version. Quel que soit le produit de contrôle de version employé, établissez une procédure de gestion des mises à jour et capturez les informations de version lors de recréations ultérieures.

Utilisez une solution de gestion d'intégrité en plus du contrôle de version pour déterminer si le contenu des fichiers a été modifié. Bien que les utilisateurs privilégiés d'un système aient la possibilité de contourner le système de contrôle de version, ils ne peuvent pas facilement éviter le système de gestion de l'intégrité, qui maintient sa base de données d'intégrité sur un système distant. Les solutions de gestion de l'intégrité fonctionnent mieux si elles sont centralisées, car les bases de données locales pourraient être modifiées par malveillance.

Configuration et personnalisation du logiciel Solaris Security Toolkit

Le logiciel Solaris Security Toolkit contient des valeurs par défaut pour les scripts, les fonctions de structure et les variables qui mettent en oeuvre toutes les directives de sécurité de l'ouvrage Sun BluePrints intitulé*Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*, et des articles Sun BluePrints en ligne concernant la sécurité. Ces paramètres *ne conviennent pas* à tous les systèmes ; vous devez donc personnaliser le logiciel Solaris Security Toolkit de sorte qu'il remplisse les conditions de sécurité requises de vos systèmes.

L'une des principales caractéristiques du logiciel Solaris Security Toolkit est que vous pouvez facilement le personnaliser en fonction de votre environnement, de vos systèmes et de vos besoins en sécurité. Pour personnaliser le logiciel Solaris Security Toolkit, ajustez ses actions à l'aide de pilotes, de scripts finish, de scripts audit, de fonctions de structure, de variables d'environnement et de modèles de fichiers.

La plupart des utilisateurs *n'ont pas* besoin de modifier le code de Solaris Security Toolkit. S'il s'avère absolument nécessaire de modifier le code pour utiliser le logiciel Solaris Security Toolkit dans votre environnement, copiez ce code vers un nom de fonction unique dans `user.run`, afin de pouvoir ensuite retrouver facilement les modifications (voir « Directives » à la page 15).

Vous trouverez tout au long de ce document des directives et des instructions pour la personnalisation du logiciel Security Toolkit. Pour des informations utiles sur la personnalisation des pilotes, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*. La personnalisation suppose la modification et la création de fichiers ou de variables.

Ce guide fournit des exemples de personnalisation du logiciel Solaris Security Toolkit. Ces exemples ne sont que quelques illustrations de personnalisation du logiciel Solaris Security Toolkit ; les possibilités de personnalisation sont très nombreuses.

Les sections suivantes contiennent des informations que vous devez impérativement connaître avant de tenter toute personnalisation du logiciel Solaris Security Toolkit. Ces informations se basent sur l'expérience acquise après de nombreux déploiements et vous éviteront nombre d'embûches et de pièges.

Stratégies et conditions requises

La personnalisation et le déploiement du logiciel Solaris Security Toolkit nécessitent une planification adéquate pour que le résultat soit conforme aux attentes de votre organisation et que la configuration de la plate-forme soit correcte.

En phase de planification, veillez à recueillir le maximum de données, y compris sur les stratégies et les normes de sécurité, sur les réglementations et directives du secteur, ainsi que sur les pratiques préférées des fournisseurs.

Outre ces informations, il est essentiel de prendre en compte les conditions de fonctionnement et d'application requises afin de garantir que la configuration résultante *n'a aucune* conséquence négative sur la capacité de la plate-forme à remplir les fonctions prévues.

Directives

Pour la personnalisation du logiciel Solaris Security Toolkit, respectez les directives suivantes. La compréhension et le respect de ces directives simplifiera le déploiement tout en le rendant plus efficace.

- En règle générale, ne modifiez *jamais* les fichiers originaux (pilotes, scripts, fichiers, etc.) fournis avec le logiciel Solaris Security Toolkit. La modification des fichiers originaux empêche et restreint toute mise à niveau du logiciel Solaris Security Toolkit, étant donné que les changements sont écrasés par les nouvelles versions de fichiers (tous les changements de personnalisation sont perdus et la configuration du système risque d'être incorrecte).

  Pour personnaliser un fichier, vous devez d'abord en faire une copie, puis apporter les modifications dans la copie en laissant ainsi l'original intact. Il n'existe qu'une seule exception à cette instruction :

  - les fichiers `sysidcfg`.
- Une nouvelle fonction du logiciel Solaris Security Toolkit 4.2 vous permet d'utiliser des suffixes de mots-clés pour les modèles se trouvant dans le répertoire `Files`. Ainsi, l'administrateur système *n'a besoin* de modifier *aucun* modèle par défaut du logiciel Solaris Security Toolkit 4.2. Utilisez des suffixes chaque fois que cela est possible.
- Attribuez un nom à votre copie de pilote ou de script de manière à bien la distinguer de l'original. Utilisez un préfixe ou un mot-clé qui vous permettra de reconnaître facilement le script. Par exemple, un préfixe qui contient le nom ou le symbole de l'entreprise, l'identifiant d'un service, un type d'application ou de plate-forme constitue un excellent système d'attribution de nom. Le TABLEAU 1-1 fournit plusieurs exemples de conventions d'attribution de nom.

TABLEAU 1-1 Conventions d'attribution de nom de fichier personnalisé

Fichier personnalisé	Convention d'attribution de nom
`abccorp-secure.driver`	Préfixe de l'entreprise
`abcc-nj-secure.driver`	Symbole de l'entreprise, site
`abbcorp-nj-webserver.driver`	Entreprise, site, type d'application
`abc-nj-trading-webserver.driver`	Entreprise, site, organisation, type d'application

- Vérifiez que les fichiers Solaris Security Toolkit suivants sont en adéquation avec votre système. Pour personnaliser ces fichiers, copiez les fichiers originaux, renommez les copies `user.init` et `user.run`, puis modifiez les copies.

`Drivers/user.init.SAMPLE`	Utilisé pour la personnalisation des paramètres globaux
`Drivers/user.run.SAMPLE`	Utilisé pour la personnalisation des fonctions globales

Remarque – N'oubliez pas que si vous supprimez `SUNWjass` à l'aide de la commande`pkgrm`, les fichiers `user.init` et `user.run`, s'ils ont été créés, ne sont pas supprimés. Ceci se produit également pour tous les fichiers client qui sont ajoutés à la structure de répertoires Solaris Security Toolkit et qui ne sont pas inclus dans la distribution logicielle originale.

Remarque – Le logiciel Solaris Security Toolkit 4.2 propose une nouvelle amélioration de la commande `pkgrm`. La présente version de la commande pkgrm vérifie en premier lieu l'intégrité de *tous* les fichiers inclus dans la distribution. Si certains fichiers sont différents, la commande `pkgrm` s'arrête et affiche un message d'erreur destiné à l'administrateur système pour que celui-ci place le fichier correct ou supprime le fichier modifié.

CHAPITRE 2

Sécurisation de systèmes : application d'une méthodologie

Ce chapitre décrit une méthodologie pour la sécurisation de systèmes. Vous pouvez appliquer le processus Solaris Security Toolkit avant de sécuriser des systèmes à l'aide du logiciel correspondant.

Ce chapitre contient les sections suivantes :

Planification et préparation

Une bonne planification est essentielle à la réussite de la sécurisation de systèmes à l'aide du logiciel Solaris Security Toolkit. La phase de planification construit un profil Solaris Security Toolkit pour le système, en fonction des stratégies et des normes de sécurité de l'entreprise, ainsi que des conditions de fonctionnement et d'application requises du système. Cette phase comprend les tâches suivantes :

Même s'ils ne sont pas décrits dans cet ouvrage, d'autres points peuvent être pris en compte, tels que la connaissance des risques, des expositions, de l'infrastructure et de ses besoins en matière de sécurité, la responsabilité, la journalisation et les audits d'utilisation.

Prise en compte des risques et des avantages

Pour la sécurisation de systèmes, vous devez prendre certaines précautions afin d'assurer le fonctionnement du système après la mise en oeuvre du logiciel Solaris Security Toolkit. De plus, il est important d'optimiser le processus afin de limiter les temps d'arrêt au maximum.

Remarque – Lors de la sécurisation d'un système déployé, il est parfois plus rapide et efficace de reconstruire le système, de le sécuriser au moment de la réinstallation, puis de recharger tous les logiciels nécessaires au fonctionnement.

Cette section présente certains facteurs qui doivent être pris en compte et parfaitement compris avant toute tentative de sécurisation d'un système. Évaluez soigneusement les risques et les avantages afin de déterminer les actions les plus appropriées à votre entreprise.

1. Connaissance des conditions requises pour les services et les applications du système

   Vous devez identifier les services et les applications exécutés sur un système avant d'exécuter le logiciel Solaris Security Toolkit. Toutes les dépendances associées aux services et aux applications doivent être énumérées afin que la configuration du logiciel Solaris Security Toolkit puisse être ajustée. L'absence d'énumération pourrait causer la désactivation des services nécessaires ou empêcher leur démarrage. Alors que la plupart des modifications apportées par le logiciel Solaris Security Toolkit peuvent être annulées, le développement d'un profil correct avant l'installation limite les temps morts lors de la mise en oeuvre du logiciel Solaris Security Toolkit.

2. Prise en compte du fait que le système doit être déconnecté et réinitialisé

   Pour que les modifications apportées par le logiciel Solaris Security Toolkit prennent effet, le système doit être réinitialisé. En fonction de l'importance du système, des services fournis et de la présence d'une fenêtre de maintenance, la mise en oeuvre du logiciel peut poser plus ou moins de problèmes à une entreprise. Pour prendre une décision, il faut d'abord évaluer attentivement le coût d'un temps d'arrêt par rapport aux risques encourus si la sécurité *n'est pas* améliorée.

3. Il peut être nécessaire de réinitialiser plusieurs fois un système pour vérifier son fonctionnement.

   Effectuez toutes les modifications sur des systèmes hors production avant de mettre en oeuvre une configuration vitale des systèmes, à chaque fois que cela est possible. Ceci n'est pas toujours le cas, par exemple en l'absence de matériel ou de logiciel suffisant pour répliquer l'environnement cible. Des tests doivent être accomplis *avant* et *après* l'exécution du logiciel Solaris Security Toolkit lors de la sécurisation. Des dépendances non identifiées nécessitant un dépannage après la sécurisation du système pourraient être présentes. Dans la plupart des cas, ces problèmes peuvent

être résolus assez rapidement en utilisant les techniques décrites dans ce chapitre. Si des problèmes de fonctionnalité sont détectés après l'exécution du logiciel Solaris Security Toolkit, il peut s'avérer nécessaire de réinitialiser plusieurs fois la plate-forme, soit pour annuler les effets du logiciel Solaris Security Toolkit, soit pour ajouter d'autres modifications à la configuration de sécurité du système afin de prendre en charge et d'activer les fonctionnalités manquantes.

4. La sécurisation d'une plate-forme ne se limite pas à la configuration de la sécurité et à l'audit du système.

   Si vous envisagez de mettre à niveau la configuration d'un système pour améliorer sa sécurité, il est essentiel de comprendre que la sécurisation et l'audit d'une plate-forme ne représentent qu'une fraction des tâches nécessaires à la protection du système, des services et des données. Ce document ne traite pas des mesures et contrôles supplémentaires. Il est toutefois conseillé de prendre en considération les problèmes liés à la gestion des comptes, à la gestion des privilèges, à l'intégrité des systèmes de fichiers et des données, aux contrôles d'accès basés sur les hôtes, à la détection des intrusions, au balayage et à l'analyse de la vulnérabilité, ainsi qu'à la sécurité des applications.

5. Le système pourrait avoir déjà été exploité ou présenter des vulnérabilités exploitables.

   La plate-forme en cours de sécurisation pourrait déjà avoir fait l'objet d'une attaque. Le logiciel Solaris Security Toolkit a probablement été mise en oeuvre trop tard pour assurer une protection contre les vulnérabilités exploitée. En cas de vulnérabilité exploitée :

   a. Réinstallez le système ;

   b. Installez le logiciel Solaris Security Toolkit ;

   c. Utilisez le logiciel Solaris Security Toolkit pour améliorer la sécurité.

Vérification des stratégies et des normes de sécurité, ainsi que de la documentation correspondante

La première étape de sécurisation d'un système consiste à connaître les stratégies et les normes de sécurité pertinentes de l'organisation, ainsi que les directives en matière de sécurité de plate-forme. Utilisez ces documents comme base du profil de Solaris Security Toolkit, car ils décrivent les conditions requises et les mesures à appliquer à tous les systèmes de l'organisation. Si l'organisation *ne dispose pas* de documentation, créez-en une pour augmenter votre capacité à personnaliser le logiciel Solaris Secure Toolkit.

Remarque – Lorsque vous recherchez de telles informations, n'oubliez pas que vous pouvez trouver du matériel dans les meilleures pratiques ou d'autres documentations.

Pour de plus amples informations sur les stratégies de sécurité, reportez-vous à l'article Sun BluePrints en ligne « Developing a Security Policy ». Ce document peut être utilisé pour mieux comprendre le rôle des stratégies de sécurité dans le plan de sécurité d'une entreprise.

Les deux exemples qui suivent illustrent les conséquences directes des stratégies de sécurité sur la configuration du profil de Solaris Security Toolkit.

Exemple 1

- **Stratégie** – Une organisation doit utiliser des protocoles de gestion qui prennent en charge une puissante authentification des utilisateurs et le chiffrement des données transmises.
- **Conséquences sur le profil** – Les protocoles utilisant un texte en clair, tels que elnet, File Transfer Protocol (FTP), Simple Network Management Protocol version 1 (SNMPv1), etc., *ne doivent pas* être utilisés. Le fichier `secure.driver` du logiciel Solaris Security Toolkit désactive ces services de sorte qu'aucune configuration supplémentaire n'est requise.

Remarque – Les services Telnet et FTP peuvent être configurés de manière à prendre en charge une authentification et un chiffrement plus puissants en utilisant des extensions telles que Kerberos. Toutefois, leurs configurations par défaut *ne prennent pas* en charge les niveaux de sécurité ajoutés.

Exemple 2

Stratégie – Tous les utilisateurs doivent obligatoirement changer leurs mots de passe tous les 30 jours.

Conséquences sur le profil – Le logiciel Solaris Security Toolkit peut être configuré pour permettre l'expiration du mot de passe. Le fichier `secure.driver` du logiciel Solaris Security Toolkit définit les mots de passe pour une période maximale de 8 semaines (56 jours). Pour vous conformer à la stratégie, vous devez changer le profil du logiciel Solaris Security Toolkit. Voir *Solaris Security Toolkit 4.2 Reference Manual*.

Même si secure.driver du logiciel Solaris Security Toolkit permet l'expiration des mots de passe lorsqu'il est exécuté sur un système, cette modification *n'affecte pas* les utilisateurs existants jusqu'à ce qu'ils changent leur mot de passe. Pour activer l'expiration des mots de passe des utilisateurs existants, appelez la commande `passwd`(1) sur chaque compte utilisateur. Pour forcer les utilisateurs existants à modifier leur mot de passe, utilisez la commande `passwd -f`. Pour de plus amples informations sur la commande `passwd`(1), reportez-vous à la collection de manuels de référence du SE Solaris 10.

Détermination des conditions requises pour les applications et les services

Cette tâche permet de garantir que les services restent fonctionnels après la sécurisation du système. Elle comprend les étapes suivantes :

Inventaire des applications et des services opérationnels

Inventaire des applications, services et fonctions opérationnelles ou de gestion. Cet inventaire est nécessaire pour déterminer le logiciel en cours d'utilisation sur un système. Les systèmes sont souvent dotés de logiciels non utilisés et de logiciels qui ne prennent pas en charge les fonctions de l'entreprise.

Les systèmes doivent, autant que possible, être réduits au maximum. Ainsi, les logiciels non utilisés pour la prise en charge d'une fonction *ne doivent pas* être installés. Les applications inutiles augmentent les failles du système et ses vulnérabilités exploitables. Par ailleurs, en règle générale, plus le nombre de logiciels sur un système est important, plus le nombre de patchs à appliquer augmente. Pour de plus amples informations sur la minimisation du SE Solaris, reportez-vous à l'article Sun BluePrints en ligne « Minimizing the Solaris Operating Environment for Security ». Pour de plus amples informations sur la minimisation des domaines de systèmes Sun Fire, reportez-vous aux articles Sun BluePrints en ligne « Part I: Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems, » et « Part II: Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems ».

Lors de l'inventaire des logiciels, veillez à inclure les composants d'infrastructure, tels que les logiciels de gestion, de contrôle et de sauvegarde, en plus des applications résidant sur le système.

Détermination des conditions requises pour les services

Après avoir terminé l'inventaire des applications et des services, déterminez si certains composants présentent des dépendances qui pourraient avoir une incidence sur la sécurisation. De nombreuses applications tierces *n'utilisent pas* directement les services fournis par le SE Solaris. Vous trouverez, dans les sections qui suivent, des informations utiles sur ces applications.

Remarque – Tous les exemples de cette section utilisent le SE Solaris 9.

Bibliothèques partagées

Il est important de connaître les bibliothèques nécessaires à la prise en charge d'une application. Ceci est particulièrement utile en cas de débogage, mais également lors de la préparation d'un système avant sa sécurisation. Si vous ne connaissez pas l'état d'un système, recueillez autant d'informations que possible de manière à bien comprendre certains problèmes, tels que les dépendances logicielles.

Pour déterminer les bibliothèques utilisées par une application, vous avez le choix entre trois méthodes, selon la version du SE installée : Cette section fournit un exemple de code pour chaque méthode.

- **Méthode 1** - Informations sur les objets de système de fichiers, par exemple binaires d'application ou bibliothèques (EXEMPLE DE CODE 2-1).
- **Méthode 2** - Informations sur un processus exécuté afin d'analyser une application en cours d'exécution (EXEMPLE DE CODE 2-2).
- **Méthode 3** - Identification des applications chargées de manière dynamique pour retracer l'heure de démarrage d'un programme (EXEMPLE DE CODE 2-3).

Méthode 1

Pour la collecte d'informations sur un objet de système de fichiers, utilisez la commande `/usr/bin/ldd`.

Par exemple, déterminez les bibliothèques nécessaires à la prise en charge du logiciel de serveur Domain Name System (DNS).

EXEMPLE DE CODE 2-1 Collecte d'informations sur les objets de système de fichiers

```
# ldd /usr/sbin/in.named
libresolv.so.2 => /usr/lib/libresolv.so.2
libsocket.so.1 => /usr/lib/libsocket.so.1
libnsl.so.1 =>    /usr/lib/libnsl.so.1
libc.so.1 =>      /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1
```

Méthode 2

Pour la collecte d'informations à partir d'un processus en cours, utilisez la commande `/usr/proc/bin/pldd` (disponible sur les SE Solaris 8, 9 et 10).

EXEMPLE DE CODE 2-2 Collecte d'informations à partir d'un processus en cours

```
# pldd 20307
20307:  /usr/sbin/in.named
/usr/lib/libresolv.so.2
/usr/lib/libsocket.so.1
/usr/lib/libnsl.so.1
/usr/lib/libc.so.1
/usr/lib/libdl.so.1
/usr/lib/libmp.so.2
/usr/platform/sun4u/lib/libc_psr.so.1
/usr/lib/dns/dnssafe.so.1
/usr/lib/dns/cylink.so.1
```

Méthode 3

La commande `pldd` indique les bibliothèques partagées qui sont chargées de manière dynamique par l'application, en plus des bibliothèques par rapport auxquelles l'application est liée. Ces informations peuvent également être obtenues à l'aide de la commande`truss` suivante.

Remarque – La sortie suivante a été raccourcie.

EXEMPLE DE CODE 2-3 Identification d'applications chargées de manière dynamique

```
# truss -f -topen,open64 /usr/sbin/in.named
20357:  open("/usr/lib/libresolv.so.2", O_RDONLY)       = 3
20357:  open("/usr/lib/libsocket.so.1", O_RDONLY)       = 3
20357:  open("/usr/lib/libnsl.so.1", O_RDONLY)          = 3
20357:  open("/usr/lib/libc.so.1", O_RDONLY)            = 3
20357:  open("/usr/lib/libdl.so.1", O_RDONLY)           = 3
20357:  open("/usr/lib/libmp.so.2", O_RDONLY)           = 3
```

EXEMPLE DE CODE 2-3 Identification d'applications chargées de manière dynamique

```
# truss -f -topen,open64 /usr/sbin/in.named
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)       = 4
20357:  open("/usr/lib/nss_files.so.1", O_RDONLY)       = 4
20357:  open("/usr/lib/dns/dnssafe.so.1", O_RDONLY)     = 4
20357:  open("/usr/lib/dns/cylink.so.1", O_RDONLY)      = 4
20357:  open("/usr/lib/dns/sparcv9/cylink.so.1", O_RDONLY) = 4
```

Ce type de sortie contient l'identificateur de processus, l'appel système (dans ce cas `open`) et ses arguments, ainsi que la valeur renvoyée par l'appel système. La valeur renvoyée indique clairement si l'appel système réussit à rechercher et à ouvrir la librairie partagée.

Après avoir pris connaissance de la liste des bibliothèques partagées, utilisez la commande suivante pour déterminer les packages du SE Solaris auxquels elles appartiennent.

```
# grep "/usr/lib/dns/cylink.so.1" /var/sadm/install/contents
/usr/lib/dns/cylink.so.1 f none 0755 root bin 63532 24346 \
  1018126408 SUNWcsl
```

La sortie de la commande indique que la bibliothèque partagée en question appartient au package `SUNWcsl` (Core, Shared Libs). Cette procédure est particulièrement utile lors de la minimisation d'une plate-forme, car elle permet d'identifier les packages requis pour la prise en charge d'une application ou d'un service.

Fichiers de configuration

Les fichiers de configuration peuvent également être utilisés pour la collecte d'informations. Cette méthode a des conséquences plus directes sur la manière dont un système est sécurisé, du fait que les fichiers de configuration peuvent être renommés ou supprimés pour désactiver des services. Pour de plus amples informations, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Pour déterminer si un fichier de configuration est en cours d'utilisation, utilisez la commande `truss`.

Remarque – La sortie suivante a été raccourcie.

EXEMPLE DE CODE 2-4 Détermination d'un fichier de configuration en cours d'utilisation

```
# truss -f -topen,open64 /usr/sbin/in.named 2>&1 | \
grep -v "/usr/lib/.*.so.*"
20384:  open("/etc/resolv.conf", O_RDONLY)              = 3
20384:  open("/dev/conslog", O_WRONLY)                  = 3
20384:  open("/usr/share/lib/zoneinfo/US/Eastern", O_RDONLY) = 4
20384:  open("/var/run/syslog_door", O_RDONLY)          = 4
20384:  open("/etc/nsswitch.conf", O_RDONLY)            = 4
20384:  open("/etc/services", O_RDONLY)                 = 4
20384:  open("/etc/protocols", O_RDONLY)                = 4
20384:  open("/etc/named.conf", O_RDONLY)               = 4
20384:  open("named.ca", O_RDONLY)                      = 5
20384:  open("named.local", O_RDONLY)                   = 5
20384:  open("db.192.168.1", O_RDONLY)                  = 5
20384:  open("db.internal.net", O_RDONLY)               = 5
```

Dans cet exemple, le service DNS utilise des fichiers de configuration, tels que`/etc/named.conf`. Comme dans l'exemple précédent, si la valeur renvoyée pour un service indique une erreur, il est probable qu'il existe un problème. Une documentation soigneuse des résultats avant et après la sécurisation peut contribuer à accélérer l'ensemble du processus de validation.

Structures des services

Cette catégorie comprend des structures ou des métaservices sur lesquels sont construites des applications plus volumineuses et plus complexes. Les types de structures dans cette catégorie sont en général les suivants :

- Services d'attribution de nom, par exemple Network Information Services (NIS), NIS+ et Lightweight Directory Access Protocol (LDAP)
- Services d'authentification, par exemple Kerberos et LDAP
- Services d'utilitaires, tels que le journal de correspondance des points de connexion utilisé par Remote Procedure Call (RPC)

Il n'est pas toujours évident de déterminer si une application dépend de ces types de services. Lorsque des ajustements particuliers sont nécessaires pour configurer une application, par exemple lorsqu'il faut ajouter celle-ci à un domaine Kerberos, la dépendance est connue. Dans certains cas, toutefois, les dépendances des applications ne nécessitent aucune tâche supplémentaire ; la dépendance risque donc de *ne pas être* documentée par le fournisseur.

Le journal de correspondance des points de connexion RPC en est un exemple type. `secure.driver` du logiciel Solaris Security Toolkit désactive le journal de correspondance des points de connexion RPC. Cette opération peut donner lieu à des comportements inattendus dans d'autres services reposant sur ce service. L'expérience montre que les services abandonnent leurs opérations, s'interrompent ou échouent lorsque le code de l'application ne présente pas une qualité suffisante pour gérer les exceptions. Pour déterminer si une application utilise le journal de correspondance des points de connexion RPC, utilisez la commande `rpcinfo`. Par exemple :

EXEMPLE DE CODE 2-5 Détermination des applications utilisant RPC

```
# rpcinfo -p
100000    3   tcp    111  rpcbind
100000    4   udp    111  rpcbind
100000    2   udp    111  rpcbind
100024    1   udp  32777  status
100024    1   tcp  32772  status
100133    1   udp  32777
100133    1   tcp  32772
100021    1   udp   4045  nlockmgr
100021    2   udp   4045  nlockmgr
100021    3   udp   4045  nlockmgr
100021    4   udp   4045  nlockmgr
100021    1   tcp   4045  nlockmgr
```

Les informations figurant dans la colonne du service proviennent du fichier `/etc/rpc` ou d'un service d'attribution de noms configuré, tel que LDAP.

Si ce fichier ne possède pas d'entrée pour un service, comme c'est souvent le cas pour les produits tiers, le champ du service peut être vide. L'identification des applications enregistrées par d'autres applications devient donc encore plus difficile.

Prenez par exemple la commande `rusers`. Cette commande repose sur le service de journal de correspondance des points de connexion RPC. Si le journal de correspondance des points de connexion RPC *n'est pas* en cours d'exécution, la commande `rusers` semble s'interrompre. Après un délai d'attente, le programme renvoie le message d'erreur suivant :

```
# rusers -a localhost
localhost: RPC: Rpcbind failure
```

Ce problème survient parce que le programme est dans l'impossibilité de communiquer avec le service. Toutefois, après le démarrage du service de journal de correspondance des points de connexion RPC à partir de `/etc/init.d/rpc`, le programme renvoie immédiatement son résultat.

Dans un autre exemple, le service de journal de correspondance des points de connexion RPC est en cours d'exécution alors que le service `rusers` n'est pas configuré pour fonctionner. Dans ce cas, la réponse générée est complètement différente et relativement facile à valider.

EXEMPLE DE CODE 2-6 Validation du service `rusers`

```
# rusers -a localhost
localhost: RPC: Program not registered
# grep rusers /etc/rpc
rusersd         100002  rusers
# rpcinfo -p | grep rusers
<No output generated>
```

Étant donné que la commande `rpcinfo` ne possède pas de registre pour le service `rusers`, il est sage de supposer que le service *n'est pas* configuré pour être exécuté. Vous pouvez valider cette hypothèse en analysant l'entrée du service dans le fichier `/etc/inet/inetd.conf`.

```
# grep rusers /etc/inet/inetd.conf
# rusersd/2-3   tli     rpc/datagram_v,circuit_v     wait root
/usr/lib/netsvc/rusers/rpc.rusersd     rpc.rusersd
```

La marque de commentaire (`#`) au début de la ligne du service indique que le service `rusers` est désactivé. Pour activer le service, éliminez le commentaire de la ligne et envoyez un signal `SIGHUP` au processus `/usr/sbin/inetd`, comme suit.

```
# pkill -HUP inetd
```

Remarque – La commande `pkill` est disponible *uniquement* sous les SE Solaris 7 à 10. Pour les autres versions, utilisez les commandes `ps` et `kill` pour respectivement rechercher et signaler le processus.

Pour déterminer si une application utilise RPC, il est également possible de faire appel à la commande `ldd` décrite ci-avant.

EXEMPLE DE CODE 2-7 Méthode alternative pour la détermination des applications qui utilisent RPC

```
# ldd /usr/lib/netsvc/rusers/rpc.rusersd
libnsl.so.1 =>   /usr/lib/libnsl.so.1
librpcsvc.so.1 =>        /usr/lib/librpcsvc.so.1
libc.so.1 =>     /usr/lib/libc.so.1
libdl.so.1 =>    /usr/lib/libdl.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-250/lib/libc_psr.so.1
```

L'entrée pour `librpcsvc.so.1` indique, outre le nom du fichier, que ce service repose sur le journal de correspondance des points de connexion RPC.

Outre le journal de correspondance des points de connexion RPC, les applications peuvent également reposer sur d'autres services de SE courants, tels que FTP, SNMP ou Network File System (NFS). Vous pouvez utiliser des techniques similaires pour déboguer ces services et déterminer s'ils sont effectivement nécessaires pour la prise en charge d'une fonction de l'entreprise. L'une des méthodes consiste à utiliser la commande `netstat` comme suit.

```
# netstat -a | egrep "ESTABLISHED|TIME_WAIT"
```

Cette commande renvoie une liste de services qui sont en cours d'utilisation ou ont récemment été utilisés, par exemple :

TABLEAU 2-1 Liste des services récemment utilisés

```
localhost.32827      localhost.32828      49152      0 49152      0
ESTABLISHED
localhost.35044      localhost.32784      49152      0 49152      0
ESTABLISHED
localhost.32784      localhost.35044      49152      0 49152      0
ESTABLISHED
```

TABLEAU 2-1 Liste des services récemment utilisés *(suite)*

```
localhost.35047      localhost.35046      49152      0 49152      0
ESTABLISHED

localhost.35046      localhost.35047      49152      0 49152      0
ESTABLISHED

filefly.ssh 192.168.0.3.2969    17615     1 50320     0 ESTABLISHED
```

Dans cet exemple, de nombreux services sont utilisés, mais il n'est pas évident de déterminer les ports qui appartiennent aux services ou aux applications. Pour obtenir ces informations, analysez les processus à l'aide de la commande `pfiles` (1) (disponible sous les SE Solaris 8, 9 et 10). La commande `pfiles` renvoie des informations pour tous les fichiers ouverts de chaque processus.

EXEMPLE DE CODE 2-8 Détermination des ports qui appartiennent aux services ou aux applications

```
# for pid in `ps -aeo pid | grep -v PID`; do
> pfiles ${pid} | egrep "^${pid}:|sockname:"
> done
```

Ces dépendances peuvent être déterminées plus efficacement à l'aide de la commande `lsof` (pour obtenir la liste des fichiers ouverts).

Téléchargez le code source `lsof` à l'adresse suivante :

ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/

Téléchargez les binaires `lsof` à l'adresse suivante :

http://www.sunfreeware.com

La commande `lsof` permet de déterminer les fichiers et les ports utilisés par les processus. Par exemple, pour déterminer les processus qui utilisent le port 35047 dans l'exemple précédent, lancez la commande suivante.

EXEMPLE DE CODE 2-9 Détermination des processus qui utilisent des fichiers et des ports

```
# ./lsof -i | grep 35047
ttsession   600 root 9u  IPv4 0x3000b4d47e8     0t1  TCP
localhost:35047->localhost:35046 (ESTABLISHED)
dtexec     5614 root 9u  IPv4 0x3000b4d59e8     0t0  TCP
localhost:35046->localhost:35047 (ESTABLISHED)
```

La sortie de la commande `lsof` indique que le port `35047` est utilisé pour la communication entre les processus `dtexec` et `ttsession`.

L'utilisation du programme `lsof` peut vous permettre de déterminer plus rapidement les dépendances entre systèmes ou entre applications nécessitant l'emploi d'un système de fichiers ou d'un réseau. Presque tout ce qui est signalé dans cette section peut être capturé à l'aide d'options du programme `lsof`.

Remarque – Il peut arriver que les méthodes décrites pour la détermination des dépendances *ne trouvent pas* les éléments qui sont rarement utilisés. Utilisez ces méthodes, mais consultez également la documentation Sun et celle du fournisseur.

Développement et mise en oeuvre d'un profil Solaris Security Toolkit

Une fois la phase de planification et de préparation terminée, développez et mettez en oeuvre un profil de sécurité. Un profil de sécurité consiste en une configuration, des pilotes de sécurisation, par exemple, *nom*`-{config|hardening|secure}.driver`, des scripts et des fichiers nécessaires à la mise en oeuvre des stratégies de sécurité spécifiques à votre entreprise.

Personnalisez l'un des profils de sécurité fournis avec le logiciel Solaris Security Toolkit ou développez-en un nouveau. Les stratégies et les normes de sécurité, ainsi que les conditions requises pour les applications, diffèrent, même légèrement, d'une entreprise à une autre.

Pour personnaliser le un profil de sécurité, ajustez ses actions à l'aide de scripts finish, de scripts audit, de variables d'environnement, de fonctions de structure et de modèles de fichiers.

Pour de plus amples informations, reportez-vous aux chapitres suivants :

- Pour obtenir des directives importantes sur la personnalisation du logiciel, reportez-vous au chapitre 1, « Configuration et personnalisation du logiciel Solaris Security Toolkit » à la page 13.
- Pour un exemple de création d'un profil de sécurité, reportez-vous au chapitre 7, « Création d'un profil de sécurité » à la page 110.
- Pour de plus amples informations sur la personnalisation des pilotes, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

  Si nécessaire, reportez-vous aux autres chapitres du manuel *Solaris Security Toolkit 4.2 Reference Manual* pour de plus amples informations sur les scripts, les fonctions de structure, les variables d'environnement et les fichiers. Il existe deux variables d'environnement qu'il est préférable de personnaliser : `JASS_FILES` et `JASS_SCRIPTS`.

Pour mettre en oeuvre des normes sur une majorité de plates-formes, tout en préservant les différences spécifiques à chacune, utilisez une technique connue sous le nom de profils de sécurité imbriqués ou hiérarchiques. Pour de plus amples informations, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*. Comparez le profil de sécurité résultant et les stratégies, normes et conditions requises de votre organisation pour garantir que des modifications ne sont pas apportées par inadvertance ou par erreur.

Installation du logiciel

La procédure d'installation du logiciel Solaris Security Toolkit est la même, que le système soit déployé ou nouveau. Pour des instructions détaillées, reportez-vous au chapitre 3.

Pour les systèmes déployés, certains cas particuliers peuvent rendre l'installation plus simple et plus rapide. Ces cas *ne sont pas* centrés sur le processus de sécurisation, mais sur les tâches qui précèdent et suivent l'installation.

Tâches précédant l'installation

Avant de sécuriser un système déployé, analysez et planifiez deux tâches significatives :

- Sauvegarde
- Vérification

Ces tâches facilitent la détermination de l'état du système déployé et la résolution des problèmes de configuration pouvant se poser avant la sécurisation du système.

Sauvegarde des données

Cette tâche se concentre sur la planification de secours. En cas de problème, il est indispensable que la configuration et les données du système soient archivées sous une forme ou une autre. Vous *devez* effectuer les opérations suivantes :

- Sauvegarder le système.
- Veiller à ce que les médias de sauvegarde puissent être lus.
- Vérifier que le contenu peut être restauré.

Vous devez réaliser ces opérations avant toute modification significative de la configuration d'un système.

Vérification de la stabilité du système

La vérification est une tâche presque aussi importante que la sauvegarde. La vérification permet d'assurer la stabilité et le fonctionnement du système avant la mise en oeuvre des modifications de configuration, telles que celles introduites par le processus de sécurisation. Le processus de vérification inclut les étapes suivantes :

- Redémarrage
- Test réussi de tous les services ou applications

Bien qu'il soit préférable de disposer d'un programme de test et d'acceptation bien défini, de tels plans ne sont pas toujours disponibles. Dans ce cas, testez logiquement le système en fonction de son utilisation. Cette tâche a pour objectif d'assurer que la configuration utilisée correspond bien à la configuration enregistrée.

Analysez tous les messages d'erreur ou d'avertissement qui s'affichent à l'initialisation du système ou au démarrage d'une application. Si vous *ne parvenez pas* à corriger les erreurs, consignez-les de manière à éviter qu'elle ne soient considérées comme des problèmes potentiels au cours du processus de sécurisation. Lorsque vous examinez les fichiers journaux, n'oubliez pas d'inclure les journaux du système, des services et des applications tels que :

- `/var/adm/messages`
- `/var/adm/sulog`
- `/var/log/syslog`
- `/var/cron/log`

Cette tâche est terminée quand vous redémarrez le système sans rencontrer de messages d'erreur ou d'avertissement, ni d'erreurs ou d'avertissements *inconnus* (tous avertissements ou erreurs *connus* sont documentées). Le système doit redémarrer dans un état connu et stable. Si vous découvrez, au cours d'une vérification, que les configurations exécutées et stockées du système ne sont pas les mêmes, réévaluez les stratégies et processus de contrôle des changements de l'organisation pour identifier le problème à l'origine de cette situation.

Tâches suivant l'installation

Les tâches suivant l'installation sont un prolongement des tâches précédant l'installation. Leur objectif est d'assurer que le processus de sécurisation *n'a pas* causé de nouvelles défaillances dans le système ou les applications. Cette tâche consiste avant tout à examiner les fichiers journaux du système et des applications. Les fichiers journaux créés après la sécurisation et la réinitialisation doivent être similaires à ceux qui avaient été collectés avant la sécurisation du système. Ils peuvent parfois contenir moins de messages parce que les services démarrés sont moins nombreux. Mais il est fondamental qu'il ne contiennent pas de nouveaux messages d'erreur ou d'avertissement.

Après avoir examiné les fichiers journaux, testez les fonctionnalités, car certaines applications pourraient rencontrer des problèmes sans consigner de messages dans le fichier journal. Pour de plus amples informations sur la vérification, reportez-vous à la section suivante.

Vérification des fonctionnalités des applications et des services

La dernière tâche de ce processus consiste à vérifier que les applications et services offerts par le système fonctionnent tous correctement. Cette tâche vérifie également que le profil de sécurité a été correctement mis en oeuvre en conformité avec les stratégies de l'entreprise en matière de sécurité. Effectuez cette tâche de manière exhaustive et immédiatement après le redémarrage de la plate-forme sécurisée, afin d'assurer la détection des anomalies ou problèmes éventuels et leur correction immédiate. Cette procédure comporte deux tâches : vérification de l'installation du profil de sécurité et vérification des fonctionnalités des applications et des services.

Vérification de l'installation du profil de sécurité

Pour vérifier que le logiciel Solaris Security Toolkit a installé correctement le profil de sécurité sans erreurs, examinez le fichier journal de l'installation `jass-install-log.txt`. Ce fichier se trouve dans le sous-répertoire `/var/opt/SUWWjass/runs`, au sein du répertoire unique à chaque sécurisation ou audit (heure/date de démarrage de l'exécution).

Remarque – Examinez ce fichier journal pour connaître les opérations effectuées par le logiciel Solaris Security Toolkit sur le système. Pour chaque exécution sur le système, un nouveau fichier journal est enregistré dans le répertoire en fonction de l'heure/la date de démarrage de l'exécution.

Après avoir vérifié que le profil a été installé, évaluez la configuration de sécurité du système. Effectuez un examen manuel ou utilisez un outil d'automatisation du processus.

Vérification des fonctionnalités des applications et des services

Pour vérifier les applications et les services de processus, lancez un plan de test et d'acceptation bien défini, afin de tester les différents composants d'un système ou d'une application, et de déterminer s'ils sont disponibles et s'ils fonctionnent correctement. En l'*absence* d'un tel plan, testez le système avec logique en fonction de son utilisation. L'objectif est de s'assurer que la sécurisation n'a pas altéré le fonctionnement des applications ou services.

Si vous découvrez qu'une application ou un service ne fonctionne pas correctement après la sécurisation du système, recherchez la cause du problème en examinant les fichiers journaux correspondants. Le plus souvent, vous pouvez utiliser la commande `truss` pour localiser le problème. Un fois le problème localisé, vous pouvez le cibler et remonter à la modification apportée par le logiciel Solaris Security Toolkit.

Maintenance de la sécurité du système

De nombreuses organisations commettent la même erreur qui consiste à prendre la sécurité en compte au moment de l'installation uniquement, puis de n'y revenir que rarement, voire jamais. La maintenance de la sécurité est un processus permanent. La sécurité d'un système doit être vérifiée périodiquement.

La maintenance d'un système sécurisé requiert une grande attention étant donné que la configuration de sécurité de tout système tend à s'ouvrir de plus en plus avec le temps. Par exemple, les failles du systèmes deviennent connues.

Les directives de base suivantes indiquent les tâches de maintenance de la sécurité d'un système :

- Vérifiez le niveau de sécurité du système avant et après l'installation de patchs. Il est également important de mettre à jour régulièrement le système à l'aide des patchs les plus récents.

  Les patchs du SE Solaris risquent d'installer des packages supplémentaires et écraser des fichiers de configuration du système. Le logiciel Solaris Security Toolkit peut vous assister lors de l'application de patchs, parce qu'il prend en charge les exécutions répétées sur un système, afin que vous sécurisiez le système après l'installation de patchs. Exécutez le logiciel après l'installation de chaque patch, en utilisant les pilotes appropriés, pour vous assurer que la configuration demeure conforme aux stratégies de sécurité. Effectuez également un examen manuel du système, car la version de Solaris Security Toolkit utilisée pourrait *ne pas* prendre en charge les nouvelles fonctions ajoutées par les patchs installés.

- Contrôlez le système à intervalles réguliers pour éviter l'apparition de comportements non autorisés. Vérifiez les comptes du système, les mots de passe et les types d'accès ; ils peuvent vous apporter de précieuses informations sur le fonctionnement d'un système.
- Déployez et maintenez un référentiel centralisé `syslog` pour la collecte et l'analyse des messages `syslog`. Vous pouvez obtenir de précieuses informations en rassemblant et en examinant ces journaux.
- Mettez en place une stratégie exhaustive d'audit et de lutte contre la vulnérabilité pour le contrôle et la maintenance des configurations du système. Cette stratégie joue un rôle fondamental dans la maintenance de configurations système sécurisées.
- Mettez périodiquement les systèmes à jour en installant la dernière version du logiciel Solaris Security Toolkit.

Le logiciel Solaris Security Toolkit inclut des profils de sécurité par défaut que vous pouvez utiliser comme point de départ.

CHAPITRE 3

Mise à niveau, installation et exécution du logiciel de sécurité

Ce chapitre décrit le téléchargement, la mise à niveau, l'installation et l'exécution du logiciel Solaris Security Toolkit et d'autres logiciels de sécurité. Il fournit également des instructions de configuration de l'environnement en mode autonome ou JumpStart, et indique comment bénéficier d'un support technique.

Suivez les instructions et les processus contenus dans cette section pour mettre à niveau ou installer, configurer et exécuter le logiciel. Ces instructions comprennent le téléchargement de logiciels supplémentaires, des exemples utiles et des directives.

Bien que le logiciel Solaris Security Toolkit soit un produit autonome, il est plus efficace lorsqu'il est utilisé avec les logiciels supplémentaires proposés en téléchargement. Ces logiciels comprennent le dernier cluster de patchs recommandés et de sécurité de SunSolve OnLine, le logiciel Secure Shell pour les versions du SE Solaris qui *ne l'incorporent pas*, le logiciel de modification des autorisations et des propriétés pour renforcer les autorisations du SE Solaris et de logiciels tiers, et des binaires de validation d'intégrité des fichiers et exécutables Sun.

Ce chapitre contient les tâches suivantes :

Tâches de planification et de préinstallation

Une planification adéquate est essentielle à la réussite de la sécurisation de systèmes à l'aide du logiciel Solaris Security Toolkit. Pour de plus amples informations sur la planification préalable à l'installation du logiciel, reportez-vous au chapitre 2.

Si vous installez le logiciel sur un système déployé, reportez-vous à la section « Tâches précédant l'installation » à la page 31 qui contient une description des tâches à effectuer avant l'installation sur les systèmes déployés.

Dépendances logicielles

Le logiciel Solaris Security Toolkit 4.2 dépend du package `SUNWloc`. Si ce package est absent, Solaris Security Toolkit échoue.

Pour de plus amples informations sur les versions du SE Solaris prises en charge, reportez-vous à la section « Versions du SE Solaris prises en charge » à la page xxi.

Pour de plus amples informations sur les versions de SMS (System Management Services) prises en charge, reportez-vous à la section « Versions de System Management Services (SMS) prises en charge » à la page xxii.

Détermination du mode à utiliser

Sécurisez les systèmes pendant ou immédiatement après l'installation du SE, afin de limiter leur durée d'exposition aux attaques sans sécurisation. Avant d'utiliser le logiciel Solaris Security Toolkit pour sécuriser un système, configurez-le de manière à ce qu'il fonctionne correctement dans votre environnement.

Le logiciel Solaris Security Toolkit a une structure modulaire. Si vous *n'utilisez pas* le produit JumpStart, la flexibilité de la structure du logiciel Solaris Security Toolkit vous permet de vous préparer efficacement à une utilisation ultérieure de JumpStart. Si vous employez JumpStart, vous bénéficiez de la capacité du logiciel Solaris Security Toolkit à s'intégrer dans les architectures JumpStart existantes.

Les sections suivantes décrivent les modes autonome et JumpStart.

Mode autonome

Le logiciel Solaris Security Toolkit est lancé directement à partir d'une invite de shell du SE Solaris en mode autonome. Ce mode vous permet d'utiliser le logiciel Solaris Security Toolkit sur les systèmes nécessitant des modifications ou mises à jour de sécurité, mais *ne peut pas* servir à la réinstallation complète du système d'exploitation. Toutefois, chaque fois que cela est possible, les systèmes d'exploitation doivent être entièrement réinstallés avant leur sécurisation.

Le mode autonome est particulièrement utile pour la sécurisation de systèmes après l'installation de patchs ou de logiciels tiers. Vous pouvez exécuter plusieurs fois le logiciel Solaris Security Toolkit sur un système sans aucun risque. Les patchs risquent d'écraser ou de changer des fichiers qui avaient été modifiés par le logiciel Solaris Security Toolkit ; en réexécutant ce dernier, vous pouvez de nouveau mettre en oeuvre les modifications de sécurité qui ont été refusées lors de l'installation du patch.

Remarque – Dans les environnements de production, activez les patchs dans les environnement de test et de développement avant de les installer dans les environnement réels.

Le mode autonome constitue l'une des options les plus efficaces et les plus rapides pour la sécurisation d'un système déployé. Aucune opération particulière n'est requise pour intégrer le logiciel Solaris Security Toolkit dans une architecture sans JumpStart, excepté les opérations décrites à la section « Téléchargement du logiciel de sécurité » à la page 42 relatives au téléchargement et à l'installation.

Mode JumpStart

La technologie JumpStart, qui est un mécanisme Sun d'installation du SE Solaris à partir d'un réseau, prend en charge l'exécution des scripts Solaris Security Toolkit au cours de l'installation. Cet ouvrage suppose que le lecteur est familiarisé avec la technologie JumpStart et qu'il a un environnement JumpStart à disposition. Pour de plus amples informations sur la technologie JumpStart, reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Le package Solaris Security Toolkit 4.2 est réadressable, il peut donc être installé dans n'importe quel répertoire à condition que les options correctes de le la commande `pkgadd` soient utilisées. `JASS_HOME_DIR` devient le répertoire de base du serveur JumpStart.

Seules quelques opérations suffisent à l'intégration du logiciel Solaris Security Toolkit dans une architecture JumpStart. Reportez-vous au chapitre 5 pour obtenir des instructions sur la configuration d'un serveur JumpStart.

Mise à niveau des procédures

Cette section contient des informations sur la mise à niveau de Solaris Security Toolkit 4.0 et 4.1 vers Solaris Security Toolkit 4.2, avec et sans mise à niveau du SE Solaris. Le système est sécurisé à l'aide du logiciel Solaris Security Toolkit sous le SE Solaris. Les procédures sont les mêmes, que la mise à niveau s'effectue à partir de la version 4.0 ou de la version 4.1. Pour éviter d'écraser toute personnalisation antérieure, il est très important d'exécuter les procédures décrites ici selon les instructions.

Attention – Vous ne pouvez installer qu'une seule version de Solaris Security Toolkit à la fois.

Le logiciel Solaris Security Toolkit 4.2 propose une nouvelle amélioration de la commande `pkgrm`. La présente version de la commande pkgrm vérifie en premier lieu l'intégrité de *tous* les fichiers inclus dans la distribution. Si certains fichiers sont différents, la commande `pkgrm` s'arrête et affiche un message d'erreur destiné à l'administrateur système pour que celui-ci place le fichier correct ou supprime le fichier modifié.

Les pilotes se trouvent dans le sous-répertoire `Drivers` du répertoire d'installation de Solaris Security Toolkit. Les pilotes créés par l'utilisateur sont également placés dans ce répertoire. Lorsque vous supprimez `SUNWjass` à l'aide de la commande `pkgrm`, les pilotes fournis par Solaris Security Toolkit et les pilotes modifiés par l'utilisateur sont également effacés. Toutefois, les pilotes personnalisés ajoutés par l'utilisateur restent intacts, à condition que ceux-ci aient des noms différents des pilotes inclus avec Solaris Security Toolkit.

Attention – Un pilote modifié *doit* être enregistré avant la mise à niveau. Ne modifiez *jamais* les fichiers originaux distribués avec le logiciel Solaris Security Toolkit. Ne modifiez pas un fichier de pilote. Copiez-le dans un nouveau fichier et modifiez ce dernier.

▼ Pour mettre à niveau le logiciel Solaris Security Toolkit et le système d'exploitation Solaris

1. **Suivez la meilleure pratique de mise à niveau du système disponible : effectuez une sauvegarde ou utilisez une mise à niveau Solaris.**
2. **Désinstallez la version précédente du logiciel Solaris Security Toolkit.**

3. **Installez le logiciel Solaris Security Toolkit 4.2.**

4. **Exécutez le logiciel Solaris Security Toolkit 4.2 en mode audit (validation par rapport au système mis à niveau), à l'aide des pilotes Solaris Security Toolkit et des pilotes spécifiés par l'utilisateur précédents.**

   Les pilotes spécifiés par l'utilisateur doivent se trouver dans le répertoire `Drivers`. Dans ce cas, ils peuvent être spécifiés pour une exécution `jass-execute` ou une sécurisation.

5. **Effectuez l'une des opérations suivantes :**

   a. **Si aucune erreur ne survient, passez à l'étape 6.**

   b. **En cas d'erreurs pendant l'exécution (par exemple, un script de contrôle d'exécution non installé est modifié ou un service doit être contrôlé par un FMRI), résolvez ces erreurs et recommencez les étapes 4 et 5 jusqu'à ce qu'aucune erreur ne soit générée.**

6. **Comparez `secure.driver` et le pilote personnalisé afin de déterminer si d'autres scripts finish ou audit doivent être ajoutés à ce dernier.**

7. **Effectuez l'une des opérations suivantes :**

   a. **S'il ne manque aucun script, passez à l'étape 8.**

   b. **S'il manque des scripts, ajoutez-les, et recommencez les étapes 4, 5, 6 et 7 jusqu'à ce que tous les scripts nécessaires soient inclus.**

8. **Exécutez Solaris Security Toolkit 4.2 en mode sécurisation.**

9. **Exécutez Solaris Security Toolkit 4.2 en mode audit et assurez-vous qu'il n'existe aucune erreur.**

10. **Vérifiez la configuration de sécurité et l'inclinaison du système pour déterminer si elles sont conformes aux exigences de sécurité.**

11. **Effectuez l'une des opérations suivantes :**

    a. **Si le système répond aux exigences de sécurité, passez à l'étape 12.**

    b. **Dans le cas *contraire*, mettez le pilote utilisé à jour et revenez à l'étape 8.**

12. **Testez le système de manière exhaustive pour vérifier qu'il fournit les services réseau requis et que toutes les applications sont entièrement opérationnelles.**

13. **En cas d'erreurs, mettez le pilote utilisé à jour et revenez à l'étape 8.**

    La mise à niveau est alors terminée.

▼ Pour mettre à niveau le logiciel Solaris Security Toolkit uniquement

1. **Désinstallez la version précédente du logiciel Solaris Security Toolkit.**
2. **Installez le logiciel Solaris Security Toolkit 4.2.**
3. **Passez à l'étape 4 de la section « Pour mettre à niveau le logiciel Solaris Security Toolkit et le système d'exploitation Solaris » à la page 40.**

Mise à niveau du SE Solaris uniquement

Vous n'avez pas besoin de désinstaller le logiciel Solaris Security Toolkit 4.2 si celui-ci est déjà installé et si vous mettez à niveau le SE Solaris uniquement (par exemple, lorsque vous mettez à niveau le SE Solaris 8 vers Solaris 10). Une fois la mise à niveau du SE Solaris terminée, exécutez Solaris Security Toolkit 4.2 en mode audit et vérifiez que la configuration de sécurité du système ne contient pas d'erreurs.

Téléchargement du logiciel de sécurité

La première étape de la sécurisation d'un système consiste à télécharger les packages de sécurité supplémentaires sur le système à sécuriser. Cette section décrit les tâches suivantes :

Remarque – Parmi les logiciels décrits dans cette section, Solaris Security Toolkit, le cluster de patchs recommandés et de sécurité, FixModes et l'algorithme message-digest 5 (MD5) sont essentiels. Vous pouvez utiliser une version commerciale de Secure Shell, disponible auprès de nombreux fournisseurs, à la place d'OpenSSH. Installez et utilisez un produit Secure Shell sur tous les systèmes. Sous les SE Solaris 9 et 10, utilisez la version de Secure Shell (SSH) incluse. Sous le SE Solaris 10, utilisez la commande `/usr/bin/digest` incluse pour les sommes de contrôle MD5.

Téléchargement du logiciel Solaris Security Toolkit

Le logiciel Solaris Security Toolkit est distribué au format du package SE Solaris. Téléchargez d'abord le logiciel Solaris Security Toolkit, puis installez-le sur le serveur où vous envisagez de l'utiliser en mode autonome ou bien sur un serveur JumpStart pour le mode JumpStart.

Remarque – Les noms de fichiers utilisés dans ces instructions *ne renvoient pas* à un numéro de version. Téléchargez *toujours* la dernière version à partir du site Web.

Tout au long de ce guide, la variable d'environnement `JASS_HOME_DIR` se réfère au répertoire racine du logiciel Solaris Security Toolkit, soit `/opt/SUNWjass` par défaut.

▼ Pour télécharger la version `pkg`

1. **Téléchargez le fichier de distribution du logiciel (`SUNWjass-`*n.n*`.pkg.tar.Z`).**

   Le fichier source se trouve à l'adresse suivante :

   `http://www.sun.com/security/jass`

   Remarque – Si vous n'arrivez pas à télécharger le logiciel, utilisez l'option « Enregistrer sous » de votre navigateur.

   ---

2. **Extrayez le fichier de distribution du logiciel dans un répertoire sur le serveur en utilisant la commande `uncompress` :**

   ```
   # uncompress SUNWjass-n.n.pkg.tar.Z
   ```

3. **Désarchivez le package de distribution à l'aide de la commande correspondante :**

   ```
   # tar -xvf SUNWjass-n.n.pkg.tar
   ```

4. **Installez le fichier de distribution du logiciel dans un répertoire sur le serveur en utilisant la commande `pkgadd` comme indiqué :**

   ```
   # pkgadd -d SUNWjass-n.n.pkg SUNWjass
   ```

   Où *n.n* correspond à la version téléchargée la plus récente.

   L'exécution de cette commande crée le répertoire `SUNWjass` dans `/opt`. Ce sous-répertoire contient tous les répertoires Solaris Security Toolkit et les fichiers associés.

Téléchargement du cluster de patchs recommandés

Les patchs sont distribués par Sun pour corriger les problèmes de performances, stabilité, fonctionnalité et sécurité du SE Solaris. Pour la sécurité d'un système, il est essentiel de toujours installer le cluster de patchs le plus récent. Afin de garantir que la dernière version du cluster de patchs recommandés et de sécurité pour le SE Solaris est installée, cette section décrit le téléchargement du dernier cluster de patchs.

Remarque – Avant d'installer des patchs, évaluez-les et testez-les sur des systèmes hors production ou pendant le programme de maintenance.

▼ Pour télécharger un cluster de patchs recommandés

Avant d'installer un cluster de patchs, lisez les fichiers `README` de chaque patch et toute autre documentation fournie. Ces documents contiennent souvent des conseils et des informations qu'il est utile de connaître avant d'installer un cluster de patchs.

1. **Téléchargez le dernier cluster de patchs à partir du site Web SunSolve OnLine à l'adresse suivante :**

   `http://sunsolve.sun.com`

2. **Cliquez sur le lien Patches dans la barre de navigation de droite.**

3. **Cliquez sur le lien Recommended Patch Clusters.**

4. **Sélectionnez la version appropriée du SE Solaris dans la liste déroulante Recommended Solaris Patch Clusters.**

   Dans le cas présent, le SE Solaris 10 est sélectionné.

5. **Choisissez l'option de téléchargement souhaitée (HTTP ou FTP) en cliquant sur le bouton radio associé, puis cliquez sur Go.**

   Une boîte de dialogue d'enregistrement sous s'affiche dans la fenêtre du navigateur.

6. **Enregistrez le fichier localement.**

7. **Déplacez le fichier de manière sécurisée vers le système en cours de sécurisation.**

   Utilisez la commande de copie sécurisée `scp`(1) ou une autre méthode de transfert de fichier sécurisé.

   Utilisez la commande `scp` comme suit :

```
# scp 10_Recommended.zip target01:
```

8. **Déplacez le fichier dans le répertoire** `/opt/SUNWjass/Patches` **et décompressez-le.**

   Par exemple :

EXEMPLE DE CODE 3-1 Déplacement d'un fichier de patch dans le répertoire `/opt/SUNWjass/Patches`

```
# cd /opt/SUNWjass/Patches
# mv /répertoire d'enregistrement du fichier/10_Recommended.zip .
# unzip 10_Recommended.zip
Archive:     10_Recommended.zip
   creating: 10_Recommended/
  inflating: 10_Recommended/CLUSTER_README
  inflating: 10_Recommended/copyright
  inflating: 10_Recommended/install_cluster
[. . .]
```

Le cluster de patchs est installé automatiquement quand vous avez téléchargé les autres packages de sécurité et exécuté le logiciel Solaris Security Toolkit.

Remarque – Si vous *ne placez pas* le cluster de patchs recommandés et de sécurité dans le répertoire `/opt/SUNWjass/Patches`, un message d'avertissement s'affiche quand vous exécutez le logiciel Solaris Security Toolkit. Vous pouvez ignorer ce message si aucun cluster de patchs n'est concerné, comme c'est souvent le cas avec les nouvelles versions du SE Solaris.

Téléchargement du logiciel FixModes

FixModes est un package qui renforce les autorisations par défaut de fichiers et de répertoires du SE Solaris. Le renforcement de ces autorisations peut améliorer considérablement la sécurité générale. Plus les autorisations sont restrictives, plus il est difficile pour les utilisateurs malveillants d'obtenir des privilèges sur un système.

Remarque – Des changements significatifs ont été apportés au SE Solaris 10 pour améliorer les autorisations par défaut d'objets précédemment modifiés par le package FixModes, afin que le logiciel ne soit plus nécessaire. Par conséquent, les scripts finish et audit `install-fixmodes` ne peuvent pas être utilisés sur des systèmes exécutant le SE Solaris 10.

▼ Pour télécharger le logiciel FixModes

1. **Téléchargez les binaires précompilés de FixModes à l'adresse suivante :**

   `http://www.sun.com/security/jass`

   FixModes est distribué en version package sous forme de fichier précompilé et compressé, formaté pour les systèmes Solaris. Le nom du fichier est `SUNBEfixm.pkg.Z`.

2. **Déplacez le fichier de manière sécurisée sur le système en cours de sécurisation à l'aide de la commande `scp` ou d'une autre méthode garantissant un transfert sécurisé du fichier.**

   Utilisez la commande `scp` comme suit :

```
# scp SUNBEfixm.pkg.Z target01:
```

3. **Décompressez et enregistrez le fichier `SUNBEfixm.pkg.Z` dans le répertoire `Packages` de Solaris Security Toolkit situé dans `/opt/SUNWjass/Packages`, à l'aide des commandes suivantes :**

```
# uncompress SUNBEfixm.pkg.Z
# mv SUNBEfixm.pkg /opt/SUNWjass/Packages/
```

   Le cluster de patchs est installé automatiquement quand vous avez téléchargé les autres packages de sécurité et exécuté le logiciel Solaris Security Toolkit.

Téléchargement du logiciel OpenSSH

Dans tout environnement sécurisé, le chiffrement est utilisé en association avec une authentification puissante pour la protection de sessions utilisateur interactives. Il faut, au minimum, chiffrer l'accès au réseau.

L'outil le plus utilisé pour la mise en oeuvre du chiffrement est le logiciel Secure Shell, en version intégrée dans le SE Solaris, en version commerciale tierce ou en version freeware. Pour mettre en oeuvre toutes les modifications de sécurité introduites par le logiciel Solaris Security Toolkit, vous devez inclure un produit Secure Shell.

Remarque – Sous les SE Solaris 9 et 10, utilisez la version de Secure Shell fournie avec le système d'exploitation. Cette version de Secure Shell bénéficie du support technique Sun et s'intègre à d'autres fonctions de sécurité du SE Solaris, telles que BSM (Basic Security Module).

Le logiciel Solaris Security Toolkit désactive tous les services utilisateur interactifs non chiffrés et lesdémons sur le système, en particulier les démons tels que `in.telnetd`, `in.ftpd`, `in.rshd` et `in.rlogind`.

Secure Shell vous permet d'accéder au système comme vous le feriez en utilisant Telnet et FTP.

▼ Pour télécharger le logiciel OpenSSH

Remarque – Si le serveur exécute le SE Solaris 9 ou 10, vous pouvez utiliser le logiciel Secure Shell intégré et ignorer les étapes d'installation d'OpenSSH décrites dans cette section. Par conséquent, les scripts finish et audit `install-ssh` ne peuvent pas être utilisés sur des systèmes exécutant le SE Solaris 10.

- **Recherchez l'article ou le livre Sun BluePrints en ligne suivant, et utilisez les instructions qu'il contient pour télécharger le logiciel :**
  - Article Sun BluePrints en ligne décrivant la compilation et le déploiement d'OpenSSH, intitulé « Building and Deploying OpenSSH on the Solaris Operating Environment », disponible à l'adresse suivante :

    `http://www.sun.com/blueprints`
  - Publication Sun BluePrints intitulée *Secure Shell in the Enterprise*, disponible dans les librairies.

  OpenSSH est installé automatiquement quand vous avez téléchargé tous les autres packages de sécurité et exécuté le logiciel Solaris Security Toolkit.

Attention – *Ne compilez pas* OpenSSH et *n'installez pas* les compilateurs sur le système en cours de sécurisation. Utilisez un système Solaris distinct exécutant la même version de SE, la même architecture et le même mode (par exemple, Solaris 8, Sun4U™ (`sun4u`) et 64 bits) pour compiler OpenSSH. Si vous mettez en oeuvre une version commerciale de SSH, aucune compilation n'est requise. L'objectif est de limiter la disponibilité des compilateurs à des intrus potentiels. Toutefois, la non installation locale des compilateurs sur un système *ne constitue pas* une protection significative contre certains agresseurs qui peuvent toujours installer des outils précompilés.

Téléchargement du logiciel MD5

Le logiciel MD5 génère des empreintes digitales numériques MD5 sur le système en cours de sécurisation. Générez les empreintes digitales numériques, puis comparez-les avec les indications des publications Sun, afin de détecter les binaires du système modifiés ou attaqués par un *cheval de Troie*, caché à l'intérieur d'un fichier apparemment sûr par des utilisateurs non autorisés. En modifiant les binaires du système, les agresseurs s'ouvrent une porte dérobée sur le système ; ils cachent leur présence et pourraient causer l'instabilité du système.

Remarque – Si le serveur exécute le SE Solaris 10, vous pouvez utiliser la commande `/usr/bin/digest` intégrée et ignorer les étapes d'installation de MD5 qui suivent cette section.

▼ Pour télécharger le logiciel MD5

Remarque – Solaris Security Toolkit n'installe pas et ne contrôle pas l'installation du logiciel MD5, comme l'indique la procédure suivante pour les systèmes Solaris 10. Le logiciel MD5 est inutile sur les systèmes exécutant le SE Solaris 10, car la commande `digest`(1M) inclut désormais la fonctionnalité MD5.

---

1. **Téléchargez les binaires MD5 à partir du site Web suivant :**

   `http://www.sun.com/security/jass`

   Les programmes MD5 sont distribués en version package sous forme de fichier compressé.

2. **Déplacez le fichier `SUNBEmd5.pkg.Z` de manière sécurisée sur le système en cours de sécurisation à l'aide de la commande `scp` ou d'une autre méthode garantissant un transfert sécurisé du fichier.**

   Utilisez la commande `scp` comme suit :

```
# scp SUNBEmd5.pkg.Z target01:
```

3. **Décompressez et déplacez le fichier vers le répertoire `Packages` situé dans répertoire `/opt/SUNWjass/Packages` de Solaris Security Toolkit, en utilisant une commande similaire à la suivante :**

```
# uncompress SUNBEmd5.pkg.Z
# mv SUNBEmd5.pkg /opt/SUNWjass/Packages/
```

Une fois le logiciel MD5 enregistré dans le répertoire `/opt/SUNWjass/Packages`, il suffit d'exécuter Solaris Security Toolkit pour l'installer.

Vous pouvez utiliser les binaires MD5 installés pour vérifier l'intégrité des exécutables sur le système au moyen de la base de données d'empreintes digitales de Solaris. Pour de plus amples informations sur la base de données d'empreintes digitales Solaris, reportez-vous à l'article Sun BluePrints en ligne intitulé « The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files ».

4. ***(Facultatif)* Téléchargez et installez les logiciels Solaris Fingerprint Database Companion et Solaris Fingerprint Database Sidekick à partir du site Web Sun BluePrints à l'adresse suivante :**

`http://www.sun.com/blueprints/tools`

Remarque – Même si l'étape 4 est facultative, il est réellement préférable de l'appliquer à tous les systèmes d'exploitation.

Installez et utilisez ces outils facultatifs avec le logiciel MD5. Ces outils simplifient le processus de validation des binaires du systèmes par rapport à la base de données de sommes de contrôle MD5. Utilisez fréquemment ces outils pour valider l'intégrité des binaires et des fichiers du SE Solaris sur un système sécurisé.

Vous pouvez télécharger ces outils et leurs instructions à partir de l'article Sun BluePrints en ligne intitulé « The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files ».

Vérifiez l'intégrité des outils de sécurité téléchargés. Avant l'installation et l'exécution de Solaris Security Toolkit et des logiciels de sécurité supplémentaires, validez leur intégrité à l'aide des sommes de contrôle MD5. Des sommes de contrôle MD5 sont disponibles à cet effet sur la page de téléchargement de Solaris Security Toolkit.

Personnalisation des profils de sécurité

De nombreux modèles de profils de sécurité sont inclus sous forme de pilotes dans la distribution du logiciel Solaris Security Toolkit. Les profils de sécurité mis en oeuvre par ces pilotes désactivent les services *non requis* et activent les fonctions de sécurité facultatives désactivées par `secure.driver`. Comme mentionné dans le chapitre précédent, le profil de sécurité par défaut et les modifications apportées par ces pilotes peuvent *ne pas convenir* à vos systèmes.

Avant d'exécuter Solaris Security Toolkit, vérifiez les profils de sécurité par défaut et personnalisez-les en fonction de votre environnement, ou développez-en de nouveaux. Vous trouverez des techniques et des instructions relatives à la personnalisation des profils de sécurité dans le manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Installation et exécution du logiciel

Il est important d'accomplir les tâches préliminaires suivantes avant l'exécution du logiciel Solaris Security Toolkit. La sécurisation est, en majeure partie, effectuée automatiquement quand vous exécutez le logiciel Solaris Security Toolkit.

- Téléchargez les logiciels de sécurité supplémentaires et le logiciel Solaris Security Toolkit sur le système à sécuriser ou sur le serveur JumpStart. Voir « Téléchargement du logiciel de sécurité » à la page 42.
- Configurez votre système pour le mode autonome ou JumpStart. Voir « Détermination du mode à utiliser » à la page 38.
- Le cas échéant, personnalisez Solaris Security Toolkit en fonction de votre environnement.
- Avant l'installation et l'exécution de Solaris Security Toolkit et des logiciels de sécurité supplémentaires, validez leur intégrité à l'aide des sommes de contrôle MD5.

Vous pouvez lancer le logiciel Solaris Security Toolkit directement à partir de la ligne de commande ou d'un serveur JumpStart.

Pour obtenir la liste des options de ligne de commande et d'autres informations sur l'exécution du logiciel, reportez-vous à l'une des sections suivantes :

- « Exécution du logiciel en mode autonome » à la page 51
- « Exécution du logiciel en mode JumpStart » à la page 62

Exécution du logiciel en mode autonome

L'EXEMPLE DE CODE 3-2 décrit l'utilisation de la ligne de commande en mode autonome.

EXEMPLE DE CODE 3-2 Échantillon d'utilisation de la ligne de commande en mode autonome

```
# ./jass-execute -h

usage:

Pour appliquer ce kit d'outils à un système en utilisant la syntaxe
suivante :
   jass-execute [-r répertoire_racine -p version_se ]
      [ -q | -o fichier_sortie ] [ -m adresse_e-mail ]
      [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente du kit d'outils à partir
d'un système :
   jass-execute -u [ -b | -f | -k ] [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ] [ -V [3|4] ]

Pour l'audit d'un système en fonction d'un profil prédéfini :
   jass-execute -a driver [ -V [0-4] ] [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ]

Pour supprimer des fichiers enregistrés lors d'une exécution
précédente du kit d'outils :
   jass-execute -c [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ] [ -V [3|4] ]

Pour afficher l'historique des applications du kit d'outils sur un
système :
   jass-execute -H

Pour afficher la dernière application du kit d'outils sur un
système :
   jass-execute -l

Pour afficher ce message d'aide :
   jass-execute -h
   jass-execute -?

Pour afficher les informations sur la version de ce programme :
   jass-execute -v

#
```

Le TABLEAU 3-1 dresse la liste des options de ligne de commande disponibles avec

TABLEAU 3-1 Utilisation des options de ligne de commande avec `jass-execute`

Option	Description
`-a` *pilote*	Détermine si un système est conforme au profil de sécurité. *Ne l'utilisez pas* avec les options `-b`, `-k`, `-f`, `-c`, `-d`, `-h`, `-H`, `-l`, `-p`, `-r` et `-u`.
`-b`	Sauvegarde tout fichier ayant été modifié manuellement depuis la dernière sécurisation, puis restaure le système à son état d'origine. Utilisez-la *uniquement* avec l'option `-u`.
`-c`	Spécifie l'option de nettoyage. Supprime des fichiers enregistrés lors d'une exécution précédente de Solaris Security Toolkit.
`-d` *pilote*	Spécifie le pilote à exécuter en mode autonome. *Ne l'utilisez pas* avec les options `-a`, `-b`, `-c`, `-f`, `-h`, `-H`, `-k` et `-u`.
`-f`	Annule les modifications effectuées pendant une sécurisation sans proposer d'exceptions, même si les fichiers ont été modifiés manuellement après une sécurisation. Utilisez-la *uniquement* avec l'option `-u`.
`-H`	Affiche l'historique du logiciel Solaris Security Toolkit sur le système.
`-h |-?`	Affiche le message d'aide de `jass-execute`, qui présente les options disponibles. Utilisez-la seule. Toute option spécifiée en plus de l'option `-h|-?` est ignorée.
`-k`	Conserve toute modification manuelle apportée aux fichiers après une sécurisation. Utilisez-la *uniquement* avec l'option `-u`.
`-l`	Affiche la dernière application du logiciel Solaris Security Toolkit installé sur le système.
`-m` *adresse_e-mail*	Indique une adresse email pour le support interne.
`-o` *fichier_sortie*	Spécifie le fichier de sortie et le chemin complet pour accéder à ce dernier.
`-p` *version_se*	Indique la version du SE Solaris. Le format est identique à celui de l'option `uname -r`. Vous *devez* l'utiliser avec l'option `-r` *répertoire_racine*.
`-q`	Spécifie le mode silencieux. Les messages ne s'affichent pas pendant l'exécution de cette commande. La sortie est stockée dans `JASS_REPOSITORY/`.
`-r` *répertoire_racine*	Indique le répertoire racine utilisé pendant l'exécution de la commande `jass-execute`. Le répertoire racine est `/`. Il est défini par la variable d'environnement Solaris Security Toolkit `JASS_ROOT_DIR`. Le SE Solaris en cours de sécurisation est disponible dans `/`. Par exemple, si vous souhaitez sécuriser un répertoire du SE distinct, temporairement monté sous `/mnt`, utilisez l'option `-r` pour spécifier `/mnt`. Vous *devez* l'utiliser avec l'option `-p` *version_se*.

TABLEAU 3-1 Utilisation des options de ligne de commande avec `jass-execute` *(suite)*

Option	Description	
`-u`	Exécute l'option d'annulation et affiche des invites interactives sur l'action à entreprendre en cas d'exception. *Ne l'utilisez pas* avec les options `-a`, `-c`, `-d`, `-h`, `-l`, `-p`, `-r`, et `-H`.	
`-V` *niveau_verbosité*	Spécifie le niveau de verbosité pour un audit. Il existe cinq niveaux (0 à 4)	
	`0`	Ligne unique indiquant la réussite ou l'échec.
	`1`	Pour chaque script, une ligne unique indique la réussite ou l'échec, puis une ligne de score total s'affiche sous toutes les lignes de script.
	`2`	Pour chaque script, affiche les résultats de tous les contrôles.
	`3`	Affiche plusieurs lignes avec une sortie complète, y compris les messages de bannière et d'en-tête. Ce niveau est la valeur par défaut.
	`4`	Affiche plusieurs lignes (toutes les données à partir du niveau 3), ainsi que toutes les entrées qui sont générées par la fonction de consignation `logDebug`. Ce niveau s'utilise pour le débogage.
`-v`	Affiche les informations sur la version de ce programme.	

une description de chacune d'elles.

Pour de plus amples informations sur les options disponibles avec la commande `jass-execute` en mode autonome, reportez-vous aux sections suivantes :

- « Option d'audit » à la page 55
- « Option de nettoyage » à la page 55
- « Option d'affichage de l'aide » à la page 57
- « Option de pilote » à la page 58
- « Option de notification par e-mail » à la page 59
- « Option d'exécution de l'historique » à la page 60
- « Option d'exécution la plus récente » à la page 60
- « Option de fichier de sortie » à la page 61
- « Option de sortie silencieuse » à la page 61
- « Option de répertoire racine » à la page 61
- « Option d'annulation » à la page 62

Pour obtenir une liste complète des pilotes disponibles, reportez-vous à la section « Répertoire `Drivers` » à la page 5. De nouvelles versions du logiciel peuvent contenir des pilotes supplémentaires.

▼ Pour exécuter le logiciel en mode autonome

1. **Exécutez** `secure.driver` **(ou un script spécifique au produit tel que** `sunfire_15k_sc-secure.driver`**) comme suit :**

EXEMPLE DE CODE 3-3 Exécution du logiciel en mode autonome

```
# ./jass-execute -d secure.driver

[NOTE] The following prompt can be disabled by setting
JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured,
it is both possible and likely that by default all remote shell
and file transfer access to this system will be disabled upon
reboot effectively locking out any user without console access to
the system.

Are you sure that you want to continue? (YES/NO) [NO]
y

[NOTE] Executing driver, secure.driver

================================================================
secure.driver: Driver started.
================================================================

================================================================
Solaris Security Toolkit Version: 4.2.0
Node name:                        ufudu
Zone name:                        global
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.10
Date:                             Tue Jul 5 16:28:24 EST 2005
================================================================
[...]
```

Pour obtenir une liste complète des pilotes disponibles, reportez-vous à la section « Répertoire `Drivers` » à la page 5. De nouvelles versions du logiciel peuvent contenir des pilotes supplémentaires.

2. **Après l'exécution du logiciel Solaris Security Toolkit sur un système, redémarrez ce dernier pour mettre en oeuvre les modifications.**

   Pendant la sécurisation, une série de modifications sont apportées à la configuration du client. Celles-ci peuvent inclure la désactivation des scripts de démarrage de services, la désactivation d'options de services et l'installation de nouveaux binaires ou de nouvelles bibliothèques par le biais de patchs. Ces modifications risquent de *ne pas être* activées tant que vous n'avez pas redémarré le client.

3. **Une fois le système réinitialisé, vérifiez que les modifications sont correctes et complètes.**

   Voir « Validation des modifications système » à la page 63.

4. **En cas d'erreurs, corrigez celles-ci et exécutez à nouveau le logiciel Solaris Security Toolkit en mode autonome.**

Option d'audit

L'option `-a` permet au logiciel Solaris Security Toolkit d'effectuer un audit afin de déterminer si un système est conforme à son profil de sécurité. Cette opération vérifie non seulement que les modifications des fichiers système sont actives, mais aussi que les processus désactivés antérieurement sont exécutés et que les packages supprimés sont réinstallés. Pour de plus amples informations sur cette fonction, reportez-vous au chapitre 6.

Synopsis d'utilisation de la ligne de commande pour l'audit d'un système en fonction d'un profil de sécurité :

```
# jass-execute -a pilote [ -V [0-4] ] [ -q | -o fichier-sortie ]
[ -m adresse-email ]
```

Option de nettoyage

L'option `-c` supprime des fichiers enregistrés lors d'une exécution précédente de Solaris Security Toolkit. Vous pouvez utiliser les options de mode silencieux (`-q`), de sortie (`-o`), d'e-mail (`-m`) et de verbosité (`-V`) avec l'option de nettoyage.

L'EXEMPLE DE CODE 3-4 décrit l'utilisation de l'option `-c` qui produit une sortie du type suivant :

EXEMPLE DE CODE 3-4 Échantillon de sortie de l'option `-c`

```
# bin/jass-execute -c
Executing driver, clean.driver

Please select Solaris Security Toolkit runs to clean:
1.  July 15, 2005 at 11:41:02 (/var/opt/SUNWjass/run/20050715114102)
2.  July 15, 2005 at 11:44:03 (/var/opt/SUNWjass/run/20050715114403)
Choice ('q' to exit)?  2
[NOTE] Cleaning previous run from /var/opt/SUNWjass/run/20050715114403

================================================================================
clean.driver: Driver started.
================================================================================


================================================================================
Toolkit Version: 4.2.0
Node name:       sstzone
Zone name:       sstzone
Host ID:         80cb346c
Host address:    10.8.28.45
MAC address:     8:0:20:cb:34:6c
OS version:      5.10
Date:            Fri Jul 15 11:44:58 PDT 2005

================================================================================
clean.driver: Performing CLEANUP of /var/opt/SUNWjass/run/20050715114403.
================================================================================

================================================================================
clean.driver: Driver finished.
================================================================================

================================================================================
[SUMMARY] Results Summary for CLEAN run of clean.driver
[SUMMARY] The run completed with a total of 1 script run.
[SUMMARY] There were  Failures in   0 Scripts
[SUMMARY] There were  Errors   in   0 Scripts
[SUMMARY] There were  Warnings in   0 Scripts
[SUMMARY] There was a Note     in   1 Script
[SUMMARY] Notes Scripts listed in:
          /var/opt/SUNWjass/run/20050715114403/jass-clean-script-notes.txt
================================================================================
```

Option d’affichage de l’aide

L'option `-h` affiche le message d'aide de la commande `jass-execute`, qui présente les options disponibles.

L'option `-h` produit une sortie du type suivant :

EXEMPLE DE CODE 3-5 Échantillon de sortie de l’option `-h`

```
# ./jass-execute -h
Pour appliquer ce kit d'outils à un système en utilisant la syntaxe
suivante :
   jass-execute [-r répertoire_racine -p version_se ]
      [ -q | -o fichier_sortie ] [ -m adresse_e-mail ]
      [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente du kit d'outils à partir
d'un système :
   jass-execute -u [ -b | -f | -k ] [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ] [ -V [3|4] ]

Pour l'audit d'un système en fonction d'un profil prédéfini :
   jass-execute -a driver [ -V [0-4] ] [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ]

Pour supprimer des fichiers enregistrés lors d’une exécution
précédente du kit d’outils :
   jass-execute -c [ -q | -o fichier_sortie ]
      [ -m adresse_e-mail ] [ -V [3|4] ]

Pour afficher l'historique des applications du kit d'outils sur un
système :
   jass-execute -H

Pour afficher la dernière application du kit d'outils sur un
système :
   jass-execute -l

Pour afficher ce message d'aide :
   jass-execute -h
   jass-execute -?

Pour afficher les informations sur la version de ce programme :
   jass-execute -v

Notez que seul le nom du pilote doit être spécifié lorsque vous
utilisez
les options ’-d’ ou ’-a’. Vous n’avez pas besoin d’indiquer de
chemin car le script
```

EXEMPLE DE CODE 3-5 Échantillon de sortie de l'option `-h` *(suite)*

```
est supposé se trouver dans le répertoire Drivers.

L'option d'annulation '-u' exclut l'une ou l'autre des options
'-d' et '-a'. Le comportement d'annulation par défaut demande à
l'utilisateur l'action à entreprendre lorsqu'un
fichier à restaurer a été modifié, car la somme de contrôle est
incorrecte.

L'option -u peut être associée aux options '-k', '-b' et '-f' pour
écraser le comportement interactif par défaut. Vous devez utiliser
l'une de ces
options en mode silencieux ('-q').

L'option '-k' peut être utilisée pour conserver toujours le fichier
actuel et la sauvegarde
lorsque la somme de contrôle est incorrecte. L'option 'b' permet
de sauvegarder
le fichier actuel et de restaurer l'original quand la somme de
contrôle est incorrecte.
L'option 'f' écrase toujours l'original si la somme de contrôle
est incorrecte, sans enregistrer l'original modifié.
```

Option de pilote

L'option `-d` *pilote* indique le pilote à exécuter en mode autonome.

Vous devez spécifier un pilote avec l'option `-d`. Le logiciel Solaris Security Toolkit appose le préfixe `Drivers/` au nom du script ajouté. Vous devez entrer *uniquement* le nom du script sur la ligne de commande.

Remarque – *N'utilisez pas* l'option `-d` avec les options `-a`, `-b`, `-c`, `-f`, `-H`, `-h`, `-k` et `-u`.

Une sécurisation `jass-execute` utilisant l'option `-d` *pilote* produit une sortie du type suivant :

EXEMPLE DE CODE 3-6 Échantillon de sortie de l'option `-d` *pilote*

```
# ./jass-execute -d secure.driver
[...]
[NOTE] Executing driver, secure.driver

================================================================
secure.driver: Driver started.
================================================================

================================================================
Solaris Security Toolkit Version: 4.2.0
Node name:                        ufudu
Zone name:                        global
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.10
Date:                             Tue Jul 5 16:28:24 EST 2005
================================================================
[...]
```

Option de notification par e-mail

L'option `-m` *adresse_email* est un mécanisme qui permet au logiciel Solaris Security Toolkit d'envoyer automatiquement la sortie de l'audit autonome, du nettoyage, de la sécurisation et de l'annulation par e-mail une fois l'exécution terminée. Le rapport électronique est généré en plus des journaux éventuellement créés sur le système à l'aide d'autres options et des journaux locaux créés par le logiciel Solaris Security Toolkit.

Échantillon d'exécution de Solaris Security Toolkit appelant `sunfire_15k_sc-config.driver` à l'aide de l'option de notification par e-mail :

```
# ./jass-execute -m root -d sunfire_15k_sc-config.driver
[...]
```

Option d’exécution de l’historique

L’option `-H` constitue un mécanisme simple qui permet de déterminer le nombre d’exécutions du logiciel Solaris Security Toolkit sur un système. Toutes les exécutions sont répertoriées, y compris celles qui ont été annulées.

L'option `-H` produit une sortie du type suivant :

EXEMPLE DE CODE 3-7 Échantillon de sortie de l'option `-H`

```
# ./jass-execute -H
Remarque : Ces informations concernent uniquement les applications
           de Solaris Security Toolkit, à partir de la version 0.3.

La liste ci-après contient les applications de Solaris Security
Toolkit sur le système. Cette liste est présentée en ordre
chronologique inverse :

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
2.   June 31, 2004 at 12:10:29 (20040631121029)
3.   June 31, 2004 at 12:04:15 (20040631120415)
```

La sortie indique que le logiciel Solaris Security Toolkit a été exécuté trois fois sur le système et que la plus récente a été annulée.

Option d’exécution la plus récente

L’option `-l` propose un mécanisme qui permet de déterminer l’exécution la plus récente. Il s’agit *toujours* de l’exécution la plus récente répertoriée également par l’option `-H`.

L'option `-l` produit une sortie du type suivant :

EXEMPLE DE CODE 3-8 Échantillon de sortie de l'option `-l`

```
# ./jass-execute -l

Remarque : Ces informations concernent uniquement les applications
           de Solaris Security Toolkit, à partir de la version 4.2.0.

La dernière application de Solaris Security Toolkit a été effectuée
le :

1.   June 31, 2005 at 12:20:19 (20040631122019) (UNDONE)
```

Option de fichier de sortie

L'option `-o` *fichier-sortie* redirige la sortie de console de `jass-execute` vers un *fichier-sortie* distinct. Vous pouvez indiquer un chemin de fichier de sortie (*fichier_sortie*) entièrement qualifié.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Elle s'avère particulièrement utile pour les connexions de terminaux bas débits. La sortie générée par Solaris Security Toolkit peut être volumineuse ; ceci dépend du niveau de verbosité (*niveau_verbosité*) spécifié.

Cette option peut être utilisée avec les options `-a`, `-d` ou `-u`.

L'option `-o` produit une sortie du type suivant :

EXEMPLE DE CODE 3-9 Échantillon de sortie de l'option `-o`

```
# ./jass-execute -o /var/tmp/root/jass-output.txt -d secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to /var/tmp/root/jass-output.txt
```

Option de sortie silencieuse

L'option `-q` évite que la sortie de Solaris Security Toolkit ne soit envoyée vers la console pendant une sécurisation.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Comme l'option `-o`, cette option est particulièrement utile quand Solaris Security Toolkit est exécuté via une tâche `cron` ou sur une connexion réseau bas débit.

Elle peut être utilisée avec les options `-a`, `-c`, `-d` ou `-u`.

L'option `-q` produit une sortie du type suivant :

EXEMPLE DE CODE 3-10 Échantillon de sortie de l'option `-q`

```
# ./jass-execute -q -d secure.driver
[NOTE] Executing driver, secure.driver
```

Option de répertoire racine

L'option `-r` *répertoire-racine* indique le répertoire racine utilisé pendant les exécutions `jass-execute`. L'option `-r` requiert également l'option `-p` afin de spécifier la version de la plate-forme (SE). Le format de l'option `-p` est équivalent à celui produit par l'option `uname -r`.

Le répertoire racine est `/`. Il est défini par la variable d'environnement Solaris Security Toolkit `JASS_ROOT_DIR`. Le SE Solaris en cours de sécurisation est disponible dans `/`. Par exemple, si vous souhaitez sécuriser un répertoire du SE distinct, temporairement monté sous `/mnt`, utilisez l'option `-r` pour spécifier `/mnt`. Tous les scripts sont appliqués à cette image de SE.

Option d'annulation

Grâce à l'option `-u`, le logiciel Solaris Security Toolkit peut annuler des modifications système effectuées pendant une sécurisation. Chaque script finish peut être annulé à l'aide de l'option `-u`. En outre, la fonction d'annulation de Solaris Security Toolkit est intégrée aux sommes de contrôle générées à chaque exécution. Pour de plus amples informations sur cette fonction, reportez-vous au chapitre 4.

Il existe trois autres options que vous pouvez utiliser avec l'option `-u` :

- L'option `-b` (sauvegarde) sauvegarde tout fichier modifié manuellement depuis la dernière sécurisation, puis restaure le système à son état d'origine.
- L'option `-f` (forçage) annule les modifications effectuées pendant une sécurisation sans proposer d'exceptions, même si les fichiers ont été modifiés manuellement après une sécurisation.
- L'option `-k` (conservation) conserve toutes les modifications manuelles effectuées depuis la dernière sécurisation.

Synopsis d'utilisation de la ligne de commande d'annulation :

```
# jass-execute -u [ -b | -f | -k ] [ -q | -o fichier_sortie ]
        [ -m adresse_e-mail ] [ -V [3|4] ]
```

Exécution du logiciel en mode JumpStart

Le mode JumpStart est contrôlé par le pilote de Solaris Security Toolkit, inséré dans le fichier `rules` sur le serveur JumpStart.

Si vous *n'avez pas* configuré votre environnement de sorte à utiliser le mode JumpStart, reportez-vous au chapitre 5.

Pour de plus amples informations sur la technologie JumpStart, reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

▼ Pour exécuter le logiciel en mode JumpStart

Pour être exécuté en mode JumpStart, le logiciel Solaris Security Toolkit doit être intégré à l'environnement JumpStart et appelé par les scripts finish associés à une installation JumpStart. Pour de plus amples informations sur l'intégration du logiciel Solaris Security Toolkit dans votre environnement, reportez-vous au chapitre 5.

1. **Quand toutes les modifications requises ont été apportées aux pilotes, installez le client en utilisant l'infrastructure JumpStart.**

   Pour effectuer cette tâche, utilisez la commande suivante à l'invite `ok` du client.

   ```
   ok> boot net - install
   ```

   Une fois l'installation terminée, le logiciel JumpStart redémarre le système.

   Le système doit être correctement configuré. Pendant la sécurisation, une série de modifications sont apportées à la configuration du client. Celles-ci peuvent inclure la désactivation des scripts de démarrage de services, la désactivation d'options de services et l'installation de nouveaux binaires ou de nouvelles bibliothèques à l'aide de patchs. Ces modifications risquent de *ne pas être* activées tant que vous n'avez pas redémarré le client.

2. **Une fois le système réinitialisé, vérifiez que les modifications sont correctes et complètes.**

   Voir « Validation des modifications système » à la page 63.

3. **Si vous rencontrez des erreurs, corrigez-les et réinstallez le système d'exploitation du client.**

Validation des modifications système

Une fois le système réinitialisé, vérifiez que les modifications sont correctes et complètes, comme l'indiquent les sections suivantes.

Contrôle d'assurance qualité des services

L'un des défis significatifs de la sécurisation d'un système consiste à déterminer les services de SE à activer pour que le système fonctionne correctement. Les services du SE Solaris peuvent être nécessaires parce qu'ils sont utilisés directement. Par exemple, Secure Shell permet de se connecter à un système. D'autres services peuvent être utilisés indirectement, tels que le démon RPC d'interface graphique (IG) d'outils de gestion de logiciels tiers.

Vous devez déterminer la plupart de ces besoins avant d'exécuter le logiciel Solaris Security Toolkit. (Voir « Détermination des conditions requises pour les applications et les services » à la page 21). Toutefois, le *seul* mécanisme définitif est l'installation et la sécurisation du système. Effectuez ensuite un test complet des fonctionnalités requises à l'aide d'un test d'assurance qualité. Vous devez suivre un plan d'assurance qualité pour tout nouveau système déployé qui vient d'être sécurisé. De même, il vous faut réaliser un test complet des systèmes déployés en cours de sécurisation afin de vérifier que toutes les fonctionnalités requises et attendues sont présentes.

Si le processus d'assurance qualité découvre des écarts, effectuez les opérations suivantes :

1. Déterminez la zone affectée en fonction des directives du chapitre 2.
2. Vérifiez que l'application est exécutée selon la configuration modifiée.
3. Annulez l'exécution de Solaris Security Toolkit.
4. Modifiez le profil de sécurité (pilote) en fonction de la solution du problème.
5. Exécutez de nouveau le logiciel Solaris Security Toolkit.

Le résultat final doit consister en un profil de sécurité pouvant être exécuté sur le système sans affecter négativement aucune fonctionnalité requise.

Évaluation de la sécurité de la configuration

Lorsque vous vérifiez que le système exécute toutes les fonctions requises, évaluez également la configuration de la sécurité afin de déterminer si le système atteint le niveau de sécurisation souhaité. Ceci peut impliquer différentes tâches en fonction de la sécurisation ou de la minimisation effectué(e) sur le système.

Vous devez au moins vérifier les points suivants de la configuration du système :

- Assurez-vous que tous les patchs recommandés et de sécurité sont installés.
- Vérifiez que *seuls* les processus requis et pertinents sont exécutés, et que leurs arguments sont corrects.
- Vérifiez que *seuls* les démons requis sont exécutés et que leurs arguments sont corrects.
- Vérifiez que *seuls* les ports requis sont ouverts sur le système (vérification locale, par exemple `netstat -a`, et distante) à l'aide d'un scanneur de ports, tel que Nmap, qui peut déterminer les ports disponibles sur une interface réseau.
- Assurez-vous que *seuls* les packages requis du SE Solaris sont installés, si le système a été minimisé.

Cette vérification est indispensable pour les systèmes nouvellement construits et sécurisés. Lors de la sécurisation d'anciens systèmes, vous devez vérifier le SE sous-jacent pour déterminer si des modifications non autorisées ont été effectuées. Pour que la vérification de l'intégrité soit plus efficace, montez la structure de fichiers du système en mode lecture seule et exécutez le logiciel de contrôle de l'intégrité à partir d'une instance de SE connue. Les outils décrits dans l'article Sun BluePrints en ligne intitulé « The Solaris Fingerprint Database—A Security Tool for Solaris Software and Files » s'avèrent utiles dans ce cas.

Validation des profils de sécurité

Une fois le système sécurisé, et les services et capacités requis validés, utilisez la fonction d'audit pour vous assurer que le profil de sécurité a été appliqué correctement et entièrement. Cette tâche est essentielle pour deux raisons. Elle permet tout d'abord de vérifier que le système est sécurisé selon les besoins. Ensuite, elle garantit que le profil de sécurité défini pour le système est correctement reporté dans la configuration de Solaris Security Toolkit. Ce contrôle est primordial car les informations de configuration sont utilisées pour maintenir le profil de sécurité du système pendant la totalité de son cycle de vie de déploiement.

Pour de plus amples informations sur la fonction d'audit, reportez-vous au chapitre 6.

Tâches suivant l'installation

Si vous installez le logiciel sur un système déployé, reportez-vous à la section « Tâches suivant l'installation » à la page 32 qui contient une description des tâches à effectuer après l'installation sur les systèmes déployés.

CHAPITRE 4

Annulation de modifications du système

Ce chapitre décrit l'annulation des modifications du système introduites par le logiciel Solaris Security Toolkit pendant la sécurisation. Cette option fournit un mécanisme automatisé permettant de restaurer un système à son état initial avant une ou plusieurs sécurisations.

Ce chapitre contient les sections suivantes :

Consignation et annulation des changements

Chaque sécurisation par Solaris Security Toolkit crée un répertoire d'exécution dans `JASS_REPOSITORY`. Les noms de ces répertoires sont basés sur la date et l'heure de début d'exécution. Outre l'affichage de la sortie sur un écran, le logiciel Solaris Security Toolkit crée un ensemble de fichiers dans le répertoire pour le suivi des modifications et la journalisation des opérations.

Les fichiers enregistrés dans le répertoire suivent les modifications apportées au système et activent la fonction d'annulation.

Attention – L'administrateur ne doit *jamais* modifier le contenu des fichiers du répertoire `JASS_REPOSITORY`. Cette opération pourrait endommager le contenu des fichiers et provoquer des erreurs inattendues ou la corruption du système quand vous utilisez la fonction d'annulation.

Quand vous utilisez le logiciel Solaris Security Toolkit pour la sécurisation d'un système, que ce soit en mode JumpStart ou autonome, le logiciel consigne les modifications dans le fichier `JASS_REPOSITORY/jass-manifest.txt`. Ce fichier contient la liste des opérations que la fonction `undo` utilise pour annuler les modifications. Il contient des informations sur les opérations de sécurisation mises en oeuvre par le logiciel Solaris Security Toolkit, y compris les fichiers créés, copiés, déplacés ou supprimés. Par ailleurs, ce fichier peut contenir aussi bien des entrées standard que des entrées personnalisées, qui sont requises pour l'annulation de modifications plus complexes, telles les installations de packages. Un fichier `jass-manifest.txt` distinct est créé pour chaque sécurisation.

Remarque – La fonction `undo` du logiciel Solaris Security Toolkit annule *uniquement* les modifications qui correspondent à des entrées dans les fichiers globaux.

La commande `undo` parcourt les fichiers globaux générés pendant l'exécution de Solaris Security Toolkit et stockés dans `JASS_REPOSITORY`. Elle peut restaurer les fichiers sauvegardés à leurs emplacements d'origine, selon que vous avez utilisez l'option de -b (sauvegarde), -f (forçage) ou -k (conservation). Pour de plus amples informations sur ces options, reportez-vous aux sections suivantes :

- « Option de sauvegarde » à la page 73
- « Option de forçage » à la page 73
- « Option de conservation » à la page 73

Si vous *n'avez pas* sauvegardé les fichiers pendant la sécurisation, et si la variable `JASS_SAVE_BACKUP` est définie dans le fichier `user.init` sur `0` ou si l'option `-c` est utilisée, la fonction d'annulation *n'est pas* disponible. Pour de plus amples informations, reportez-vous à la section « Conditions requises pour l'annulation de modifications du système » à la page 69.

L'annulation d'une modification par Solaris Security Toolkit *n'entraîne pas* la suppression du répertoire associé. Par contre, deux fichiers sont créés dans le répertoire `JASS_REPOSITORY` : `jass-undo-log.txt` et `reverse-jass-manifest.txt`. Ensuite, la modification qui a été annulée n'apparaît plus dans la liste à la prochaine exécution de `jass-execute -u`. Une sécurisation ne peut être annulée qu'une seule fois.

Conditions requises pour l'annulation de modifications du système

L'utilisation de la fonction d'annulation du logiciel Solaris Security Toolkit est soumise aux restrictions et conditions suivantes.

- Dans les versions 0.3 à 4.2 de Solaris Security Toolkit, vous avez la possibilité d'utiliser la fonction d'annulation pour des exécutions en mode autonome ou JumpStart. Toutefois, vous pouvez annuler des modifications *uniquement* en mode autonome. La fonction d'annulation *ne peut pas* être utilisée pendant une installation JumpStart.
- Si vous configurez Solaris Security Toolkit afin de *ne pas créer* de fichiers de sauvegarde, en mode JumpStart ou autonome, la fonction d'annulation *n'est pas* disponible. La création de copies de sauvegarde est désactivée si le paramètre `JASS_SAVE_BACKUP` est défini sur `0`.
- Une exécution *ne peut être annulée qu'une seule fois*.
- Si vous développez un nouveau script finish, veillez à utiliser les fonctions de structure de Solaris Security Toolkit. Vous devez créer un script audit correspondant et ajouter des entrées au fichier global à l'aide de la fonction `add_to_manifest`. Sinon, le logiciel Solaris Security Toolkit n'aura aucun moyen de connaître votre personnalisation.
- *Ne modifiez en aucun cas* le contenu des répertoires `JASS_REPOSITORY`. La modification des fichiers peut endommager le contenu et causer des erreurs inattendues ou la corruption du système quand vous utilisez la fonction d'annulation.

Personnalisation de scripts pour l'annulation des modifications

Solaris Security Toolkit dispose d'une structure suffisamment flexible pour la conception et la construction de scripts finish. La structure vous permet d'étendre les capacités du logiciel Solaris Security Toolkit en fonction des besoins de votre organisation, tout en vous facilitant la gestion de la configuration des systèmes pendant leurs cycles de vie.

Lors de la personnalisation de scripts, il est important de comprendre l'effet de chacune des actions sur la fonction d'annulation. Pour simplifier la personnalisation des scripts, des fonctions auxiliaires introduisent les modifications voulues dans les fichiers globaux. (La fonction `undo` utilise le contenu des fichiers globaux pour annuler les sécurisations). Dans la plupart des cas, ces fonctions auxiliaires fournissent ce dont vous avez besoin pour personnaliser les scripts de votre organisation.

Pour obtenir une liste des fonctions auxiliaires et des informations sur leur utilisation, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*. Utilisez ces fonctions auxiliaires à la place des commandes système équivalentes, afin que les annulations référencent les entrées correspondantes dans les fichiers globaux.

Il peut toutefois arriver qu'aucune fonction auxiliaire ne soit associée à la fonction que vous devez exécuter. Si tel est le cas, utilisez la fonction spéciale appelée `add_to_manifest`. En utilisant cette fonction, vous pouvez insérer manuellement des entrées dans les fichiers globaux sans faire appel à une fonction auxiliaire. Utilisez cette fonction spéciale avec précaution en veillant à protéger l'intégrité du système et le référentiel de Solaris Security Toolkit. Par exemple, vous pouvez utiliser cette fonction spéciale pour ajouter des packages qui ne sont pas au format `pkg` de Sun. Dans cet exemple, vous devez indiquer à la fonction `undo` la méthode de suppression des packages ajoutés sous un autre format lors de la sécurisation.

Avec les fonctions auxiliaires et la fonction spéciale `add_to_manifest`, le logiciel Solaris Security Toolkit offre un outil simple et flexible pour personnaliser des scripts et étendre les modifications aux annulations.

Si vous modifiez le comportement d’un script finish sans utiliser ces fonctions, le logiciel Solaris Security Toolkit ne pourra pas identifier les modifications apportées. Par conséquent, vous devez annuler manuellement les modifications qui *ne sont pas* référencées dans les fichiers globaux.

Autre exemple : avant de modifier un fichier sur le système, vous devez d'abord en enregistrer la version originale. Hors du contexte du logiciel Solaris Security Toolkit, les utilisateurs accomplissent généralement cette tâche en exécutant la commande `/usr/bin/cp`. Toutefois, si vous utilisez directement cette commande dans le contexte du logiciel Solaris Security Toolkit, ce dernier n'a aucun moyen de savoir qu'une entrée globale doit être créée. À la place de la commande `cp`, utilisez la fonction auxiliaire `backup_file`. Cette fonction enregistre une copie du fichier original, avec un suffixe de `SUFFIXE_JASS` et ajoute une entrée globale indiquant au logiciel Solaris Security Toolkit qu'une copie du fichier a été effectuée. Cette fonction entraîne également le calcul des sommes de contrôle du fichier. Les sommes de contrôle du fichier sont utilisées par la fonction d'annulation ainsi que par la commande `jass-check-sum`.

Contrôle des fichiers modifiés manuellement

Même si la commande `jass-execute -u` contrôle automatiquement les fichiers qui ont été modifiés manuellement après une sécurisation, il s'avère parfois utile d'utiliser la commande `jass-check-sum` pour répertorier et vérifier les fichiers qui ont été modifiés.

Cette commande vous permet de passer en revue le contenu du répertoire `JASS_REPOSITORY` et d'effectuer les sommes de contrôle sur tous les fichiers répertoriés dans les fichiers globaux, afin de déterminer les fichiers modifiés depuis l'enregistrement de leurs sommes de contrôle pendant la sécurisation. Effectué avant une annulation forcée, ce contrôle permet d'obtenir de précieuses informations qui vous éviteront des heures de dépannage inutile.

Ci-dessous, un exemple de sortie.

EXEMPLE DE CODE 4-1 Échantillon de sortie de fichiers modifiés manuellement

```
# ./jass-check-sum
File Name              Saved CkSum             Current CkSum
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
/etc/inet/inetd.con    1643619259:6883         2801102257:6879
/etc/logadm.conf       2362963540:1042         640364414:1071
/etc/default/inetd     3677377803:719          2078997873:720
```

La sortie indique que trois fichiers ont été modifiés après la sécurisation.

Utilisation d'options avec la fonction d'annulation

Cette section décrit la commande `jass-execute -u` et les options que vous pouvez utiliser pendant l'exécution d'une annulation.

Remarque – Vous *ne pouvez pas* utiliser les options `-c`, `-d`, `-a`, `-h`, `-l` et `-H` avec la fonction d'annulation. Vous devez vous servir de l'option `-b`, `-k` ou `-f` lors d'une annulation en mode silencieux.

La commande `jass-execute -u` constitue la méthode standard d'exécution d'une `annulation`. Cette commande détecte automatiquement les fichiers qui ont été modifiés manuellement depuis la dernière sécurisation. Si le logiciel Solaris Security Toolkit détecte des fichiers modifiés manuellement après une sécurisation, il vous demande de choisir l'une des réponses suivantes :

1. Effectuez une copie de sauvegarde du fichier le plus récent avant de restaurer l'original (le fichier qui existait avant la sécurisation).
2. Conservez le fichier le plus récent et *ne restaurez pas* le fichier original.
3. Forcez l'écrasement de tout fichier modifié manuellement (certaines données pourraient, de ce fait, être perdues) et restaurez le fichier original.
4. Effectuez toujours une copie de sauvegarde du fichier le plus récent avant de restaurer l'original (le fichier qui existait avant la sécurisation).
5. Conservez toujours le fichier le plus récent et *ne restaurez pas* le fichier original.
6. Forcez toujours l'écrasement de tout fichier modifié manuellement (certaines données pourraient, de ce fait, être perdues) et restaurez le fichier original.

Si vous souhaitez définir le traitement par la commande d'annulation des fichiers modifiés depuis la sécurisation, utilisez les options `-b (sauvegarde), -k` (conservation) ou `-f` (forçage) lorsque vous exécutez la commande d'annulation.

Le TABLEAU 4-1 contient la liste des options de ligne de commande que vous pouvez utiliser avec la commande d'annulation. Pour de plus amples informations sur chaque option, reportez-vous aux sections ci-après.

TABLEAU 4-1 Utilisation des options de ligne de commande avec la commande d'annulation

Option	Description
`-b`	Sauvegarde tout fichier modifié manuellement depuis la dernière sécurisation, puis restaure le système à son état d'origine.
`-f`	Annule les modifications effectuées pendant une sécurisation sans vous proposer d'exception, même si les fichiers ont été modifiés manuellement après une sécurisation.
`-k`	Conserve toute modification manuelle apportée aux fichiers après une sécurisation.
`-m`	Envoie la sortie à une adresse e-mail.
`-o`	Dirige la sortie vers un fichier.
`-q`	Empêche l'affichage de la sortie à l'écran. Également appelée « option silencieuse ». La sortie est stockée dans le fichier `JASS_REPOSITORY/jass-undo-log.txt`.
`-V`	Spécifie le niveau de verbosité d'une annulation.

Option de sauvegarde

L'option `-b` sauvegarde automatiquement les fichiers qui ont été modifiés manuellement depuis la dernière sécurisation, puis restaure les fichiers à leur état d'origine avant la sécurisation. Pour mettre en oeuvre les modifications manuelles, vous *devez* comparer les fichiers restaurés et les fichiers sauvegardés, et ajuster vous-même les différences. Un fichier sauvegardé à l'aide de cette option est similaire à l'exemple suivant.

```
/etc/motd.BACKUP.JASS_SUFFIX
```

Option de forçage

L'option `-f` annule les modifications apportées pendant une sécurisation sans aucune exception, même si les fichiers ont été modifiés manuellement après une sécurisation. L'annulation *ne compare pas* les sommes de contrôle des fichiers enregistrés et les versions actuelles des fichiers. En conséquence, si vous avez modifié des fichiers manuellement après une sécurisation, les modifications sont écrasées et perdues après l'annulation.

Il peut s'avérer nécessaire de mettre de nouveau en oeuvre les modifications manuellement après l'exécution d'une annulation, et d'ajuster les différences entre des groupes de fichiers, en fonction des types de modifications apportées.

Remarque – Pour éviter ces problèmes, utilisez la commande `jass-check-sum` ou l'option de ligne de commande `-b` précédemment citée.

Option de conservation

L'option `-k` conserve automatiquement toute modification manuelle apportée aux fichiers après une sécurisation au lieu de restaurer les fichiers originaux. L'option `-k` détecte les incohérences dans les fichiers, génère et consigne un avertissement et *n'écrase pas* le fichier avec l'original. Les *seules* modifications annulées sont celles pour lesquelles les sommes de contrôle enregistrées sont correctes.

Cette option n'est pas sans inconvénients. Par exemple, un système peut devenir incohérent si un sous-ensemble de fichiers modifiés par un script finish est modifié ultérieurement.

Prenez le script finish `remove-unneeded-accounts.fin`. Ce script modifie les fichiers `/etc/passwd` et `/etc/shadow` sur le système. Si un utilisateur change manuellement un mot de passe après une sécurisation, la somme de contrôle associée au fichier `/etc/shadow` *ne correspond pas* à la valeur enregistrée par le logiciel Solaris Security Toolkit. En conséquence, en cas d'utilisation de l'option de conservation, *seul* le fichier `/etc/passwd` retrouve son état d'origine. Le fichier `/etc/shadow` conserve sa forme actuelle. Les deux fichiers ne sont plus cohérents.

Option de fichier de sortie

L'option `-o` */chemin/complet/du/fichier_sortie* redirige la sortie de console de `jass-execute` vers un fichier de sortie (*fichier-sortie*) distinct.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Elle est particulièrement utile en présence d'une connexion de terminal bas débit, car une annulation Solaris Security Toolkit génère souvent un volume significatif de données en sortie.

Option de sortie silencieuse

Remarque – Vous devez vous servir de l'option `-b`, `-k` ou `-f` lors d'une annulation en mode silencieux.

L'option `-q` empêche le logiciel Solaris Security Toolkit d'afficher la sortie à l'écran. Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Comme l'option `-o`, cette option est particulièrement utile lorsque le logiciel Solaris Security Toolkit est exécuté via une tâche `cron` ou une connexion réseau bas débit.

Option de notification par e-mail

L'option `-m` *adresse_email* indique au logiciel Solaris Security Toolkit qu'il doit envoyer une copie de l'exécution complète à une adresse e-mail. La notification par e-mail s'ajoute aux journaux générés sur le système à l'aide d'autres options.

Annulation de modifications du système

Il est parfois nécessaire d'annuler les modifications apportées pendant une ou plusieurs sécurisations Solaris Security Toolkit. Si vous estimez que les modifications apportées pendant une sécurisation ont des conséquences négatives sur le système, vous pouvez les annuler.

Par exemple, si vous découvrez après une sécurisation qu'un service requis, tel que Solaris Volume Manager (SVM), a été désactivé, effectuez les opérations suivantes :

1. Annulez la sécurisation.
2. Créez un pilote personnalisé.

   Reportez-vous à la section Personnalisation des pilotes du chapitre 4 du manuel *Solaris Security Toolkit 4.2 Reference Manual* pour obtenir des instructions sur la personnalisation des pilotes.
3. Activez les services SVM à utiliser à l'aide de la variable d'environnement `JASS_SVCS_ENABLE`.

   Reportez-vous à la section `JASS_SVCS_ENABLE` du chapitre 7 du *Solaris Security Toolkit 4.2 Reference Manual* pour obtenir des instructions sur l'utilisation de `JASS_SVCS_ENABLE`.
4. Recommencez la sécurisation.

Cette section décrit l'annulation des modifications apportées pendant une ou plusieurs sécurisations. L'annulation d'une sécurisation est soumise à certaines restrictions et conditions. Voir « Conditions requises pour l'annulation de modifications du système » à la page 69.

▼ Pour annuler une exécution de Solaris Security Toolkit

1. **Sauvegardez et réinitialisez le système.**

   Sauvegardez et réinitialisez le système avant chaque annulation pour garantir que le système revienne ou puisse revenir à un état connu et à un fonctionnement correct.
2. **Déterminez les options que vous voulez utiliser avec la commande `jass-execute -u`.**

   Voir « Utilisation d'options avec la fonction d'annulation » à la page 71.

   Les instructions qui suivent supposent que vous utilisez la commande `jass-execute -u`.

3. **Pour annuler une ou plusieurs sécurisations à l'aide de l'option standard `-u`, entrez la commande suivante à partir de `JASS_HOME_DIR/bin`:**

```
# ./jass-execute -u
```

Le logiciel Solaris Security Toolkit collecte des informations sur chaque sécurisation en recherchant tous les fichiers globaux contenus dans `JASS_REPOSITORY`. Si un fichier global est vide ou absent, le logiciel suppose qu'aucune modification ne doit être annulée et l'annulation de ce fichier est ignorée. De plus, si le répertoire du fichier global contient également un fichier intitulé `jass-undo-log.txt`, le logiciel suppose que l'annulation a déjà été effectuée et ne l'exécute donc pas. Une fois toutes les informations collectées, les résultats s'affichent. Ci-dessous, un exemple de sortie.

EXEMPLE DE CODE 4-2 Échantillon de sortie de sécurisations pouvant être annulées

```
# ./jass-execute -u
[NOTE] Executing driver, undo.driver
Please select a JASS run to restore through:
1. January 24, 2003 at 13:57:27
(/var/opt/SUNWjass/run/20030124135727)
2. January 24, 2003 at 13:44:18
(/var/opt/SUNWjass/run/20030124134418)
3. January 24, 2003 at 13:42:45
(/var/opt/SUNWjass/run/20030124134245)
4. January 24, 2003 at 12:57:30
(/var/opt/SUNWjass/run/20030124125730)

Choice? ('q' to exit)?
```

Dans cet exemple, quatre sécurisations distinctes ont été trouvées. Ces sécurisations ont apporté des modifications au système et *n'ont pas* été annulées. La liste des sécurisations est *toujours* présentée par ordre chronologique inverse. La première entrée dans la liste correspond à la sécurisation la plus récente.

4. **Vérifiez la sortie pour déterminer les sécurisations à annuler, puis entrez les numéros correspondants.**

Pour chaque entrée sélectionnée, le logiciel Solaris Security Toolkit annule chaque sécurisation de numéro d'index égal ou inférieur à la valeur sélectionnée. Ainsi, il annule les modifications dans l'ordre inverse où elles ont été effectuées, en commençant par la sécurisation la plus récente pour terminer par celle que vous avez sélectionnée. En suivant l'exemple précédent, si vous sélectionnez la sécurisation 3, vous `annulez` d'abord les modifications de la sécurisation 1, puis celles de la sécurisation 2 et enfin celles de la sécurisation 3.

L'EXEMPLE DE CODE 4-3 illustre la sortie générée quand l'annulation porte sur deux entrées de fichier global.

EXEMPLE DE CODE 4-3 Échantillon de sortie d'une d'annulation portant sur plusieurs entrées de fichier global

```
[...]

================================================================
undo.driver: Performing UNDO of
//var/opt/SUNWjass/run/20050715145837.
================================================================

[...]

================================================================
undo.driver: Undoing Finish Script: update-cron-allow.fin
================================================================

[NOTE] Undoing operation COPY.
cp -p /etc/cron.d/cron.allow.JASS.20050715145906
/etc/cron.d/cron.allow
rm -f /etc/cron.d/cron.allow.JASS.20050715145906

[NOTE] Removing a Solaris Security Toolkit-created file.
rm -f /etc/cron.d/cron.allow

[...]
```

Dans cet exemple, le logiciel Solaris Security Toolkit annule une opération de copie et supprime un fichier qui avait été ajouté pendant une sécurisation. La sortie d'une annulation indique les commandes utilisées pour restaurer le système, de telle sorte que le processus est facile à comprendre et à identifier au cas où vous auriez besoin de dépanner la configuration d'un système.

Si Solaris Security Toolkit réussit à vérifier les fichiers modifiés depuis la dernière sécurisation, l'annulation continue jusqu'à ce que toutes les sécurisations et tous les fichiers globaux correspondants soient traités et les modifications annulées.

Outre la collecte d'informations sur chaque sécurisation qu'il effectue en recherchant tous les fichiers globaux contenus dans `JASS_REPOSITORY`, le logiciel Solaris Security Toolkit effectue les opérations suivantes :

a. Il compare la somme de contrôle de chaque fichier modifié.

b. Il génère et consigne un message pour toute erreur dans les fichiers de somme de contrôle.

c. Il vous demande l'action à entreprendre pour ces fichiers.

5. **Si l'annulation détecte une exception (un fichier qui a été modifié manuellement après la sécurisation), entrez l'une des options.**

Remarque – Le logiciel Solaris Security Toolkit mémorise les options de sauvegarde, conservation et forçage sélectionnées pour un fichier d'exception spécifique. Vous n'avez donc pas à sélectionner de nouveau ces options quand ce fichier constitue une nouvelle fois une exception pendant une annulation.

L'exemple de sortie suivant illustre une exception et les possibilités de traitement de cette exception.

EXEMPLE DE CODE 4-4 Échantillon de sortie d'une exception d'annulation

```
[...]

================================================================
undo.driver: Undoing Finish Script: enable-process-accounting.fin
================================================================

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]    filename = /var/spool/cron/crontabs/adm
[WARN]    current  = db27341e3e1f0f27d371d2e13e6f47ce
[WARN]    saved    = a7f95face84325cddc23ec66d59374b0

Sélectionnez une action :
1. Sauvegarde – Enregistre le fichier actuel AVANT de restaurer
l'original.
2. Conservation   - Conserve le fichier actuel SANS effectuer de
modifications.
3. Forçage  - Ignore les modifications manuelles et ÉCRASE le
fichier actuel.

REMARQUE : Les options supplémentaires suivantes s'appliquent à ce
fichier et à TOUS
les fichiers suivants :
4. TOUJOURS sauvegarder.
5. TOUJOURS conserver.
6. TOUJOURS forcer.

Entrez 1, 2, 3, 4, 5 ou 6 :
```

Dans cet exemple, si vous choisissez l'élément 1, la sortie suivante s'affiche.

EXEMPLE DE CODE 4-5 Échantillon de sortie de l'option de sauvegarde pendant une annulation

```
Entrez 1, 2, 3, 4, 5 ou 6 : 1

[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.

[NOTE] BACKUP specified, creating backup copy of
/var/spool/cron/crontabs/adm.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /var/spool/cron/crontabs/adm to
/var/spool/cron/crontabs/adm.BACKUP.JASS.20050715151817
cp -p /var/spool/cron/crontabs.JASS/adm.JASS.20050715151719
/var/spool/cron/crontabs/adm
rm -f /var/spool/cron/crontabs.JASS/adm.JASS.20050715151719

[NOTE] Undoing operation COPY.
cp -p /var/spool/cron/crontabs.JASS/root.JASS.20050715151717
/var/spool/cron/crontabs/root
rm -f /var/spool/cron/crontabs.JASS/root.JASS.20050715151717

[NOTE] Undoing operation MAKE DIRECTORY.
rmdir /var/spool/cron/crontabs.JASS

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc3.d/S22acct

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc0.d/K22acct
```

Si vous choisissez l'élément 4, la sortie suivante s'affiche.

EXEMPLE DE CODE 4-6 Échantillon de sortie de l'option « Toujours sauvegarder » pendant une annulation

```
Enter 1, 2, 3, 4, 5, or 6: 4
[NOTE] Always do BACKUP selected. Overriding JASS_UNDO_TYPE with
BACKUP.

[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.

[NOTE] BACKUP specified, creating backup copy of
/var/spool/cron/crontabs/adm.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /var/spool/cron/crontabs/adm to
/var/spool/cron/crontabs/adm.BACKUP.JASS.20050715152126
cp -p /var/spool/cron/crontabs.JASS/adm.JASS.20050715151953
/var/spool/cron/crontabs/adm
rm -f /var/spool/cron/crontabs.JASS/adm.JASS.20050715151953

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]    filename = /var/spool/cron/crontabs/root
[WARN]    current  = 741af21a62ea7a9e7abe6ba04855aa76
[WARN]    saved    = bcf180f45c65ceff3bf61012cb2b4982
[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.
[NOTE] BACKUP specified, creating backup copy of
/var/spool/cron/crontabs/root.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /var/spool/cron/crontabs/root to
/var/spool/cron/crontabs/root.BACKUP.JASS.20050715152127
cp -p /var/spool/cron/crontabs.JASS/root.JASS.20050715151951
/var/spool/cron/crontabs/root
rm -f /var/spool/cron/crontabs.JASS/root.JASS.20050715151951

[NOTE] Undoing operation MAKE DIRECTORY.
rmdir /var/spool/cron/crontabs.JASS

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc3.d/S22acct

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc0.d/K22acct
```

Une fois que Solaris Security Toolkit a terminé les annulations sélectionnées, vous devez passer en revue les fichiers marqués comme modifiés depuis la dernière sécurisation et effectuer toute modification système nécessaire. *Ne redémarrez pas* le système tant que vous n'avez pas manuellement analysé ces modifications, car elles peuvent provoquer un état incohérent du système.

Remarque – Dans l'exemple, le fichier modifié a été sauvegardé sous un nouveau nom : `/etc/.login.BACKUP.JASS.20050715151817`. Après l'annulation, comparez ce fichier à `/etc/.login` pour déterminer si d'autres ajustements sont nécessaires.

---

6. **Ajustez toutes les exceptions éventuelles avant de continuer.**

7. **Après l'ajustement des exceptions, redémarrez le système.**

   Le redémarrage du système est nécessaire pour que les modifications apportées à la configuration du SE Solaris soient prises en compte.

Attention – Lorsqu'il est exécuté en mode JumpStart, Solaris Security Toolkit définit le mot de passe `root`. En cas d'annulation ultérieure, le mot de passe `root` redevient le mot de passe *no* antérieur. Ainsi, tout utilisateur peut se connecter au compte racine sans mot de passe. Réinitialisez le mot de passe `root` à l'aide de la commande `passwd`(1) après avoir effectué une annulation. Le logiciel Solaris Security Toolkit 4.2 imprime également un message d'avertissement lorsqu'il se trouve dans cet état.

CHAPITRE 5

Configuration et gestion de serveurs JumpStart

Ce chapitre décrit la configuration et la gestion de serveurs JumpStart en vue de l'utilisation du logiciel Solaris Security Toolkit. La technologie JumpStart, qui est un mécanisme d'installation du SE Solaris basé sur un réseau Sun, peut exécuter le logiciel Solaris Security Toolkit au cours du processus d'installation.

Le mode JumpStart de Solaris Security Toolkit se base sur la technologie JumpStart, disponible pour le produit SE Solaris à partir de la version 2.1. La technologie JumpStart facilite la gestion de la complexité en automatisant complètement l'installation du SE Solaris et du logiciel système, ce qui évite les erreurs et permet la normalisation des systèmes. Il s'agit d'une solution permettant de satisfaire les conditions d'une installation et d'un déploiement rapides des systèmes.

Les avantages de la technologie JumpStart sont évidents lors de la sécurisation de systèmes. En utilisant la technologie JumpStart avec le logiciel Solaris Security Toolkit, vous pouvez sécuriser des systèmes pendant les installations automatisées du SE Solaris. Cette solution permet de garantir que la sécurité système est abordée et normalisée au moment de l'installation du système. Pour obtenir JumpStart Enterprise Toolkit (JET), qui facilite les installations basées sur JumpStart et inclut des modules prenant en charge la sécurisation au moyen du logiciel Solaris Security Toolkit, consultez le site de téléchargement de Sun à l'adresse suivante :

`http://www.sun.com/download/`

Pour de plus amples informations sur la technologie JumpStart, reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Ce chapitre contient les sections suivantes :

Configuration de serveurs et d'environnements JumpStart

Pour une utilisation dans un environnement JumpStart, installez la source Solaris Security Toolkit située dans `/opt/SUNWjass` (pour les téléchargements `pkg`) dans le répertoire de base du serveur JumpStart. Le répertoire par défaut sur un serveur JumpStart est `/jumpstart`. Une fois cette tâche terminée, `JASS_HOME_DIR` devient le répertoire de base du serveur JumpStart.

Cette section suppose que le lecteur maîtrise la technologie JumpStart et qu'il a un environnement JumpStart à disposition.

Seules quelques opérations sont nécessaires pour intégrer le logiciel Solaris Security Toolkit dans une architecture JumpStart.

▼ Pour configurer l'environnement au mode JumpStart

1. **Installez la source Solaris Security Toolkit dans le répertoire racine du serveur JumpStart.**

   Le logiciel Solaris Security Toolkit peut être installé dans `JASS_REPOSITORY`, soit `/jumpstart` dans le cas présent, comme l'indique l'exemple suivant :

   ```
   # pwd
   /opt/SUNWjass
   # pkgadd -R /jumpstart -d . SUNWjass
   ```

   En général, le logiciel Solaris Security Toolkit est installé dans le répertoire `SI_CONFIG_DIR` du serveur JumpStart, qui devrait également être `JASS_HOME_DIR`.

2. **Si vous devez modifier le fichier `sysidcfg` du SE Solaris 2.5.1, apportez ces modifications au fichier contenu dans le répertoire `JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1`.**

   Si vous utilisez le SE Solaris 2.5.1, le fichier `sysidcfg` dans `JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1` *ne peut pas* être utilisé directement parce que cette version de Solaris ne prend en charge que les fichiers `sysidcfg` contenus dans `SI_CONFIG_DIR` et non dans des sous-directoires distincts. Pour résoudre cette restriction sous le SE Solaris 2.5.1, le logiciel Solaris Security Toolkit possède un répertoire `SI_CONFIG_DIR/sysidcfg` qui est relié au fichier `JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1/sysidcfg`.

3. **Copiez** `JASS_HOME_DIR/Drivers/user.init.SAMPLE` **dans** `JASS_HOME_DIR/Drivers/user.init` **à l'aide de la commande suivante :**

```
# pwd
/jumpstart/opt/SUNWjass/Drivers
# cp user.init.SAMPLE user.init
```

4. **Si vous souhaitez installer le package Solaris Security Toolkit sur le système cible pendant une installation JumpStart, vous devez placer ce package dans le répertoire** `JASS_PACKAGE_MOUNT` **défini dans le fichier** `user.init`**. Par exemple :**

```
# cp /chemin/à/SUNWjass.pkg JASS_HOME_DIR/Packages
```

5. **Si vous rencontrez des problèmes avec un serveur JumpStart à multiconnexion, modifiez les deux entrées de** `JASS_PACKAGE_MOUNT` **et** `JASS_PATCH_MOUNT` **pour corriger le chemin d'accès aux répertoires** `JASS_HOME_DIR/Patches` **et** `JASS_HOME_DIR/Packages`**.**

6. **Si vous voulez installer le logiciel Solaris Security Toolkit dans un sous-répertoire de** `SI_CONFIG_DIR`**, tel que** `SI_CONFIG_DIR/path/to/JASS`**, ajoutez ce qui suit au fichier** `user.init` **:**

```
if [ -z "${JASS_HOME_DIR}" ]; then
       if [ "${JASS_STANDALONE}" = 0 ]; then
              JASS_HOME_DIR="${SI_CONFIG_DIR}/path/to/JASS"
       fi
fi
export JASS_HOME_DIR
```

7. **Sélectionnez ou créez un pilote Solaris Security Toolkit (par exemple, le pilote par défaut** `secure.driver`**).**
   - Si vous entendez utiliser *tous* les scripts répertoriés dans `hardening.driver` et `config.driver`, ajoutez le chemin `Drivers/secure.driver` au fichier `rules`.
   - Si vous devez utiliser *uniquement les scripts sélectionnés*, faites des copies de ces fichiers, puis modifiez les copies. Reportez-vous à la section Personnalisation des pilotes du chapitre 4 du manuel *Solaris Security Toolkit 4.2 Reference Manual* pour obtenir des instructions sur la copie et la modification des pilotes.

Attention – Ne modifiez *jamais* les scripts originaux inclus avec le logiciel Solaris Security Toolkit. Pour permettre une migration efficace vers les versions supérieures du logiciel Solaris Security Toolkit, conservez séparément les fichiers d'origine et les fichiers personnalisés.

8. **Une fois le pilote terminé, apportez la modification correcte au fichier `rules`.**

   L'entrée ajoutée au fichier doit être similaire à la suivante :

```
hostname imbulu - Profiles/core.profile Drivers/secure-abc.driver
```

   Une autre modification peut être nécessaire pour que le logiciel Solaris Security Toolkit soit correctement intégré dans l'environnement JumpStart existant.

9. **Si vous utilisez les fichiers `sysidcfg` inclus avec le logiciel Solaris Security Toolkit pour automatiser l'installation du client JumpStart, vérifiez d'abord l'applicabilité de ces fichiers.**

   Si le serveur JumpStart rencontre une erreur lors de l'analyse syntaxique du fichier `sysidcfg`, le contenu du fichier est ignoré dans sa totalité.

   Après avoir terminé toutes les étapes de configuration décrites dans cette section, vous êtes en mesure d'utiliser la technologie JumpStart pour installer le SE Solaris sur le client, et sécuriser ou minimiser le système d'exploitation pendant le processus d'installation.

Utilisation de modèles de profils JumpStart

Les modèles de profils JumpStart sont des fichiers *exclusivement* utilisés avec le mode JumpStart. Le contenu obligatoire et facultatif des profils est décrit dans l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Utilisez les modèles de profils JumpStart comme échantillons pour vos propres modifications sur site. Vérifiez les profils afin de déterminer, le cas échéant, les modifications nécessaires pour une utilisation dans votre environnement.

Effectuez des copies des profils, puis modifiez les copies pour votre site. Ne modifiez pas les originaux, parce que vos personnalisations pourraient être écrasées par les mises à jour du logiciel Solaris Security Toolkit.

Les profils JumpStart suivants sont inclus avec le logiciel Solaris Security Toolkit :

- `core.profile`
- `end-user.profile`
- `developer.profile`
- `entire-distribution.profile`
- `oem.profile`
- `minimal-SunFire_Domain*.profile`

Ces profils sont décrits ci-après.

core.profile

Ce profil JumpStart installe le plus petit cluster du SE Solaris, à savoir `SUNWCreq`. Il spécifie que le partitionnement du disque comprend des partitions racine et swap, sans apporter aucune autre modification à la configuration.

end-user.profile

Ce profil JumpStart installe le cluster d'utilisateur final du SE Solaris, `SUNWCuser`, et les deux packages de SE Solaris requis pour que la comptabilisation de processus fonctionne correctement. De plus, le partitionnement du disque a été défini de manière à inclure *uniquement* les partitions racine et swap.

developer.profile

Ce profil JumpStart installe le cluster de développeur du SE Solaris, `SUNWCprog`, et les deux packages de SE Solaris requis pour que la comptabilisation de processus fonctionne correctement. Comme dans la définition de `core.profile`, les *seules* définitions supplémentaires apportées à la configuration, outre le cluster du SE Solaris, concernent le partitionnement du disque afin d'inclure les partitions racine et swap.

entire-distribution.profile

Ce profil JumpStart installe le cluster de distribution complète du SE Solaris, `SUNWCall`. Comme pour les autres profils, le partitionnement du disque est défini de manière à inclure les partitions racine et swap.

oem.profile

Ce profil JumpStart installe le cluster OEM du SE Solaris, `SUNWCXall`. Ce cluster est un surensemble du cluster de distribution complète ; il installe le logiciel OEM fourni.

minimal-SunFire_Domain*.profile

Remarque – Utilisez ces profils *uniquement* sur des systèmes exécutant les SE Solaris 8 ou 9.

Tous les profils suivants sont basés sur l'article Sun BluePrints en ligne *Minimizing Domains for Sun Fire V1280, 12K, and 15K Systems*. Les profils JumpStart suivants sont identiques à ceux mentionnés dans l'article :

- `minimal-SunFire_Domain-Apps-Solaris8.profile`
- `minimal-SunFire_Domain-Apps-Solaris9.profile`
- `minimal-SunFire_Domain-NoX-Solaris8.profile`
- `minimal-SunFire_Domain-NoX-Solaris9.profile`
- `minimal-SunFire_Domain-X-Solaris8.profile`
- `minimal-SunFire_Domain-X-Solaris9.profile`

Ajout et suppression de clients

Les scripts `add-client` et `rm-client` sont utilisés pour configurer un serveur afin que ce dernier puisse exécuter le logiciel JumpStart et effectuer l'installation d'un client à partir du réseau. Les scripts se trouvent dans le répertoire `JASS_HOME_DIR/bin`. Le mode JumpStart est contrôlé par le pilote de Solaris Security Toolkit, inséré dans le fichier `rules` sur le serveur JumpStart.

Si vous *n'avez pas* configuré votre environnement de sorte qu'il utilise le mode JumpStart, reportez-vous à la section « Configuration de serveurs et d'environnements JumpStart » à la page 84.

Dans le cas de systèmes SPARC, la commande `add-client` installe le client JumpStart et les informations de configuration requises par Solaris Security Toolkit. La commande est exécutée à partir du serveur JumpStart.

Dans le cas de systèmes x86/x64, requérant des clients Dynamic Host Configuration Protocol (DHCP), vous devez utiliser le script `add_install_client` fourni avec le média d'installation Solaris.

Script `add-client`

Pour simplifier l'ajout de clients à partir des serveurs JumpStart, utilisez cescript qui est inclus avec le logiciel Solaris Security Toolkit. La commande et les options sont décrites dans les paragraphes suivants, mais la technologie JumpStart sous-jacente *ne l'est pas*. Reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment* pour de plus amples informations sur la technologie JumpStart.

Le script `add-client` est un wrapper autour de la commande `add_install_client` et accepte les arguments suivants.

Synopsis de la commande `add-client` :

```
# add-client -c client -i serveur -m classe-client -o SE-client -s sysidcfg
```

Le TABLEAU 5-1 décrit l'entrée correcte pour la commande `add-client`.

TABLEAU 5-1 Commande JumpStart `add-client`

Option	Description
`-c` *client*	Nom d'hôte résolvable du client JumpStart.
`-h|-?`	Affiche des informations d'utilisation. À utiliser sans autre option. Toutes les options supplémentaires sont ignorées.
`-i` *serveur*	Adresse IP ou nom d'hôte résolvable de l'interface du serveur JumpStart pour ce client JumpStart. Si aucune valeur n'est spécifiée, la liste des interfaces disponibles sur l'hôte local s'affiche.
`-m` *classe-client*	Classe de l'ordinateur du client JumpStart. Cette valeur a le même format que la sortie de la commande `uname -m`.
`-o` *SE-client*	Version du SE Solaris, disponible dans le répertoire `JASS_HOME_DIR/OS`, à installer sur le client. Si aucune valeur n'est spécifiée, une liste de toutes les versions du SE Solaris disponibles dans le répertoire `JASS_HOME_DIR/OS` s'affiche.
`-s` *sysidcfg*	Chemin d'accès facultatif à un autre répertoire contenant un fichier `sysidcfg` que vous voulez utiliser pour l'identification et la configuration du système. Par défaut, cette valeur est définie sur le répertoire `JASS_HOME_DIR/Sysidcfg/`*version_Solaris*`/`, où la *version_Solaris* est extraite de l'argument `-o` requis utilisé. Si vous indiquez un chemin facultatif, utilisez un chemin relatif au répertoire `JASS_HOME_DIR`. *S*pécifiez *uniquement* le chemin d'accès au fichier `sysidcfg`.
`-v`	Informations sur la version de ce programme. Toutes les options supplémentaires sont ignorées.

Pour ajouter un client JumpStart intitulé `fr` à l'aide des valeurs par défaut, vous pouvez effectuer les opérations suivantes :

```
# /opt/SUNWjass/bin/add-client -c fr -m sun4u
Selecting default operating system, version_Solaris.
Selecting default system interface, adresse_IP.
cleaning up preexisting install client "fr"
removing fr from bootparams
updating /etc/bootparams
```

Pour ajouter un client JumpStart intitulé `fr` à un serveur JumpStart appelé `serveurjump1` en utilisant le SE Solaris 9 (12/03) et l'option `-s` *sysidcfg*, vous pouvez effectuer les opérations suivantes :

```
# /opt/SUNWjass/bin/add-client -c fr -i serveurjump1 -m sun4u -o
Solaris_9_2003-12 -s Hosts/alpha
cleaning up preexisting install client "fr"
removing fr from bootparams
updating /etc/bootparams
```

Script `rm-client`

Pour simplifier la suppression de clients des serveurs JumpStart, utilisez cescript qui est inclus avec le logiciel Solaris Security Toolkit. La commande et les options sont décrites dans les paragraphes suivants, mais la technologie JumpStart sous-jacente *ne l'est pas*. Reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment* pour de plus amples informations sur la technologie JumpStart.

Le script `rm-client` est un wrapper autour de la commande `rm_install_client` comme le script `add-client` :

Exemple d'utilisation : **`rm-client`** `[-c]` *`client`*

Où *`client`* correspond au nom d'hôte résolvable du client JumpStart.

Le TABLEAU 5-2 décrit l'entrée correcte pour la commande `rm-client`.

TABLEAU 5-2 Commande JumpStart `rm-client`

Option	Description
`-c` *client*	Nom d'hôte résolvable du client JumpStart.
`-h|-?`	Affiche des informations d'utilisation. À utiliser sans autre option. Toutes les options supplémentaires sont ignorées.
`-v`	Informations sur la version de ce programme. Toutes les options supplémentaires sont ignorées.

Pour supprimer un client JumpStart intitulé `fr`, utilisez la commande `rm-client` suivante :

```
# ./rm-client -c fr
removing fr from bootparams
```

CHAPITRE 6

Audit de sécurité de systèmes

Ce chapitre décrit l'audit (la validation) de la sécurité d'un système à l'aide du logiciel Solaris Security Toolkit. Utilisez les informations et les procédures figurant dans ce chapitre pour maintenir un profil de sécurité donné après la sécurisation. Pour les systèmes qui sont déjà déployés, vous pouvez utiliser les informations contenues dans ce chapitre afin d'évaluer la sécurité du système avant la sécurisation.

Remarque – Le terme *audit* est utilisé dans ce chapitre et dans cet ouvrage pour définir le processus automatisé de validation de la sécurité par rapport à un profil de sécurité prédéfini effectué par Solaris Security Toolkit. L'utilisation de ce terme dans cet ouvrage *ne signifie pas* que le système est complètement sécurisé après l'utilisation de l'option d'audit.

Ce chapitre contient les sections suivantes :

Maintenance de la sécurité

La maintenance de la sécurité est un processus permanent qui doit être périodiquement revu et vérifié. La maintenance d'un système sécurisé requiert le maximum d'attention étant donné que la configuration de sécurité par défaut de tout système tend à s'ouvrir de plus en plus avec le temps. (Pour de plus amples informations sur la maintenance de la sécurité, reportez-vous à la section « Maintenance de la sécurité du système » à la page 34).

Solaris Security Toolkit fournit une méthode automatisée permettant de contrôler la sécurisation d'un système en déterminant son niveau de conformité par rapport à un profil de sécurité spécifique.

Remarque – Cette méthode est disponible *uniquement* en mode autonome à l'aide de la commande `jass-execute -a` et *ne peut pas* être utilisée pendant une installation JumpStart.

Vérifiez périodiquement le niveau de sécurité des systèmes, selon une procédure manuelle ou automatique (par exemple, via une `tâche cron` ou un script`rc`). Par exemple, cinq jours après la sécurisation d'une nouvelle installation, exécutez la commande d'audit du logiciel Solaris Security Toolkit (`jass-execute -a` *nom-pilote*) pour déterminer si le niveau de sécurité du système a changé par rapport à l'état défini dans le profil de sécurité.

La fréquence d'audit de la sécurité dépend de la sensibilité de l'environnement et de votre stratégie de sécurité. Certains utilisateurs effectuent un audit toutes les heures, d'autres tous les jours et d'autres encore une fois par mois. Certains effectuent un mini audit (avec un nombre limité de contrôles) toutes les heures et un audit complet (avec tous les contrôles possibles) une fois par jour. La sécurisation doit absolument être vérifiée après chaque redémarrage du système, en plus des autres routines d'audits.

Vérifiez tous les composants essentiels afin de maintenir la sécurité des systèmes déployés. Si la sécurité *n'est pas* vérifiée périodiquement, les configurations dérivent souvent avec le temps par entropie ou suite à des modifications apportées par inadvertance ou par malveillance. Sans contrôles périodiques, ces changements ne sont pas détectés et aucune mesure corrective ne peut être prise. Le résultat en est un système de moins en moins sûr et de plus en plus vulnérable.

Outre les audits périodiques, effectuez des vérifications après les mises à niveau, les installations de patchs et chaque fois que des changements significatifs sont apportés à la configuration du système.

Contrôle de la sécurité avant la sécurisation

Dans certains cas, il peut s'avérer utile de vérifier la sécurité de systèmes déployés *avant* leur sécurisation. Par exemple, si vous êtes responsable de systèmes déployés administrés par une autre personne, inspectez l'état de ces systèmes afin de connaître leur niveau de sécurité et, le cas échéant, de les mettre en conformité avec les profils de sécurité utilisés sur vos systèmes.

Personnalisation des audits de sécurité

L'option d'audit est un mécanisme extrêmement flexible et extensible pour l'évaluation de l'état d'un système. Comme pour les scripts de sécurisation, vous pouvez personnaliser les actions des scripts audit. Par exemple, vous pouvez personnaliser les variables d'environnement, la structure et les fonctions auxiliaires, et ajouter des fonctionnalités à la structure d'audit.

Pour la plupart des utilisateurs, les scripts d'audit standard et les scripts spécifiques au produit peuvent être utilisés comme modèles afin de personnaliser l'audit en fonction de l'environnement. Dans ce cas, utilisez les pilotes, les scripts finish, les variables d'environnement et les modèles de fichiers pour personnaliser les scripts d'audit. Les modifications de personnalisation peuvent être effectuées avec un minimum d'effort, sans modification du code. Quelles que soient les modifications introduites pour la sécurisation, le logiciel Solaris Security Toolkit les détecte automatiquement quand vous effectuez l'audit.

Certains utilisateurs doivent créer des pilotes et des scripts propriétaires ou spécifiques au site entièrement nouveaux. Utilisez les modèles et les échantillons pour vous guider lors du codage de nouveaux pilotes et scripts. Veuillez noter que les pilotes spécifiques au site, les scripts finish, les variables et les fonctions *ne sont pas* reconnus automatiquement par le logiciel Solaris Security Toolkit quand vous utilisez l'option d'audit. Par exemple, si vous ajoutez un pilote spécifique au site nommé `abcc-nj-secure.driver` contenant un script finish `abcc-nj-install-foo.fin`, il peut être nécessaire de créer un script d'audit spécifique au site `abcc-nj-install-foo.aud`. De même, si vous commencez par le script d'audit *uniquement*, vous devez créer le script finish correspondant.

Parfois, certains utilisateurs veulent ajouter des contrôles ou des fonctionnalités qui *ne sont pas* prévus par le logiciel Solaris Security Toolkit. Il faut alors ajouter les contrôles ou les nouvelles fonctionnalités dans le script audit. (Vous pouvez aussi introduire les modifications dans le script finish correspondant). Si vous ajoutez ou modifiez le code du fichier à l'aide du `user.run`, agissez avec une extrême précaution afin de ne pas introduire de bogues ou de failles.

Pour personnaliser ou créer de nouveaux pilotes, scripts, variables et fonctions, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Vous pouvez avoir besoin, par exemple, d'ajouter un patch que le logiciel Solaris Security Toolkit *n'installe pas*. Vous avez la possibilité d'utiliser l'un des modèles standard ou spécifiques au produit, ou bien d'en créer un. Si vous créez vos propres modèles, créez un script finish pour ajouter le patch, puis le script audit correspondant pour vérifier l'installation du patch. Si vous utilisez des scripts finish (`.fin`) et audit (`.aud`) existants comme modèles vous devez copier ces deux scripts vers de nouveaux fichiers uniques.

Préparation d'un audit de sécurité

Pour utiliser les instructions contenues dans ce chapitre, vous devez disposer d'un profil de sécurité. Pour de plus amples informations sur le développement et la mise en oeuvre d'un profil de sécurité, reportez-vous au chapitre 2.

De nombreux profils de sécurité sont inclus sous forme de pilotes dans le logiciel Solaris Security Toolkit. Comme mentionné précédemment dans cet ouvrage, les profils de sécurité par défaut et les modifications apportées par ceux-ci peuvent ne pas convenir à vos systèmes. En général, les profils de sécurité mis en oeuvre représentent des limites supérieures de sécurité. Par là, nous entendons des limites qui désactivent les services inutiles et activent les fonctions de sécurité facultatives désactivées par `secure.driver`.

Les profils de sécurité standard et spécifiques au produit conviennent aux environnements de nombreux utilisateurs du logiciel Solaris Security Toolkit. Si tel est votre cas, vous devez déterminer le profil de sécurité qui reflète le mieux le type de sécurité voulu, puis utiliser ce profil pour l'évaluation et la sécurisation de vos systèmes.

Vérifiez et personnalisez les modèles de profils de sécurité en fonction de votre environnement, ou développez-en de nouveaux. Pour obtenir des techniques et des directives sur la personnalisation des profils de sécurité, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*. Cette approche permet de sécuriser votre système selon les besoins de votre organisation et de minimiser le nombre de fausses erreurs renvoyées lors d'une évaluation de la sécurité. Par exemple, si vous savez que Telnet doit être activé, vous pouvez personnaliser le profil de sécurité de manière à ce que le logiciel *ne considère pas* Telnet comme une vulnérabilité lors de l'évaluation de la sécurité. Ainsi, un site utilisant Telnet avec Kerberos pour l'authentification et le chiffrement ne considère pas l'utilisation de Telnet comme une vulnérabilité.

Utilisation d'options et contrôle de la sortie des audits

Cette section décrit les options disponibles pour l'exécution d'un audit et les options de contrôle de la sortie. Ce chapitre contient les sections suivantes :

Options de ligne de commande

Le synopsis de la ligne de commande suivant décrit l'audit d'un système par rapport à un profil de sécurité :

```
# jass-execute -a pilote [ -V [0-4]] [ -q | -o fichier_sortie ] [ -m adresse_e-mail ]
```

Pendant l'exécution de la commande d'audit du logiciel Solaris Security Toolkit, vous pouvez utiliser les options indiquées dans le TABLEAU 6-1.

TABLEAU 6-1 Utilisation des options de ligne de commande avec la commande d'audit

Option	Description
`-a` *pilote*	Détermine si un système est conforme au profil de sécurité.
`-m` *adresse_e-mail*	Indique une adresse e-mail pour le support interne.
`-o` *fichier_sortie*	Indique un nom de fichier pour la sortie de l'exécution de Solaris Security Toolkit.
`-q`	Spécifie le mode silencieux. Les messages ne s'affichent pas pendant l'exécution de cette commande. La sortie est stockée dans `JASS_REPOSITORY/`.
`-V` *niveau_verbosité*	Spécifie le niveau de verbosité (`0` à `4`) de l'audit.

Pour de plus amples informations sur les options disponibles avec la commande `jass-execute -a`, reportez-vous aux sections suivantes :

- « Option d'affichage de l'aide » à la page 95
- « Option de notification par e-mail » à la page 96
- « Option de sortie de fichier » à la page 97
- « Option de sortie silencieuse » à la page 97
- « Option de verbosité » à la page 98

Option d'affichage de l'aide

L'option `-h` affiche le message d'aide de la commande `jass-execute`, qui présente les options disponibles.

L'option -h produit une sortie du type suivant :

EXEMPLE DE CODE 6-1 Échantillon de sortie de l'option -h

```
# ./jass-execute -h

Pour appliquer ce kit d'outils à un système, en utilisant la
syntaxe suivante :
  jass-execute [-r répertoire_racine -p version_es ]
  [ -q | -o fichier_sortie ] [ -m adresse_e-mail ]
  [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente du kit d'outils à partir
d'un système :
  jass-execute -u [ -b | -f | -k ] [ -q | -o fichier_sortie ]
     [ -m adresse_e-mail ] [ -V [3|4] ]

Pour l'audit d'un système en fonction d'un profil prédéfini :
  jass-execute -a driver [ -V [0-4] ] [ -q | -o fichier_sortie ]
     [ -m adresse_e-mail ]

Pour afficher l'historique des applications du kit d'outils sur un
système :
  jass-execute -H

Pour afficher la dernière application du kit d'outils sur un
système :
  jass-execute -l

Pour afficher ce message d'aide :
  jass-execute -h
  jass-execute -?

Pour afficher les informations sur la version de ce programme :
  jass-execute -v
```

Option de notification par e-mail

L'option -m *adresse_email* est un mécanisme qui permet au logiciel Solaris Security Toolkit d'envoyer automatiquement la sortie par e-mail une fois l'exécution terminée. Le rapport électronique est généré en plus des journaux éventuellement créés sur le système à l'aide d'autres options.

Échantillon d'exécution de Solaris Security Toolkit appelant sunfire_15k_sc-config.driver à l'aide de l'option de notification par e-mail :

```
# ./jass-execute -m root -a sunfire_15k_sc-config.driver
[...]
```

Option de sortie de fichier

L'option `-o` *fichier-sortie* redirige la sortie de la console de la commande `jass-execute` vers un fichier distinct, *fichier-sortie*.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Cette option est particulièrement pratique si elle est utilisée avec une connexion de terminal bas débit, car Solaris Security Toolkit génère un volume significatif de sortie.

Cette option peut être utilisée avec les options `-d`, `-u` ou `-a`.

L'option `-o` produit une sortie du type suivant :

EXEMPLE DE CODE 6-2 Échantillon de sortie de l'option `-o`

```
# ./jass-execute -o jass-output.txt -a secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
#
```

Option de sortie silencieuse

L'option `-q` désactive la sortie de Solaris Security Toolkit vers le flux d'entrée/sortie standard (`stdio`) pendant une sécurisation.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Comme pour l'option `-o`, cette option est particulièrement utile quand Solaris Security Toolkit est exécuté via une tâche `cron` ou avec une connexion réseau bas débit.

Cette option peut être utilisée avec les options `-d`, `-u` ou `-a`.

L'option `-q` produit une sortie du type suivant :

EXEMPLE DE CODE 6-3 Échantillon de sortie de l'option `-q`

```
# ./jass-execute -q -a secure.driver
[NOTE] Executing driver, secure.driver
```

Option de verbosité

L'option `-V` spécifie le niveau de verbosité d'un audit. Cette option est disponible *uniquement* pour les audits. Les niveaux de verbosité offrent une haute flexibilité d'affichage des résultats d'audit. Par exemple, si vous avez 100 ordinateurs à contrôler, il peut être plus pratique de limiter la sortie à une seule ligne par ordinateur afin de déterminer ceux qui ont réussi l'audit et ceux qui ont échoué. Ensuite, vous pouvez lancer un audit uniquement sur les ordinateurs ayant échoué et générer ainsi des informations plus complètes en sortie afin de mieux cerner le problème.

Les cinq niveaux de verbosité (0 à 4) sont contrôlés par l'option `-V`. Chaque niveau incrémentiel fournit des détails supplémentaires permettant de mieux comprendre les contrôles qui ont réussi et ceux qui ont échoué. Le TABLEAU 6-2 décrit les niveaux de verbosité.

TABLEAU 6-2 Niveaux de verbosité d'un audit

Niveau	Sortie
0	Affiche une ligne unique indiquant la réussite ou l'échec.
1	Affiche, pour chaque script, une ligne unique indiquant la réussite ou l'échec, puis une ligne de score total sous toutes les lignes de script.
2	Affiche, pour chaque script, les résultats de tous les contrôles.
3	Affiche plusieurs lignes avec une sortie complète, y compris les messages de bannière et d'en-tête. Ce niveau est la valeur par défaut.
4	Affiche plusieurs lignes (toutes les données à partir du niveau 3), ainsi que toutes les entrées qui sont générées par la fonction de consignation `logDebug`. Ce niveau s'utilise pour le débogage.

Remarque – Le niveau de verbosité par défaut pour la commande `jass-execute -V` est 3.

Pour une description complète des niveaux de verbosité, reportez-vous à la page man `jass-execute` ou à la section `JASS_VERBOSITY` du chapitre 7 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Sortie de bannières et de messages

Vous pouvez configurer l'option d'audit de Solaris Security Toolkit de sorte qu'elle signale ou omette les bannières et les messages. La variable JASS_LOG_BANNER *ne peut pas* être utilisée avec les niveaux de verbosité 0 à 2. Ces options de sortie s'appliquent aux niveaux 3 et 4. Par exemple, vous pouvez éliminer les messages de réussite (variable JASS_LOG_SUCCESS) de la sortie afin de signaler et de vous concentrer *uniquement* sur les messages d'échec (variable JASS_LOG_FAILURE).

Le TABLEAU 6-3 contient la liste des bannières et des messages que vous pouvez contrôler par l'intermédiaire des variables de consignation. (Pour de plus amples informations sur les variables de consignation, reportez-vous à la section JASS_LOG_BANNER du chapitre 7 du manuel *Solaris Security Toolkit 4.2 Reference Manual*). Pour de plus amples informations sur les niveaux de verbosité, reportez-vous à la page man `jass-execute` ou à la section JASS_VERBOSITY du chapitre 7 du manuel *Solaris Security Toolkit 4.2 Reference Manual*. Si la variable de consignation est définie sur `0`, aucune sortie n'est générée pour les messages de ce type. En revanche, si la variable de consignation est définie sur `1`, les messages sont affichés. Par défaut, ces variables sont définies de manière à afficher les messages. Le TABLEAU 6-3 décrit les variables de consignation.

TABLEAU 6-3 Affichage des bannières et des messages dans la sortie d'un audit

Variable de consignation	Préfixe de journal	Description
JASS_LOG_BANNER	Sortie de toutes les bannières	Ce paramètre contrôle l'affichage des messages de bannières. Ces messages sont généralement entourés de séparateurs contenant un signe égale (=) ou un tiret (-).
JASS_LOG_ERROR	[ERR]	Ce paramètre contrôle l'affichage des messages d'erreur. S'il est réglé sur 0, aucun message d'erreur n'est généré.
JASS_LOG_FAILURE	[FAIL]	Ce paramètre contrôle l'affichage des messages d'échec. S'il est réglé sur 0, aucun message d'échec n'est généré.
JASS_LOG_NOTICE	[NOTE]	Ce paramètre contrôle l'affichage des messages d'avis. S'il est réglé sur 0, aucun message d'avis n'est généré.
JASS_LOG_SUCCESS	[PASS]	Ce paramètre contrôle l'affichage des messages de réussite. S'il est réglé sur 0, aucun message de réussite n'est généré.
JASS_LOG_SUMMARY	[SUMMARY]	Ce paramètre contrôle l'affichage des messages de résumé. S'il est réglé sur 0, aucun message de résumé n'est généré.
JASS_LOG_WARNING	[WARN]	Ce paramètre contrôle l'affichage des messages d'avertissement. S'il est réglé sur 0, aucun message d'avertissement n'est généré.

L'utilisation de ces options s'avère très pratique lorsque vous souhaitez afficher *uniquement* des messages spécifiques. En définissant ces options, vous pouvez minimiser les messages en sortie et vous concentrer sur les messages essentiels. Par exemple, en définissant toutes les variables de consignation sur `0` à l'exception de `JASS_LOG_FAILURE` (définie sur la valeur par défaut `1`), *seuls* les rapports d'audit concernant des échecs sont générés par la fonction `logFailure`.

EXEMPLE DE CODE 6-4 Échantillon de sortie d'un rapport d'audit contenant uniquement les échecs

```
# JASS_LOG_FAILURE=1
# export JASS_LOG_FAILURE
# JASS_LOG_BANNER=0
# JASS_LOG_ERROR=0
# JASS_LOG_NOTICE=0
# JASS_LOG_SUCCESS=0
# JASS_LOG_SUMMARY=0
# JASS_LOG_WARNING=0
# export JASS_LOG_BANNER JASS_LOG_ERROR
# export JASS_LOG_NOTICE JASS_LOG_SUCCESS
# export JASS_LOG_WARNING
# bin/jass-execute -a abc.driver -V2
update-at-deny     [FAIL] User adm is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User zz999999 is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User gdm is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User lp is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User nobody4 is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User root is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User smmsp is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User sys is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User uucp is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] User webservd is not listed in /etc/cron.d/at.deny.
update-at-deny     [FAIL] Script Total: 10 Errors
update-inetd-conf  [FAIL] Service svc:/network/telnet:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/ftp:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/finger:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/login:rlogin was enabled.
update-inetd-conf  [FAIL] Service svc:/network/shell:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/login:eklogin was enabled.
update-inetd-conf  [FAIL] Service svc:/network/login:klogin was enabled.
update-inetd-conf  [FAIL] Service svc:/network/shell:kshell was enabled.
update-inetd-conf  [FAIL] Service svc:/application/font/stfsloader:default was
enabled.
update-inetd-conf  [FAIL] Service svc:/network/security/ktkt_warn:default was
enabled.
update-inetd-conf  [FAIL] Service svc:/network/rpc/smserver:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/rpc/rstat:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/rpc/rusers:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/nfs/rquota:default was enabled.
update-inetd-conf  [FAIL] Service svc:/network/rpc/gss:default was enabled.
```

EXEMPLE DE CODE 6-4 Échantillon de sortie d'un rapport d'audit contenant uniquement les échecs *(suite)*

```
update-inetd-conf  [FAIL] Service 100235 is enabled in /etc/inet/inetd.conf.
update-inetd-conf  [FAIL] Service 100083 is enabled in /etc/inet/inetd.conf.
update-inetd-conf  [FAIL] Service 100068 is enabled in /etc/inet/inetd.conf.
update-inetd-conf  [FAIL] Script Total: 18 Errors
abc.driver         [FAIL] Driver Total: 28 Errors
abc.driver         [FAIL] Grand Total: 28 Errors
#
```

Sortie de nom d'hôte, de nom de script et d'horodatage

Vous pouvez configurer l'option d'audit de Solaris Security Toolkit de manière à inclure le nom d'hôte, le nom de script et les informations d'horodatage pour les niveaux de verbosité `0` à `2`. Par exemple, si vous avez un nombre élevé d'ordinateurs à contrôler, vous pouvez trier la sortie par nom d'hôte, nom de script ou horodatage. Le TABLEAU 6-4 contient la liste des variables.

TABLEAU 6-4 Affichage du nom d'hôte, du nom de script et de l'horodatage

Nom de la variable	Description de la variable
`JASS_DISPLAY_HOSTNAME`	Lorsque ce paramètre est défini sur 1, le logiciel Solaris Security Toolkit ajoute à chaque entrée de journal le nom d'hôte du système. Cette information se base sur le paramètre `JASS_HOSTNAME`. Par défaut, ce paramètre est vide et le kit d'outils *n'affiche* pas cette information.
`JASS_DISPLAY_SCRIPTNAME`	Par défaut, ce paramètre est défini sur 1 et le logiciel Solaris Security Toolkit ajoute à chaque entrée de journal le nom d'hôte du script d'audit en cours d'exécution. Définissez ce paramètre sur une autre valeur pour que le kit d'outils *n'affiche pas* cette information.
`JASS_DISPLAY_TIMESTAMP`	Lorsque ce paramètre est défini sur 1, le logiciel Solaris Security Toolkit ajoute à chaque entrée de journal l'horodatage associé à l'audit. Cette information se base sur le paramètre `JASS_TIMESTAMP`. Par défaut, ce paramètre est vide et le logiciel *n'affiche pas* cette information.

En configurant le logiciel Solaris Security Toolkit de sorte qu'il ajoute le nom d'hôte, le nom de script et l'horodatage, vous pouvez combiner de nombreux audits d'un seul système ou d'un groupe de systèmes, et les trier ensuite en fonction de ces données clé. Vous avez la possibilité d'utiliser ces informations pour rechercher les problèmes touchant plusieurs systèmes ou symptomatiques de processus de déploiement. Par exemple, en utilisant les informations de cette manière, un administrateur peut savoir si tous les systèmes construits suivant un procédé donné présentent *toujours* les mêmes échecs.

Par exemple, en définissant le paramètre JASS_DISPLAY_TIMESTAMP sur 1 et le paramètre JASS_DISPLAY_SCRIPTNAME sur 0, vous obtenez une sortie du type suivant.

EXEMPLE DE CODE 6-5 Échantillon de sortie de journal d'audit

```
# JASS_DISPLAY_TIMESTAMP=1
# JASS_DISPLAY_SCRIPTNAME=0
# export JASS_DISPLAY_TIMESTAMP JASS_DISPLAY_SCRIPTNAME
# bin/jass-execute -a abc.driver -V2
20050716132908 [FAIL] User adm is not listed in /etc/cron.d/at.deny.
20050716132908 [PASS] User bin is listed in /etc/cron.d/at.deny.
20050716132908 [FAIL] User zz999999 is not listed in /etc/cron.d/at.deny.
...
...
...
20050716132908 [FAIL] Script Total: 18 Errors
20050716132908 [FAIL] Driver Total: 28 Errors
20050716132908 [FAIL] Grand Total: 28 Errors
20050716132908 [SUMMARY] Results Summary for AUDIT run of dan.driver
20050716132908 [SUMMARY] The run completed with a total of 2 scripts run.
20050716132908 [SUMMARY] There were  Failures in   2 Scripts
20050716132908 [SUMMARY] There were  Errors   in   0 Scripts
20050716132908 [SUMMARY] There were  Warnings in   0 Scripts
20050716132908 [SUMMARY] There was a Note     in   1 Script
20050716132908 [SUMMARY] Failure Scripts listed in:
/var/opt/SUNWjass/run/20050716132908/jass-script-failures.txt
20050716132908 [SUMMARY] Notes Scripts listed in:
/var/opt/SUNWjass/run/20050716132908/jass-script-notes.txt
#
```

Exécution d'un audit de sécurité

L'évaluation périodique de la sécurité des systèmes fournit une référence qui permet de déterminer le niveau de conformité de la sécurité par rapport au profil de sécurité mis en oeuvre. Le plus souvent, l'évaluation de la sécurité est similaire à une tâche de maintenance exécutée un certain temps après la sécurisation de nouvelles installations. L'option d'évaluation de la sécurité est conçue pour que vous puissiez exécuter les mêmes pilotes de sécurisation que ceux employés lors de la sécurisation du système. Toutefois, vous utilisez à présent l'option -a pour contrôler l'état actuel par rapport au profil de sécurité mis en oeuvre pendant la sécurisation. Cette solution élimine la complexité tout en offrant un grande flexibilité. Par exemple, quand vous mettez à jour le profil de sécurité, les évaluations de sécurité suivantes utilisent le profil de sécurité actualisé.

Dans un autre exemple, vous pourriez être responsable de la sécurisation de systèmes qui sont déjà déployés. Avant de passer à leur sécurisation, effectuez une évaluation de la sécurité. Vous définissez dans ce cas le profil de sécurité, personnalisez un modèle de profil de sécurité Solaris Security Toolkit ou utilisez l'un des modèles de profils de sécurité tel quel.

▼ Pour exécuter un audit de sécurité

Avant d'effectuer un audit, vous devez définir ou choisir un profil de sécurité. Pour de plus amples informations, reportez-vous à la section « Préparation d'un audit de sécurité » à la page 94.

Attention – Si vous effectuez une évaluation de la sécurité sur un système déployé que vous *n'avez pas* encore sécurisé, sauvegardez d'abord l'ordinateur et redémarrez-le pour vérifier que sa configuration est connue et cohérente, et qu'elle fonctionne. Les erreurs ou les avertissements détectés lors du redémarrage préliminaire doivent être corrigés ou notés avant de passer à l'évaluation de la sécurité du système.

1. **Choisissez le profil de sécurité (pilote de sécurisation) que vous voulez utiliser :**
   - Si vous avez précédemment sécurisé le système, utilisez le même profil de sécurité.

     Par exemple, `secure.driver`.
   - Si vous *n'avez pas* encore sécurisé le système, utilisez l'un des profils de sécurité standard ou votre propre profil.

     Par exemple, `secure.driver` ou `abccorp-secure.driver`.

   Pour obtenir une liste et des informations complètes et mises à jour sur les pilotes standard et spécifiques au produit disponibles, reportez-vous à la page man `security_drivers` ou au chapitre 4 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

2. **Déterminez les options de ligne de commande que vous voulez utiliser et la méthode de contrôle de la sortie.**

   Voir « Utilisation d'options et contrôle de la sortie des audits » à la page 94.

3. **Entrez la commande** `jass-execute -a`**, le nom du profil de sécurité et les options voulues.**

   L'échantillon ci-après décrit un audit utilisant `abc-secure.driver`.

EXEMPLE DE CODE 6-6 Échantillon de sortie d'un audit

```
# ./jass-execute -a abc-secure.driver
[NOTE] Executing driver, abc-secure.driver

[...]

================================================================
abc-secure.driver: Audit script: enable-rfc1948.aud
================================================================

#----------------------------------------------------------------
# RFC 1948 Sequence Number Generation
#
# Rationale for Verification Check:
#
# L'objectif de ce script est de vérifier que le système
# est configuré et qu'il utilise RFC 1948 pour son algorithme de
génération de numéros de séquence TCP
# (ID par connexion unique). Pour cela,
# le paramètre 'TCP_STRONG_ISS' doit être défini sur '2' dans le
fichier
# the /etc/default/inetinit.
#
# Détermination de la conformité :
#
[...]
#----------------------------------------------------------------

[PASS] TCP_STRONG_ISS is set to '2' in /etc/default/inetinit.
[PASS] System is running with tcp_strong_iss=2.

# Score total de vulnérabilité de ce script audit

[PASS] Audit Check Total : 0 Error(s)

================================================================

# Score total de vulnérabilité de ce profil de pilote

[PASS] Driver Total : 0 Error(s)

================================================================
abc-secure.driver: Driver finished.
```

EXEMPLE DE CODE 6-6 Échantillon de sortie d'un audit *(suite)*

```
================================================================

# Score total global de vulnérabilité de cette exécution

[PASS] Grand Total : 0 Error(s)
```

Après le démarrage d'un audit, le logiciel Solaris Security Toolkit a accès aux fichiers du répertoire `JASS_HOME_DIR/Audit`. Bien que les fichiers contenus dans les répertoires `JASS_HOME_DIR/Audit` et `JASS_HOME_DIR/Finish` partagent les mêmes noms de fichiers de base, ils n'ont pas les mêmes suffixes. Le script `driver.run` convertit automatiquement les scripts finish définis par la variable `JASS_SCRIPTS` en scripts audit, en changeant leurs suffixes `.fin` en `.aud`. Il indique également les fichiers contenant tous les messages générés à chaque niveau d'avertissement pendant l'exécution.

L'audit démarre et initialise l'état du logiciel Solaris Security Toolkit. Chaque pilote auquel le système accède pendant l'audit évalue l'état de l'ensemble de ses modèles de fichiers et scripts d'audit. Le résultat de chaque contrôle est une réussite ou un échec, ce qui est représenté par une valeur de vulnérabilité respectivement égale à zéro ou différente de zéro. Dans la plupart des cas, l'échec est représenté par le numéro 1. Chaque script exécuté produit un score total de sécurité basé sur la valeur totale de vulnérabilité de chaque contrôle contenu à l'intérieur d'un script. La valeur totale de vulnérabilité pour chaque pilote est affichée une fois l'évaluation du pilote terminée. Un total global de tous les scores est présenté à la fin de l'audit.

L'option d'évaluation de la sécurité permet d'avoir une vue complète de l'état d'un système au moment où l'évaluation commence. Le logiciel Solaris Security Toolkit contrôle l'état stocké du système en inspectant les fichiers de configuration et l'état de fonctionnement du système en inspectant les informations de la table de processus, le pilote de périphérique, etc. Le logiciel Solaris Security Toolkit vérifie l'existence de chaque fichier ou service, et s'assure que le logiciel associé à un service est installé, configuré, activé et en cours d'exécution. Cette méthode fournit un instantané précis de l'état actuel d'un système.

CHAPITRE 7

Sécurisation d'un système

Ce chapitre décrit l'application des informations contenues dans les chapitres précédents à un exemple réaliste d'installation et de sécurisation d'un nouveau SE Solaris 8 ou 9. Ce chapitre explique comment déployer le logiciel Solaris Security Toolkit avec un pare-feu Check PointFirewall-1 NG pour le SE Solaris 8.

Utilisez les informations contenues dans ce chapitre comme instructions et exemple pour la sécurisation d'un nouveau système et d'applications.

Les ouvrages et les articles Sun BluePrint accessibles en ligne peuvent vous guider au cours du processus de minimisation et de sécurisation de nombreux systèmes Sun. Consultez le site Web suivant pour obtenir les articles et les ouvrages spécifiques à un produit :

`http://www.sun.com/blueprints`

Ce chapitre contient les sections suivantes :

Planification et préparation

Pour déployer efficacement des systèmes minimisés et sécurisés, comme l'indique cette étude de cas, la planification et la préparation sont deux facteurs fondamentaux. L'infrastructure de réseau sous-jacente, les stratégies et les procédures doivent être en place. De plus, le support et la maintenance des systèmes doivent être définis et

communiqués. Pour de plus amples informations sur la planification et la préparation, reportez-vous au chapitre 2. L'exemple décrit dans ce chapitre documente les processus et les tâches qu'un administrateur système doit effectuer afin d'obtenir une image du SE Solaris minimisée et sécurisée pour un système à pare-feu.

Dans cet exemple, l'administrateur système doit créer une solution automatisée et évolutive en vue de la construction et le déploiement de systèmes Check PointFirewall-1 NG pour un fournisseur de services qui souhaite offrir un service pare-feu à ses clients. Dans ce cas, les exigences et les considérations du fournisseur de services sont les suivantes :

- Étant donné que le fournisseur de services a prévu de déployer un nombre important de ces systèmes, le temps employé à la construction et au déploiement de chacun de ces systèmes est un facteur essentiel qui doit être optimisé.
- Les systèmes sont installés en utilisant un réseau d'administration dédié connecté à l'interface Ethernet interne de chaque système. Ce réseau est utilisé *uniquement* par le personnel du fournisseur de services et *non* par les abonnés.
- Toutes les autres interfaces sont sur des interfaces réseau physiques séparées et sont filtrées.
- La sécurité du réseau d'administration est vitale pour la sécurité générale des systèmes à pare-feu déployés.

En fonction de ces facteurs, l'administrateur système décide d'automatiser l'installation, la minimisation et la sécurisation des images de SE en utilisant la technologie JumpStart et le logiciel Solaris Security Toolkit.

Suppositions et restrictions

Ce chapitre suppose l'utilisation d'un logiciel Solaris Security Toolkit déjà fonctionnel et d'une installation en technologie JumpStart. Le chapitre 3 fournit des instructions et des directives pour l'installation du logiciel.

Ce chapitre suppose également le développement d'une configuration personnalisée pour la minimisation et la sécurisation d'une application spécifique. Le logiciel Solaris Security Toolkit *ne possède pas* de pilotes ou de profils JumpStart spécifiques à l'application. Par conséquent, il vous faut créer des pilotes et des profils personnalisés pour cette application. Cette tâche consiste à copier des pilotes et des profils existants, et à les modifier en fonction de l'application.

Dans cet exemple, l'administrateur système doit disposer du niveau de compétence suivant :

- Il doit disposer de connaissances et d'une expérience suffisantes pour configurer le système d'exploitation et les applications.
- Il doit savoir tester et affiner la configuration.

- Il possède les connaissances nécessaires à la construction d'un environnement JumpStart à partir duquel le système client est installé. Reportez-vous à l'ouvrage Sun BluePrint *JumpStart Technology : Effective Use in the Solaris Operating Environment*.
- Il maîtrise les techniques de minimisation du système d'exploitation. Reportez-vous à l'ouvrage *Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*.
- Il maîtrise les principes de base du logiciel Solaris Security Toolkit et est prêt à construire une configuration personnalisée à l'aide des techniques et directives de minimisation et de sécurisation. Voir le chapitre 1.

Environnement du système

L'exemple est basé sur l'environnement matériel et logiciel suivant :

- Check PointFirewall-1 NG
- SE Solaris 8
- Technologie JumpStart
- Cluster du SE Solaris(`SUNWCreq`)
- Logiciel Solaris Security Toolkit
- Plate-forme reposant sur la technologie SPARC
- Au moins deux interfaces Ethernet

Conditions de sécurité requises

Dans cet exemple, les conditions requises de haut niveau et les packages ont été identifiés, mais les composants et les services spécifiques à tous les packages doivent être définis. Il faut également identifier les capacités du SE Solaris nécessaires pour administrer et gérer les systèmes.

La liste suivante précise l'utilisation des composants logiciels :

- Secure Shell pour l'administration à distance
- Client FTP pour le téléchargement de fichiers à distance
- Commandes `scp` et `sftp` pour la copie des fichiers

Vous pouvez développer un profil de sécurité à partir de cette liste. Pour de plus amples informations sur le développement de profils de sécurité et l'utilisation de modèles de profils, reportez-vous à la section « Développement et mise en oeuvre d'un profil Solaris Security Toolkit » à la page 30.

Création d'un profil de sécurité

Un profil de sécurité définit les modifications introduites par le logiciel Solaris Security Toolkit lors de la sécurisation et de la minimisation de la configuration de sécurité d'un système. Aucun des profils de sécurité ou des pilotes standard inclus dans le logiciel Solaris Security Toolkit ne remplit les conditions requises par les systèmes Check PointFirewall-1 NG minimisés. Par conséquent, vous devez créer un profil de sécurité personnalisé pour mettre en oeuvre les modifications appropriées du système.

La méthode de création d'un profil de sécurité pour cet exemple est décrite en diverses sections de ce chapitre. D'abord, vous devez créer de nouveaux fichiers de pilotes à partir des pilotes existants. Ensuite, vous modifiez les nouveaux pilotes afin de les rendre conforme aux conditions de sécurité précédemment précisées. La minimisation est décrite à la section « Installation du logiciel » à la page 110 et les modifications de sécurisation à la section « Personnalisation de la configuration de sécurisation » à la page 118.

Installation du logiciel

Cette section décrit le processus d'installation du logiciel. La description est effectuée en tenant compte de toutes les exceptions et instructions spécifiques à cet exemple. Pour obtenir des instructions générales sur l'installation du logiciel, reportez-vous au chapitre 3.

Remarque – Vous pouvez utiliser les instructions suivantes comme modèle pour la gestion des situations correspondantes.

Cette section décrit les tâches suivantes :

Téléchargement et installation du logiciel de sécurité

Téléchargez et installez Solaris Security Toolkit et les composants logiciels de sécurité supplémentaires, y compris les patchs, sur le serveur JumpStart en procédant comme suit.

▼ Pour télécharger et installer le logiciel de sécurité

1. **Téléchargez le logiciel Solaris Security Toolkit et les composants de sécurité additionnels.**

   Voir « Téléchargement du logiciel de sécurité » à la page 42.

2. **Installez le logiciel Solaris Security Toolkit et les composants de sécurité additionnels.**

   Voir « Installation et exécution du logiciel » à la page 50.

Attention – *N'exécutez pas* encore le logiciel Solaris Security Toolkit. Effectuez d'abord la configuration et la personnalisation additionnelles décrites dans les sections suivantes.

Installation de patchs

Les patchs du système d'exploitation peuvent corriger des vulnérabilités, des problèmes de disponibilité, des défauts au niveau des performances ou d'autres aspects d'un système. Quand vous installez un nouveau système d'exploitation, vérifiez que les patchs requis sont installés, puis effectuez cette vérification régulièrement.

Le logiciel Solaris Security Toolkit fournit un mécanisme d'installation du cluster de patchs de sécurité et recommandés disponible sur le site de SunSolve Online. Ce cluster de patchs spécifiques au système d'exploitation contient les patchs les plus fréquemment nécessaires.

▼ Pour installer les patchs

1. **Vous devez au minimum télécharger le cluster de patchs recommandés et de sécurité dans le répertoire**`Patches` **et le décompresser.**

   Si le script `install-recommended-patches.fin` est inclus dans le pilote de sécurisation, ce cluster de patchs est installé automatiquement.

   Il existe une problème supplémentaire concernant Check PointFirewall-1 NG. Cette application requiert des patchs spécifiques qui *ne sont pas* inclus dans le cluster des patchs de sécurité et recommandés. Check PointFirewall-1 NG nécessite les patchs suivants :

   - 108434
   - 108435

2. **Pour automatiser l'installation des patchs 108434 et 108435, téléchargez les dernières versions des patchs à partir du site de SunSolve OnLine et placez-les dans le répertoire** `Patches`**.**

3. **Créez un nouveau script finish (par exemple,** `fw1-patch-install.fin`**) qui appelle la fonction auxiliaire** `add_patch`**, avec le nom de chaque patch.**

   Ce script finish appelle les fonctions auxiliaires correctes avec les deux ID de patchs requis pour Check PointFirewall-1 NG. Par exemple :

```
# !/bin/sh

# add_patch 108434-10

# add_patch 108435-10
```

Spécification et installation du cluster du système d'exploitation

Une fois l'organisation des disques pour l'installation du système d'exploitation définie, la première tâche consiste à spécifier le cluster du SE Solaris à installer. Choisissez l'un des cinq clusters d'installation fournis avec le SE Solaris : `SUNWCreq`, `SUNWCuser`, `SUNWCprog`, `SUNWCall` et `SUNWCXall`.

▼ Pour spécifier et installer le cluster du système d'exploitation

1. **Spécifiez le cluster du système d'exploitation à installer.**

   L'objectif de cet exemple étant de construire un pare-feu minimisé et dédié, utilisez le plus petit des clusters du SE Solaris disponibles, `SUNWCreq`, également connu sous le nom de `Core`.

   Ce cluster contenant un nombre relativement faible de packages, d'autres packages seront probablement requis. Ces autres packages *doivent* être inclus dans le profil avec la définition du cluster du SE Solaris.

   La définition du profil de la ligne de base ajoute ce qui suit au profil précédemment défini.

   ```
   cluster          SUNWCreq
   ```

   Le cluster d'installation `SUNWCreq` comprend des packages qui *ne sont pas* nécessaires au bon fonctionnement d'un serveur pare-feu Sun. Supprimez ces packages inutiles après avoir défini une ligne de base de travail. Reportez-vous à l'article Sun BluePrints en ligne « Minimizing the Solaris Operating Environment for Security: Updated for the Solaris 9 Operating Environment ».

2. **Effectuez une installation avec le profil de sécurité défini pour déterminer la présence éventuelle de problèmes de dépendance au niveau des packages.**

   Certaines dépendances de packages surviennent pendant l'installation. Check PointFirewall-1 NG requiert les packages du SE Solaris suivants :

   - `SUNWter` – Informations sur le terminal
   - `SUNWadmc` – Bibliothèques de noyaux d'administration du système
   - `SUNWadmfw` – Structure d'administration du système et du réseau
   - `SUNWlibC` et `SUNWlibCx` – Requis pour l'application Check PointNG

   La liste complète des packages du profil est la suivante :.

   ```
   cluster          SUNWCreq
   package          SUNWter          add
   package          SUNWlibC         add
   package          SUNWlibCx        add
   package          SUNWlibC         add
   package          SUNWlibC         add
   ```

Remarque – Bien que cette liste soit complète pour l'exemple actuel, d'autres packages peuvent être ajoutés ou supprimés en fonction de l'environnement de déploiement de cette configuration.

Des modifications peuvent encore être apportées à liste finale des packages tant que le fonctionnement et la sécurité du système n'ont pas été vérifiés (voir « Test d'assurance qualité » à la page 124). Si tel est le cas, modifiez le profil, réinstallez le système et recommencez le test.

3. **Créez un script `minimize-firewall.fin`, basé sur les dépendances des packages des deux étapes précédentes.**

Configuration du serveur et du client JumpStart

Cette section décrit la configuration du serveur et du client JumpStart en vue de l'utilisation d'un profil de sécurité pour la minimisation. Pour de plus amples informations sur l'utilisation du logiciel Solaris Security Toolkit dans un environnement JumpStart, reportez-vous au chapitre 5.

Cette section décrit les tâches suivantes :

Préparation de l'infrastructure

Préparez l'infrastructure en procédant comme suit. Les tâches suivantes permettent la création d'une configuration de base pour le client, en utilisant les pilotes, les profils et les scripts finish existants. Après la mise en oeuvre de cette configuration de base, vérifiez son fonctionnement, puis personnalisez-la pour l'application de votre choix.

▼ Pour préparer l'infrastructure

1. **Configurez le serveur et l'environnement JumpStart.**

   Reportez-vous au chapitre 5 pour des instructions détaillées.

2. **Ajoutez le client au serveur JumpStart en utilisant la commande** `add-client`**.**

EXEMPLE DE CODE 7-1 Ajout d'un client au serveur JumpStart

```
# pwd
/jumpstart
# bin/add-client -c marc -o Solaris_8_2002-02 -m sun4u
-s nomex-jumpstart
cleaning up preexisting install client "marc"
removing marc from bootparams
updating /etc/bootparams
```

3. **Créez une entrée de fichier** `rules` **pour le client, en spécifiant le profil JumpStart et le script finish. Par exemple :**

```
hostname marc - Profiles/xsp-minimal-firewall.profile \
  Drivers/xsp-firewall-secure.driver
```

4. **Créez un fichier nommé** `xsp-minimal-firewall.profile` **pour le profil et un fichier nommé** `xsp-firewall-secure.driver` **pour le pilote en copiant les fichiers fournis avec le logiciel Solaris Security Toolkit.**

   Vous devez créer ces fichiers pour pouvoir terminer l'étape suivante. Initialement, ces fichiers peuvent être des copies de fichiers distribués avec le logiciel Solaris Security Toolkit.

Remarque – Ne modifiez *jamais* les fichiers originaux distribués avec le logiciel Solaris Security Toolkit.

L'exemple suivant illustre la création des fichiers.

EXEMPLE DE CODE 7-2 Création d'un profil

```
# pwd
/jumpstart/Drivers
# cp install-Sun_ONE-WS.driver xsp-firewall-secure.driver
# cp hardening.driver xsp-firewall-hardening.driver
[...]
# pwd
/jumpstart/Drivers
# cp minimal-Sun_ONE-WS-Solaris8-64bit.profile \
     xsp-minimal-firewall.profile
```

L’exemple suivant utilise une configuration de serveur Web dédié, parce qu'il s'agit-là d'un point de départ adéquat pour le développement d'un pare-feu dédié.

5. **Après leur création, modifiez les fichiers de profil et de pilote comme suit :**

   a. **Remplacez la référence** `xsp-firewall-secure.driver` **à** `hardening.driver` **par** `xsp-firewall-hardening.driver`**.**

   b. **Remplacez les deux scripts finish définis dans** `JASS_SCRIPTS` **par les références à** `minimize-firewall.fin` **et au script finish (par exemple,** `fw1-patch-install.fin`**).**

      Le script modifié doit être similaire au suivant.

EXEMPLE DE CODE 7-3 Échantillon de sortie d'un script modifié

```
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
                minimize-firewall.fin
                fw1-patch-install.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

6. **Vérifiez que l'entrée du fichier** `rules` **est correcte en utilisant la commande suivante.**

EXEMPLE DE CODE 7-4 Vérification de la validité du fichier `rules`

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/end-user.profile...
Validating profile Profiles/xsp-minimal-firewall.profile...
Validating profile Profiles/test.profile...
Validating profile Profiles/entire-distribution.profile...
Validating profile Profiles/oem.profile...
The custom JumpStart configuration is ok.
```

   A ce stade, il doit être possible de commencer l'installation JumpStart sur le client, `marc` dans cet exemple. Utilisez la configuration JumpStart, les pilotes Solaris Security Toolkit, les scripts finish et les profils que vous avez créés.

7. **Si vous rencontrez des problèmes pendant la vérification du fichier** `rules`**, reportez-vous à la section** **« Validation et vérification du fichier Rules » à la page 117****.**

8. **A partir de l'invite `ok` du client, entrez la commande suivante pour installer le client en utilisant l'infrastructure JumpStart.**

```
ok> boot net - install
```

Si le client n'est pas *construit*, vérifiez la configuration et modifiez-la jusqu'à ce qu'elle fonctionne correctement. Notez que tous les aspects de la configuration JumpStart *ne sont pas* décrits dans cette section. Reportez-vous à l'ouvrage Sun BluePrint *JumpStart Technology : Effective Use in the Solaris Operating Environment* pour de plus amples informations.

Après avoir terminé l'exécution du fichier `rules` et vérifié que les patchs sont correctement installés, vous pouvez démarrer l'installation de base du système client, ainsi que sa minimisation et sa sécurisation.

Validation et vérification du fichier Rules

Lors de la validation du fichier `rules`, vous risquez de rencontrer une série de problèmes. Certains problèmes les plus fréquents sont décrits dans cette section.

La première exécution du fichier `rules` donne la sortie suivante.

EXEMPLE DE CODE 7-5 Échantillon de sortie du fichier `rules`

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/xsp-minimal-firewall.profile...
Error in file "rules", line 20
hostname marc - Profiles/xsp-minimal-firewall.profile
Drivers/xsp-firewall-secure.driver
ERROR: Profile missing:
   Profiles/xsp-minimal-firewall.profile
```

Dans cet exemple, le profil spécifié dans l'entrée du fichier `rules` pour`marc` n'existe pas. Le profil `xsp-minimal-firewall.profile` n'était pas présent dans le répertoire `Profiles`. Normalement, cette erreur est due à une faute de frappe dans le nom de fichier ou à l'omission du répertoire des profils, ou simplement parce le profil n'a pas encore été créé. Réglez le problème et recommencez le contrôle.

Le second contrôle détecte deux autres problèmes. Le premier problème concerne le pilote appelé dans `xsp-firewall-secure.driver`. Au lieu d'appeler `xsp-firewall-hardening.driver`, `xsp-firewall-secure.driver` appelle toujours `hardening.driver`.

Le second problème est que la variable `JASS_SCRIPTS` est réglée sur `minimize-Sun_ONE-WS.fin` et non sur `minimize-firewall.fin`.

Le script suivant est incorrect.

EXEMPLE DE CODE 7-6 Échantillon de script incorrect

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="minimize-Sun_ONE-WS.fin"
. ${DIR}/driver.run
. ${DIR}/hardening.driver
```

Le script suivant est correct.

EXEMPLE DE CODE 7-7 Échantillon de script correct

```
#!/bin/sh
DIR="`/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
minimize-firewall.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

Personnalisation de la configuration de sécurisation

La configuration de sécurisation du pare-feu proposé est prête à être personnalisée et affinée. Les scripts initiaux se basent sur `hardening.driver`. Ceci signifie que tous les services du système sont désactivés.

Étant donné que le SE Solaris 8 *ne contient pas* de client Secure Shell, vous devez effectuer des modifications pour permettre l'administration à distance, via le réseau, des pare-feux. En ce qui concerne le pare-feu dans cet exemple, il est spécifié que les services FTP doivent rester activés et qu'un client Secure Shell doit être installé pour

l'administration à distance. Limitez ces deux services uniquement au réseau privé de gestion, en empêchant donc l'écoute sur toutes les autres interfaces réseau. Pour de plus amples informations sur la restriction de ces services, reportez-vous à l'article Sun BluePrints en ligne intitulé « Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment ».

Laissez non seulement ces deux services activés, mais également les services RPC, de manière à pouvoir utiliser l'IG pour configurer Sostice DiskSuite et effectuer la mise en miroir du disque. Si vous n'envisagez pas de vous servir de l'IG de Solstice DiskSuite, les services RPC sont inutiles. Dans cet exemple, l'IG est requise et les services RPC sont activés. Notez que l'installation et la configuration de Solstice DiskSuite ne font pas l'objet de cet ouvrage.

La modification finale pour ce client consiste en un fichier `syslog.conf` personnalisé qui utilise le serveur `SYSLOG` central du fournisseur de services. Ce fichier `syslog.conf` personnalisé doit être installé sur chacun des systèmes de pare-feu.

Un grand nombre d'options de configuration de Solaris Security Toolkit doivent être modifiées. Chacune des modifications nécessaires est décrite en détails dans les sections suivantes.

Activation du service FTP

Le pare-feu dans cet exemple requiert que les services FTP soient activés.

▼ Pour activer le service FTP

1. **Pour laisser le service FTP activé, modifiez le comportement par défaut du fichier `update-inetd-conf.fin` en définissant les variables `JASS_SVCS_DISABLE` et `JASS_SVCS_ENABLE`.**

   Pour désactiver tous les services standard du SE Solaris à l'exception du service FTP, la meilleure méthode, dans cet exemple, consiste à définir `JASS_SVCS_ENABLE` sur `ftp`, tout en veillant à ce que `JASS_SVCS_DISABLE` conserve sa valeur par défaut obtenue via le script `finish.init`. Voir *Solaris Security Toolkit 4.2 Reference Manual*.

2. **Pour mettre en oeuvre le changement à l'aide des variables d'environnement, ajoutez une entrée du type ci-dessous à** `xsp-firewall-secure.driver` **avant l'appel de** `xsp-firewall-hardening.driver`**.**

```
JASS_SVCS_ENABLE="ftp"
```

3. **Vérifiez que le service FTP n'est disponible que sur le réseau de gestion du fournisseur de services, en le mettant en oeuvre au moyen du logiciel de pare-feu.**

   Parmi les autres conditions requises, le service FTP doit être disponible *uniquement* sur le réseau de gestion du fournisseur de services. Sous le SE Solaris 8, vous pouvez mettre en oeuvre cette condition en incorporant des wrappers TCP sur le système ou par l'intermédiaire du logiciel de pare-feu. Dans cet exemple, effectuez cette opération à l'aide du logiciel de pare-feu.

Installation du logiciel Secure Shell

Remarque – Les présentes instructions s'appliquent *uniquement* aux systèmes exécutant le SE Solaris 8. Si le système exécute le SE Solaris 9 ou 10, vous pouvez utiliser le logiciel Secure Shell distribué avec le SE Solaris et ignorer les étapes d'installation d'OpenSSH décrites dans cette section.

Le SE Solaris 8 *n'inclut pas* de client Secure Shell, par conséquent, si le système exécute le SE Solaris 8, vous devez installer un client Secure Shell pour l'administration à distance.

Vous pouvez configurer le logiciel Solaris Security Toolkit pour installer l'outil OpenSSH. Utilisez le script `install-openssh.fin`, répertorié dans le fichier`config.driver` utilisé par `xsp-firewall-secure.driver`.

▼ Pour installer Secure Shell

1. **Copiez le fichier** `config.driver` **par défaut sur** `xsp-firewall-config.driver`**.**
2. **Dans la copie du fichier, annulez le commentaire relatif à** `install-openssh.fin`**.**
3. **Modifiez l'entrée dans** `xsp-firewall-secure.driver` **qui appelle** `config.driver` **afin qu'elle appelle** `xsp-firewall-config.driver`**.**

4. **Procurez-vous la dernière version d'OpenSSH.**

   Comme pour les patchs et le système d'exploitation, veillez à toujours utiliser la version la plus récente d'OpenSSH. Pour des informations sur la toute dernière version d'OpenSSH, consultez les pages Web correspondantes à l'adresse suivante :

   `http://www.openssh.org`

5. **Compilez le dernier package OpenSSH, attribuez-lui un nom et installez-le dans le répertoire** `Packages`**.**

   Pour de plus amples informations sur ce package, reportez-vous à l'article Sun BluePrints en ligne intitulé « Configuring OpenSSH for the Solaris Operating Environment ».

6. **Mettez à jour le script** `install-openssh.fin` **afin qu'il reflète le nom du package OpenSSH.**

   Il peut être nécessaire de modifier le script `install-openssh.fin`. Ce script définit le nom du package OpenSSH dont le format doit être du type suivant :

   ```
   OBSDssh-3.5p1-sparc-sun4u-5.8.pkg
   ```

   Où le nom de package est constitué par le numéro de version (`3.5p1`), l'architecture (`sparc`), la version de l'architecture (`sun4u`), le système d'exploitation pour lequel ce package a été compilé (`5.8`) et un suffixe `pkg`.

7. **Vérifiez que SSH n'est disponible que sur le réseau de gestion du fournisseur de services, en le mettant en oeuvre au moyen du logiciel de pare-feu.**

   Parmi les autres conditions requises, Secure Shell doit être disponible uniquement sur le réseau de gestion du fournisseur de services. Sous le SE Solaris 8, vous pouvez mettre en oeuvre cette condition en incorporant des wrappers TCP sur le système ou par l'intermédiaire du logiciel de pare-feu. Dans cet exemple, effectuez cette opération à l'aide du logiciel de pare-feu. Notez que cette condition peut également être mise en oeuvre en modifiant la configuration du serveur Secure Shell.

Activation du service RPC

Laissez les services RPC activés afin de pouvoir utiliser Solstice DiskSuite pour la mise en miroir du disque, qui nécessite RPC.

Cette modification est relativement simple grâce à un script finish spécifique, `disable-rpc.fin`, qui désactive les services RPC pendant l'exécution de Solaris Security Toolkit.

Remarque – L'accès à distance aux services RPC sur un système doit être explicitement interdit par la configuration du pare-feu du système.

▼ Pour activer RPC

- **Supprimez le commentaire de l'entrée de** `disable-rpc.fin` **dans** `xsp-firewall-hardening.driver`**.**

  Désactivez les scripts à partir des pilotes en annulant leurs commentaires au lieu de les supprimer. Annulez les commentaires des entrées avec précaution dans la définition `JASS_SCRIPTS`, parce que *seules* certaines combinaisons de commentaires sont acceptées.

  Le commentaire ci-après, contenu dans le `script driver.funcs`décrit les indicateurs de commentaires acceptés par le logiciel Solaris Security Toolkit dans la définition `JASS_SCRIPTS`.

```
#Gestionnaire de commentaires très rudimentaire. Ce code reconnaît
uniquement
#les commentaires contenant un seule signe # devant le nom de
fichier
#(séparé ou non par un espace). Ensuite, il ignore uniquement
#l'argument suivant.
```

Personnalisation du fichier `syslog.conf`

La modification finale pour ce client consiste en un fichier `syslog.conf` personnalisé qui utilise le serveur `SYSLOG` central du fournisseur de services. Ce fichier `syslog.conf` personnalisé doit être installé sur chacun des systèmes de pare-feu.

▼ Pour personnaliser le fichier `syslog.conf`

1. **Copiez le fichier** `syslog.conf` **standard du fournisseur de services, renommez-le** `syslog.conf.marc` **et placez-le dans le répertoire** `Files/etc`**.**

   Le logiciel Solaris Security Toolkit permet de copier des fichier selon plusieurs méthodes. La méthode la plus appropriée pour cette configuration est d'ajouter au fichier le nom d'hôte du système sous forme de suffixe, de sorte que le fichier `syslog.conf` soit *uniquement* copié sur le client `marc`, parce qu'il contient des modifications uniques spécifiques au pare-feu. Dans le cas présent, le client s'intitule `marc`, de sorte que le nom de fichier utilisé dans `Files/etc` est `syslog.conf.marc`. Il est important de noter que la définition de `JASS_FILES` *ne doit pas* contenir de suffixe. Pour de plus amples informations, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

2. **Si le fichier standard** `syslog.conf` **du fournisseur de services** ***n'est pas*** **disponible, créez un fichier**`syslog.conf` **personnalisé en procédant comme suit :**

   a. **Copiez le fichier** `syslog.conf` **inclus avec le logiciel Solaris Security Toolkit, renommez-le** `syslog.conf.marc` **et placez-le dans le répertoire** `Files/etc`**.**

   b. **Modifiez** `syslog.conf.marc` **pour le rendre conforme à la norme du fournisseur de services de** `SYSLOG`**.**

3. **Vérifiez que le fichier** `/etc/syslog.conf` **est répertorié dans la définition** `JASS_FILES` **de** `xsp-firewall-hardening.driver`**.**

   Par défaut, la définition modifiée `JASS_FILE` dans `xsp-firewall-hardening.driver` est la suivante.

EXEMPLE DE CODE 7-8 Échantillon de sortie du fichier `xsp-firewall-hardening.driver` modifié

```
JASS_FILES="
                    /etc/dt/config/Xaccess
                    /etc/init.d/inetsvc
                    /etc/init.d/nddconfig
                    /etc/init.d/set-tmp-permissions
                    /etc/issue
                    /etc/motd
                    /etc/notrouter
                    /etc/rc2.d/S00set-tmp-permissions
                    /etc/rc2.d/S07set-tmp-permissions
                    /etc/rc2.d/S70nddconfig
                    /etc/syslog.conf
"
```

A ce stade, toutes les modifications requises ont été effectuées. L'installation du système d'exploitation, la minimisation et la sécurisation sont entièrement automatisés et personnalisés pour une application spécifique. Les *seuls* processus qui *ne sont pas* entièrement automatisées sont la configuration et l'installation du logiciel de pare-feu et de Solstice DiskSuite. Même si ces configurations peuvent être réalisées en utilisant la technologie JumpStart, les instructions correspondantes ne sont pas traitées dans cet ouvrage. Reportez-vous à l'ouvrage Sun BluePrints *JumpStart Technology: Effective Use in the Solaris Operating Environment*.

Installation du client

Après avoir apporté toutes les modifications voulues au pilotes, installez le client en procédant comme décrit dans cette section.

▼ Pour installer le client

1. **Quand toutes les modifications requises ont été apportées aux pilotes, installez le client en utilisant l'infrastructure JumpStart.**

   Utilisez la commande suivante à l'invite `ok` du client.

   ```
   ok> boot net - install
   ```

2. **Si vous rencontrez des erreurs, corrigez-les et réinstallez le système d'exploitation du client.**

Test d'assurance qualité

La dernière tâche de ce processus consiste à vérifier que les applications et services offerts par le système fonctionnent correctement. Cette tâche permet aussi de vérifier que le profil de sécurité a correctement mis en oeuvre les modifications requises.

Il est important que cette tâche soit accomplie avec soin et immédiatement après la réinitialisation de la plate-forme qui vient d'être sécurisée et minimisée, afin d'assurer la détection des anomalies ou problèmes éventuels et leur rapide correction. Cette procédure comporte deux tâches : la vérification de l'installation du profil et celle du fonctionnement des applications et des services.

▼ Pour vérifier l'installation du profil

Pour vérifier que le logiciel Solaris Security Toolkit a installé correctement le profil de sécurité sans erreur, contrôlez et évaluez ce qui suit :

1. **Vérifiez le fichier journal de l'installation.**

   Ce fichier est installé dans le répertoire `JASS_REPOSITORY/jass-install-log.txt`.

   Remarque – Ce fichier journal peut être utilisé comme référence pour connaître avec précision les opérations effectuées sur le système par le logiciel Solaris Security Toolkit. Pour chaque exécution sur le système, un nouveau fichier journal est enregistré dans le répertoire en fonction de l'heure de démarrage de l'exécution. Ces fichiers, et tous les autres fichiers présents dans le répertoire `JASS_REPOSITORY`, ne doivent *jamais* être modifiés directement.

   ---

2. **Utilisez l'option d'audit pour évaluer la configuration de sécurité du système.**

   Pour de plus amples informations sur l'option d'audit, reportez-vous au chapitre 6. Dans cet exemple, vous utilisez la commande suivante du répertoire d'installation du logiciel Solaris Security Toolkit sur le client.

   EXEMPLE DE CODE 7-9 Évaluation d'une configuration de sécurité

```
# ./jass-execute -a xsp-firewall-secure.driver
[NOTE] Executing driver, xsp-firewall-secure.driver
================================================================
xsp-firewall-secure.driver: Driver started.
================================================================

================================================================
Solaris Security Toolkit Version:   4.2.0
[...]
```

   Si la vérification de Solaris Security Toolkit rencontre des incohérences, celles-ci sont consignées. Un résumé des incohérences détectées est généré au terme de la vérification. La sortie complète de la vérification se trouve dans le répertoire `JASS_REPOSITORY`.

▼ Pour vérifier le fonctionnement des applications et des services

La vérification des applications et des services passe par la mise en oeuvre d'un plan de test et d'acceptation bien défini. Ce plan permet de tester les différents composants d'un système ou d'une application, et de s'assurer que ceux-ci sont disponibles et fonctionnent correctement. En l'*absence* d'un tel plan, testez le système avec logique en vous basant sur la manière dont il est utilisé. L'objectif est de s'assurer que la sécurisation n'a pas altéré le fonctionnement des applications ou services.

1. **En cas d'anomalie de fonctionnement d'une application ou d'un service après la sécurisation du système, utilisez les techniques décrites dans le chapitre 2 pour déterminer le problème.**

   Par exemple, utilisez la commande `truss`. Cette commande peut souvent être utilisée pour déterminer à quel point une application présente un problème. Une fois ceci déterminé, il est possible de cibler le problème et de remonter à la modification effectuée par le logiciel Solaris Security Toolkit.

   Remarque – D'après l'expérience collective des développeurs de Solaris Security Toolkit, la plupart des problèmes peuvent être évités en suivant la démarche expliquée dans cet ouvrage.

   ---

2. **De même, testez le logiciel Check PointFirewall-1 NG, remontez aux modifications du logiciel Solaris Security Toolkit et corrigez les problèmes.**

3. **Si la liste finale des packages doit être modifiée, modifiez le profil, réinstallez le système et recommencez le test.**

Glossaire

La liste suivante définit les abréviations et acronymes du logiciel Solaris Security Toolkit.

A

`ab2` AnswerBook2

ABI Application Binary Interface (interface binaire d'application)

ARP Address Resolution Protocol (protocole de résolution d'adresse)

ASPPP Asynchronous Point-to-Point Protocol (protocole point à point asynchrone)

B

BART Basic Auditing and Reporting Tool (outil d'audit et de rapport de base)

BIND Berkeley Internet Name Domain (domaine de nom Internet Berkeley)

BSD Berkeley Software Distribution (distribution logicielle Berkeley)

BSM Basic Security Module *(Solaris)* (module de sécurité de base)

C

CD Disque compact

CD-ROM Disque compact – mémoire morte

CDE Common Desktop Environment

`cp`**(1)** Commande de copie de fichiers

`cron`**(1M)** Commande de démon d'horloge

D

DHCP Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte)

DMI Desktop Management Interface (interface d'administration du bureau)

DMTF Distributed Management Task Force (groupe DMTF)

DNS Domain Name System (système de noms de domaine)

E

EEPROM Electronically Erasable Programmable Read-Only Memory (mémoire morte effaçable et programmable électroniquement)

F

FACE Framed Access Command Environment (environnement de commande d'accès structuré)

FMRI Fault Management Resource Identifier (identificateur de ressources de gestion défectueuses)

FTP File Transfer Protocol (protocole de transfert de fichiers)

G

GID Group Identifier (identificateur de groupe)

H

HSFS High Sierra File System (système de fichiers High Sierra)

HTTP HyperText Transfer Protocol (protocole de transfert hypertexte)

I

ID Identificateur

IETF Internet Engineering Task Force (groupe IETF)

IG Interface graphique

INETD Internet Service Daemon (démon de service Internet)

IP Internet Protocol (protocole Internet)

IPF Internet Protocol Filter (filtre de protocole Internet)

ISA Instruction Set Architecture (architecture ISA)

J

JASS JumpStart Architecture and Security Scripts, *désormais* Solaris Security Toolkit

K

KDC Kerberos Key Distribution (distribution de clés Kerberos)

L

LDAP Lightweight Directory Access Protocol (protocole d'accès aux annuaires léger)

`lp`**(1)** Commande d'impression *(requête d'envoi d'impression)*

M

MAN Management Network (réseau de gestion) *(réseau interne I1 des systèmes haut de gamme Sun Fire)*

MD5 Algorithme Message-Digest 5

MIP Mobile Internet Protocol (protocole Internet mobile)

MSP Midframe Service Processor (processeur de service midframe)

`mv`**(1)** Commande de déplacement de fichiers

N

NFS Network File System (système de fichiers sur réseau)

NG Next Generation (génération suivante)

NGZ Non-Global Zone (zone non globale)

NIS, NIS+ Network Information Services (services d'informations en réseau)

NP No Password (aucun mot de passe)

NSCD Name Service Cache Daemon (démon de cache de service de noms)

O

OEM Original Equipment Manufacturer (fabricant d'équipement d'origine)

P

PAM Pluggable Authentication Module (module d'authentification enfichable)

PDF Portable Document Format (format de document portable)

Perl Practical Extraction and Report Language (langage pratique d'extraction et de rapport)

PICL Platform Information and Control Library (informations sur la plate-forme et bibliothèque de contrôle)

PPP Point-to-Point Protocol (protocole point à point)

PROM Programmable Read-Only Memory (mémoire morte programmable)

Q

QA Quality Assurance (assurance qualité)

R

RBAC Role-Based Access Control (contrôle d'accès basé sur les rôles)

rc run-control (contrôle d'exécution) (*fichier ou script*)

RFC Remote Function Call (appel de fonction à distance)

`rlogin`**(1)** Commande de connexion à distance

RPC Remote Procedure Call (appel de procédure à distance)

`rsh`**(1)** Commande de shell à distance

S

SA System Administrator (administrateur système)

SC System Controller (contrôleur système) (*systèmes haut de gamme et milieu de gamme Sun Fire*)

SCCS Source Code Control System (système de contrôle du code source)

`scp`**(1)** Commande de copie sécurisée (*programme de copie de fichiers à distance*)

SE Système d'exploitation

SLP Service Location Protocol (protocole d'emplacement de service)

SMA System Management Agent

SMC Solaris Management Console

SMF Service Management Facility

SMS System Management Services

SNMP Simple Network Management Protocol (protocole d'administration réseau simple)

SP Service Provider (fournisseur de services)

SPARC Scalable Processor Architecture (architecture de processeur évolutive)

SPC SunSoft Print Client (client d'impression SunSoft)

SSH Secure Shell (*SE Solaris 9 et 10*)

SVM Solaris Volume Manager

T

TCP Transmission Control Protocol (procole de contrôle de transmission)

`tftp`**(1)** Programme de transfert de fichiers trivial

`ttl` Durée de vie

U

UDP User Datagram Protocol (protocole datagramme utilisateur)

UFS Unix File System (système de fichiers Unix)

UID Identificateur d'utilisateur

UUCP UNIX-to-UNIX Copy (copie UNIX)

V

VOLD Volume Management Daemon (démon du gestionnaire de volumes)

W

WBEM Web-based Enterprise Management (gestion d'entreprise basée sur le Web)

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W