Guide d'administration de Solaris™ Security Toolkit 4.1

Sun Microsystems, Inc.
www.sun.com

Référence : 817-7652-10
Octobre 2004, révision A

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

Table des matières

Figures

Tableaux

Exemples de code

Préface

Le présent manuel comprend des informations de référence destinées à faciliter la compréhension et l'utilisation du logiciel Solaris Security Toolkit. Il s'adresse en priorité aux personnes qui utilisent le logiciel Solaris Security Toolkit afin de sécuriser les versions 8 et 9 du système d'exploitation (SE) Solaris™, en particulier les administrateurs, consultants et autres utilisateurs chargés de déployer de nouveaux systèmes Sun ou de sécuriser les systèmes déployés. Les instructions fournies s'appliquent à l'utilisation du logiciel en mode JumpStart™ ou en mode autonome.

Avant de lire ce document

Ce manuel s'adresse aux administrateurs système certifiés Sun pour le système d'exploitation Solaris™ ou aux administrateurs réseau certifiés Sun pour le système d'exploitation Solaris™ maîtrisant également les protocoles et les topologies réseau standard.

Comme ce document s'adresse à un public varié, votre expérience ou vos connaissances en matière de sécurité détermineront l'utilisation que vous en ferez.

Organisation de ce guide

Ce manuel tient lieu de guide de l'utilisateur. Il contient des informations, des instructions et des directives relatives à l'utilisation du logiciel à des fins de sécurisation de systèmes. Cet ouvrage est ainsi organisé :

Le **Chapitre 1** décrit la conception et l'objectif du logiciel Solaris Security Toolkit. Il traite des composants clés, des fonctionnalités, des avantages et des plates-formes prises en charge.

Le **Chapitre 2** explique comment sécuriser des systèmes. Il propose une méthode à appliquer avant de sécuriser des systèmes à l'aide du logiciel Solaris Security Toolkit.

Le **Chapitre 3** explique comment télécharger, installer et exécuter le logiciel Solaris Security Toolkit et d'autres logiciels ayant trait à la sécurité.

Le **Chapitre 4** explique comment rétablir le système en annulant les modifications introduites par le logiciel Solaris Security Toolkit pendant l'exécution des opérations de durcissement.

Le **Chapitre 5** décrit comment configurer et gérer les serveurs JumpStart en vue d'utiliser le logiciel Solaris Security Toolkit.

Le **Chapitre 6** décrit comment contrôler (valider) la sécurité d'un système à l'aide du logiciel Solaris Security Toolkit. Utilisez les indications et les procédures figurant dans ce chapitre pour maintenir un profil de sécurité donné après le durcissement.

Le **Chapitre 7** décrit comment appliquer à un scénario réaliste les informations contenues dans les chapitres précédents pour installer et sécuriser un nouveau système.

Utilisation des commandes UNIX®

Ce document peut ne pas contenir d'informations sur les commandes et procédures UNIX® de base telles que l'arrêt et le démarrage du système ou la configuration des périphériques. Consultez les sources d'information suivantes pour en savoir plus à ce sujet :

- la documentation des logiciels fournis avec votre système ;
- la documentation du système d'exploitation Solaris, disponible à l'adresse

  `http://docs.sun.com`

Invites de shell

Shell	Invite
Shell C	*nom-machine*%
Superutilisateur du shell C	*nom-machine*#
Shells Bourne et Korn	$
Superutilisateur des shells Bourne et Korn	#

Conventions typographiques

Police de caractère*	Signification	Exemples
AaBbCc123	Noms de commandes, de fichiers et de répertoires ; affichage sur l'écran de l'ordinateur	Modifiez le fichier .login. Utilisez la commande ls -a pour afficher la liste de tous les fichiers. % Vous avez du courrier.
AaBbCc123	Ce que vous tapez, par opposition à l'affichage sur l'écran de l'ordinateur	% **su** Mot de passe :
AaBbCc123	Titres d'ouvrages, nouveaux mots ou termes, mots importants. Remplacez les variables de la ligne de commande par des noms ou des valeurs réels.	Consultez le chapitre 6 du *Guide de l'utilisateur.* Il s'agit d'options de *classe*. Vous *devez* être un superutilisateur pour effectuer ces opérations. Pour supprimer un fichier, tapez rm *nom_fichier*.

* Les paramètres de votre navigateur peuvent différer de ceux-ci.

Documentation Sun sur le Web

Vous pouvez visualiser, imprimer ou acquérir une large sélection de documents Sun à l'adresse suivante :

http://www.sun.com/documentation

Sites Web tiers

Sun rejette toute responsabilité quant à la disponibilité des sites Web tiers mentionnés dans ce document. Sun ne peut en aucun cas être tenu responsable du contenu, des publicités, des produits ou de toute autre matériel disponibles sur ces sites ou accessibles à partir de ces sites ou ressources. Sun ne pourra en aucun cas être tenu pour responsable en cas de pertes ou de dommages réels ou supposés causés par l'utilisation (ou liés à celle-ci) ou la prise en compte des informations, biens ou services disponibles sur de tels sites ou resources ou accessibles par leur intermédiaire.

Ressources connexes

Les publications et sites Web apparentés sont recensés ci-dessous.

Publications

- Andert, Donna, Wakefield, Robin, and Weise, Joel. « Trust Modeling for Security Architecture Development », Sun BluePrints™ OnLine, Décembre 2002, http://www.sun.com/blueprints/1202/817-0775.pdf.
- Dasan, Vasanthan, Noordergraaf, Alex, and Ordica, Lou. « The Solaris Fingerprint Database - A Security Tool for Solaris Software and Files », Sun BluePrints OnLine, Mai 2001, http://www.sun.com/blueprints/0501/Fingerprint.pdf.
- Englund, Martin, « Securing Systems with Host-Based Firewalls - Implemented With SunScreen Lite 3.1 Software », Sun BluePrints OnLine, Septembre 2001, http://sun.com/blueprints/0901/sunscreenlite.pdf.

- Garfinkel, Simon, and Spafford, Gene. *Practical UNIX and Internet Security*, 2ème Édition, O'Reilly & Associates, Avril 1996.
- Howard, John S., and Noordergraaf, Alex. *JumpStart Technology : Effective Use in the Solaris Operating Environment*, The Official Sun Microsystems Resource Series, Prentice Hall, Octobre 2001.
- Moffat, Darren J., FOCUS on SUN : *Solaris BSM Auditing*, http://www.securityfocus.com/infocus/1362.
- Noordergraaf, Alex. « Solaris™ Operating Environment Minimization for Security : A Simple, Reproducible and Secure Application Installation Methodology Updated for Solaris 8 Operating Environment », Sun BluePrints OnLine, Novembre 2000, http://sun.com/blueprints/1100/minimize-updt1.pdf.
- Noordergraaf, Alex. « Minimizing the Solaris Operating Environment for Security : Updated for Solaris 9 Operating Environment », Sun BluePrints OnLine, Novembre 2002, http://sun.com/blueprints/1102/816-5241.pdf.
- Noordergraaf, Alex. « Securing the Sun Cluster 3.x Software », article Sun BluePrints OnLine, Février 2003, http://www.sun.com/solutions/blueprints/0203/817-1079.pdf.
- Noordergraaf, Alex, « Securing the Sun Enterprise 10000 System Service Processors », article Sun BluePrints OnLine, Mars 2002, http://www.sun.com/blueprints/0302/securingenter.pdf.
- Noordergraaf, Alex, et. al. *Enterprise Security : Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8,* Sun Microsystems™, Prentice Hall Press, ISBN 0-13-100092-6, Juin 2002.
- Noordergraaf, Alex and Nimeh, Dina. « Securing the Sun Fire 12K and 15K Domains », article Sun BluePrints OnLine, Février 2003, http://www.sun.com/blueprints/0203/817-1357.pdf.
- Noordergraaf, Alex and Nimeh, Dina. « Securing the Sun Fire 12K and 15K System Controllers », article Sun BluePrints OnLine, Février 2003, http://www.sun.com/blueprints/0203/817-1358.pdf.
- Noordergraaf, Alex and Watson, Keith. « Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment », Sun BluePrints OnLine, Décembre 2002, http://www.sun.com/blueprints/1202/816-5242.pdf.
- O'Donnell, Nicholas and Noordergraaf, Alex. « Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems », articles Sun BluePrints OnLine, Septembre 2003, http://www.sun.com/blueprints/0903/817-3340.pdf [Partie I] et http://www.sun.com/blueprints/0903/817-3628.pdf [Partie II].
- Osser, William and Noordergraaf, Alex. « Auditing in the Solaris 8 Operating Environment », Sun BluePrints OnLine, Février 2001 http://www.sun.com/blueprints/0201/audit_config.pdf.
- Reid, Jason M. and Watson, Keith. « Building and Deploying OpenSSH in the Solaris Operating Environment », Sun BluePrints OnLine, Juillet 2001, http://sun.com/blueprints/0701/openSSH.pdf.

- Reid, Jason M. « Configuring OpenSSH for the Solaris Operating Environment », article Sun BluePrints OnLine, Janvier 2002, http://www.sun.com/blueprints/0102/configssh.pdf.
- Reid, Jason. *Secure Shell in the Enterprise*, The Official Sun Microsystems Resource Series, Prentice Hall, Juin 2003
- *Solaris Advanced Installation Guide*, Sun Microsystems, `http://docs.sun.com`.
- *SunSHIELD Basic Security Module Guide*, Sun Microsystems, Inc., http://docs.sun.com.
- Watson, Keith and Noordergraaf, Alex. « Solaris Operating Environment Network Settings for Security : Updated for Solaris 9 Operating Environment », Sun BluePrints OnLine, Juin 2003, http://www.sun.com/solutions/blueprints/0603/816-5240.pdf.
- Weise, Joel, and Martin, Charles R. « Developing a Security Policy », article Sun BluePrints OnLine, Décembre 2001, http://www.sun.com/solutions/blueprints/1201/secpolicy.pdf.

Sites Web

- AUSCERT, *UNIX Security Checklist*, http://www.auscert.org.au/render.html?it=1935&cid=1920
- CERT/CC sur http://www.cert.org est un centre de recherche et de développement en matière de sécurité informatique financé par des fonds fédéraux.
- Chkrootkit, http://www.chkrootkit.org
- Galvin, Peter Baer, *The Solaris Security FAQ*, http://www.itworld.com/Comp/2377/security-faq/
- HoneyNet Project, « Know Your Enemy : Motives » http://project.honeynet.org/papers/motives/
- Liste des logiciels de fichiers ouverts, ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
- Scanner de port Nmap, http://www.insecure.org
- Outil OpenSSH, http://www.openssh.com/
- Pomeranz, Hal, *Solaris Security Step by Step*, `http://www.sans.org/`
- Rhoads, Jason, *Solaris Security Guide*, http://www.sabernet.net/papers/Solaris.html
- Security Focus, disponible à l'adresse http://www.securityfocus.org, est un site de discussion sur des questions de sécurité.
- Sendmail Consortium, informations sur la configuration de `sendmail`, http://www.sendmail.org/

- Spitzner, Lance, *Armoring Solaris*, http://secinf.net/unix_security/Armoring_Solaris.html
- SSH Communications Security, Secure Shell (SSH) tool, http://www.ssh.com/
- Sun BluePrints OnLine, http://sun.com/blueprints
- Outils Sun BluePrints OnLine pour les logiciels FixModes et scripts MD5, http://jsecom15k.sun.com/ECom/EComActionServlet?StoreId=8&PartDetailId=817-0074-10&TransactionId=try&LMLoadBalanced=
- Informations sur le mécanisme d'authentification Sun Enterprise Authentication Mechanism™, http://www.sun.com/software/solaris/ds/ds-seam
- SunSolve℠ – http://sunsolve.sun.com

Support technique Sun

Si vous ne trouvez pas de réponses dans le présent manuel à vos éventuelles questions techniques, rendez-vous sur :

http://www.sun.com/service/contacting

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et vos suggestions. Envoyez-nous vos commentaires en vous rendant à l'adresse suivante :

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

Veuillez inclure le titre et la référence du document en question dans votre commentaire :

Guide d'administration de Solaris Security Toolkit 4.1, référence 817-7652-10.

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 indications générales pour garder le contrôle de la version des modifications et des déploiements et fournit des informations importantes pour la personnalisation du logiciel Solaris Security Toolkit.

Ce chapitre traite des points suivants :

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 automatique, extensible et évolutif pour sécuriser et maintenir sécurisés les systèmes Solaris OS. À l'aide du logiciel Solaris Security Toolkit, vous pouvez durcir et réduire vos systèmes ou effectuer des audits de sécurité.

- **Durcissement** – La modification des configurations de Solaris OS pour accroître la sécurité d'un système.

- **Réduction** : élimination des packages du SE Solaris qui ne sont pas nécessaires sur un système donné. (Chaque système étant différent, il faut évaluer au cas par cas les packages effectivement superflus.) L'élimination des packages superflus réduit le nombre de composants auxquels appliquer des patchs et à sécuriser ainsi que le nombre de points d'intrusion possibles.
- **Audit** : processus permettant de déterminer si la configuration d'un système est conforme à un profil de sécurité prédéfini.
- **Score** : valeur associée au nombre d'échecs détectés au cours d'un audit. Si aucun échec (d'aucun type) n'est détecté, le score final est de 0. Le logiciel Solaris Security Toolkit augmente le score (également appelé valeur de vulnérabilité) par incréments de 1 pour chaque échec détecté.

L'installation et la configuration du système doivent autant que possible être automatisées (l'idéal serait qu'elles soient 100 % automatiques). Ces instructions couvrent l'installation et la configuration du système d'exploitation, la configuration du réseau, les comptes utilisateurs, les applications et les modifications de sécurité. Les modifications de sécurité peuvent inclure le durcissement et/ou la réduction, selon le type d'usage du système. Le logiciel JumpStart est une technologie permettant d'automatiser les installations du SE Solaris. Le logiciel JumpStart permet l'installation de systèmes sur un réseau de manière entièrement automatique ou avec un minimum d'intervention humaine. Le logiciel Solaris Security Toolkit contient des profils et des scripts permettant l'implémentation et l'automatisation de la plupart des tâches associées au durcissement et à la réduction de systèmes sous Solaris dans les installations basées sur le logiciel JumpStart.

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

Indépendamment du mode d'installation de votre système, vous pouvez initialement utiliser le logiciel Solaris Security Toolkit pour durcir et réduire vos systèmes. Utilisez ensuite périodiquement le logiciel Solaris Security Toolkit pour s'assurer que le profil de sécurité des systèmes sécurisés n'a pas été modifié par accident ou par malveillance.

Remarque – Le terme *audit* désigne la procédure automatisée selon laquelle le logiciel Solaris Security Toolkit valide un niveau de sécurité en la comparant avec 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 cette option.

Description des composants du logiciel

Cette section contient une présentation de la structure des composants du logiciel Solaris Security Toolkit. Le logiciel Solaris Security Toolkit est un ensemble de fichiers et de répertoires. La FIGURE 1-1 illustre la structure du logiciel.

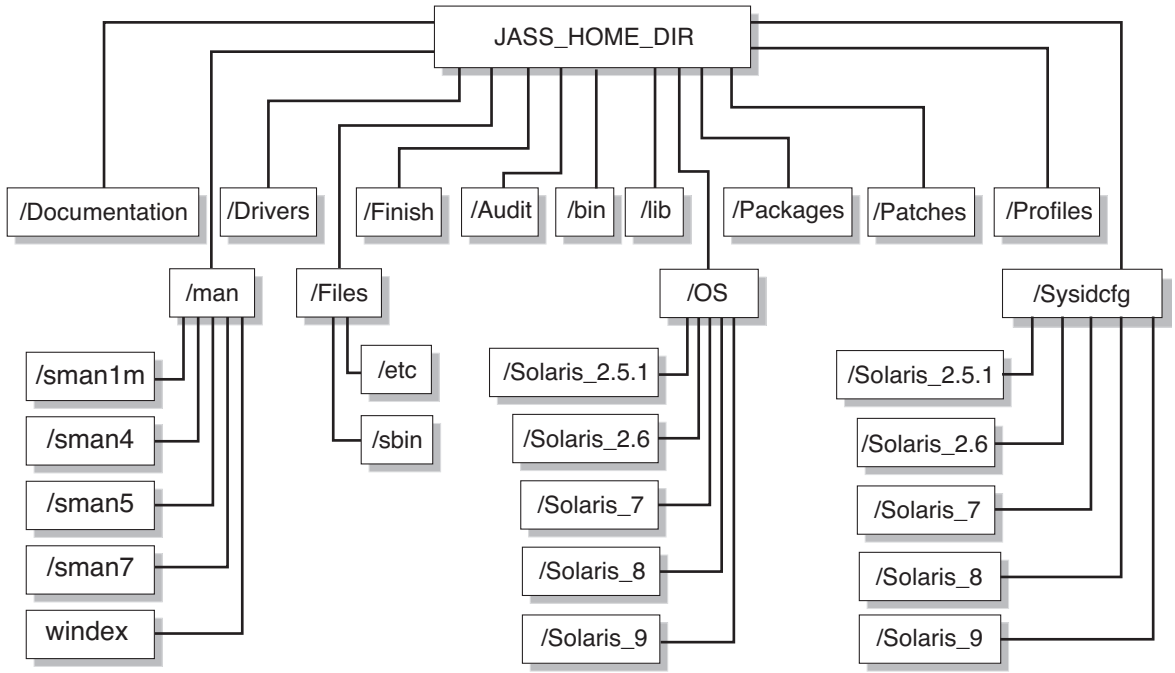

FIGURE 1-1 Structure des composants du logiciel

En plus de ces répertoires et sous-répertoires, les fichiers suivants sont situés au niveau supérieur de la structure du logiciel Solaris Security Toolkit, dans `/bin` :

- `add-client` – Programme d'aide JumpStart pour ajouter des clients dans un environnement JumpStart.
- `rm-client` – Programme d'aide JumpStart pour supprimer des clients d'un environnement JumpStart.
- `make-jass-pkg` – Commande offrant la possibilité de créer un package Solaris à partir du contenu du répertoire Solaris Security Toolkit afin de simplifier la distribution intérieure d'une configuration personnalisée Solaris Security Toolkit.
- `jass-check-sum` – Commande offrant la possibilité de déterminer si des fichiers modifiés par le logiciel Solaris Security Toolkit ont été changés, en se basant sur une somme de contrôle créée à chaque exécution de Solaris Security Toolkit.

- `jass-execute` – Commande permettant de configurer l'application Solaris Security Toolkit.

Répertoires

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

- `/Audit`
- `/bin`
- `/Documentation`
- `/man`
- `/Drivers`
- `/Files`
- `/Finish`
- `/lib`
- `/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 listé et des renvois à d'autres chapitres sont fournis pour des informations détaillées.

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 d'audit qui permettent de vérifier la conformité du système avec un profil ou un groupe de profils de sécurité préalablement 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 le *Solaris Security Toolkit 4.1 Reference Manual*.

Répertoire `Documentation`

Ce répertoire contient des fichiers texte comprenant des informations destinées à l'utilisateur, telles que le fichier `README`.

Répertoire `man`

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

Pour de plus amples informations sur ces pages de manuel, consultez-les directement ou reportez-vous au manuel *Solaris Security Toolkit 4.1 Man Page Guide*.

Répertoire `Drivers`

Ce répertoire contient des fichiers d'information sur la configuration indiquant quels fichiers sont exécutés et installés quand vous utilisez le logiciel Solaris Security Toolkit. Ce répertoire contient des pilotes, des scripts et des fichiers de configuration.

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

- `common_{log|misc}.funcs`
- `config.driver`
- `desktop-{config|hardening|secure}.driver`
- `driver.{funcs|init|run}`
- `hardening.driver`
- `finish.init`
- `install-Sun_ONE-WS.driver`
- `jumpstart-{config|hardening|secure}.driver`
- `secure.driver`
- `starfire-{config|hardening|secure}.driver`
- `suncluster3x-{config|hardening|secure}.driver`
- `sunfire_15k_domain-{config|hardening|secure}.driver`
- `sunfire_15k_sc-{config|hardening|secure}.driver`
- `sunfire_mf_msp-{config|hardening|secure}.driver`
- `undo.{funcs|init|run}`
- `hardening.driver`
- `user.init.SAMPLE`
- `user.run.SAMPLE`
- `audit_{private|public}.funcs`

Tous les pilotes spécifiques au produit et certains autres pilotes comportent trois fichiers chacun :

- *nom*`-secure.driver`
- *nom*`-config.driver`
- *nom*`-hardening.driver`

Ces trois fichiers sont placés entre crochets 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, vous devez utiliser uniquement le *nom*`-secure.driver`. Ce pilote appelle automatiquement les pilotes associés.

L'architecture de Solaris Security Toolkit comprend des informations de configuration pour permettre l'utilisation des scripts driver, finish et audit dans différents environnements, sans besoin de les modifier. Toutes les variables utilisées dans les scripts finish et audit sont conservées dans un groupe 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 trois fichiers principaux de configuration, qui se trouvent tous dans le répertoire `Drivers` :

- `driver.init`
- `finish.init`
- `user.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 extraits du répertoire Files. Pour de plus amples informations sur les scripts finish et audit, reportez-vous aux chapitres correspondants dans ce manuel.

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

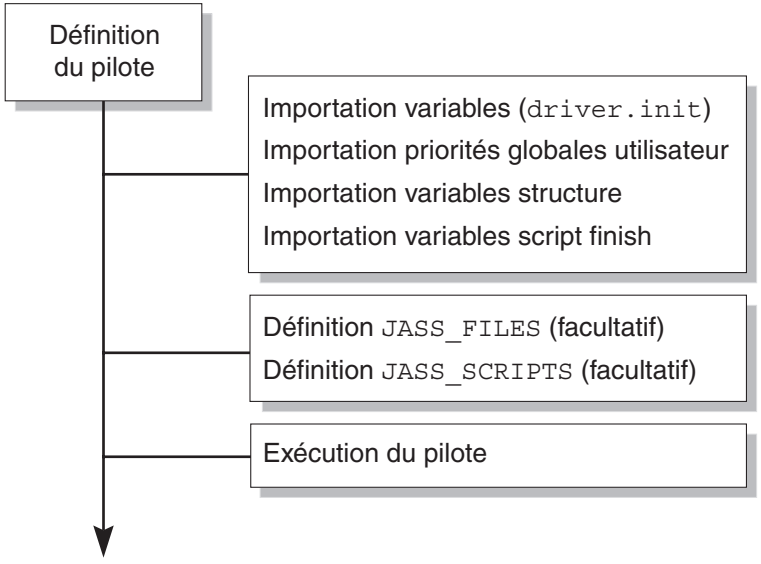

FIGURE 1-2 Flux de contrôle du pilote

Toutes les variables d'environnement des fichiers `.init` sont importées en premier. Une fois ces variables importées, le pilote passe à la deuxième partie pour la définition de `JASS_FILES` et `JASS_SCRIPTS`. Ces définitions sont facultatives ; il est possible de définir un seul environnement, les deux ou aucun. La troisième partie du pilote appelle `driver.run` pour l'exécution des tâches définies par les variables d'environnement `JASS_FILE` et `JASS_SCRIPTS`.

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

EXEMPLE DE CODE 1-1 Flux de contrôle du pilote

```
DIR="`/bin/dirname $0`"

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
```

Cet exemple de code définit et exporte la variable d'environnement `DIR` de sorte que les pilotes reconnaissent le pilote de départ. Ensuite, la variable d'environnement `JASS_FILES` est définie comme celle contenant les fichiers copiés du répertoire `JASS_HOME_DIR/Files` sur le client. La variable d'environnement `JASS_SCRIPTS` est alors définie avec les scripts finish qui sont exécutés par le logiciel Solaris Security Toolkit. Enfin, le durcissement est exécuté en appelant le pilote `driver.run`. Une fois appelé, 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`. Il stocke les fichiers copiés sur le client JumpStart.

Ce répertoire contient les fichiers suivants :

- `/.cshrc`
- `/.profile`
- `/etc/default/sendmail`
- `/etc/dt/config/Xaccess`
- `/etc/hosts.{allow|deny}`
- `/etc/init.d/nddconfig`
- `/etc/init.d/set-tmp-permissions`
- `/etc/init.d/sms_arpconfig`
- `/etc/init.d/swapadd`
- `/etc/issue`
- `/etc/motd`
- `/etc/notrouter`
- `/etc/rc2.d/S00set-tmp-permissions`
- `/etc/rc2.d/S07set-tmp-permissions`
- `/etc/rc2.d/S70nddconfig`
- `/etc/rc2.d/S73sms_arpconfig`
- `/etc/rc2.d/S73swapadd`
- `/etc/security/audit_class`
- `/etc/security/audit_control`
- `/etc/security/audit_event`
- `/etc/sms_domain_arp`
- `/etc/sms_sc_arp`
- `/etc/syslog.conf`

Répertoire `Finish`

Ce répertoire contient les scripts finish qui introduisent les modifications et les mises à jour du système lors de l'installation. 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 le *Solaris Security Toolkit 4.1 Reference Manual*.

Répertoire `OS`

Ce répertoire contient uniquement les images du SE Solaris. Ces images sont utilisées pendant l'installation du logiciel JumpStart comme source d'installation du client et pour fournir le scripts `add_install_client` et `rm_install_client`. Le script `add_client` accepte ces noms de répertoires supplémentaires.

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

Les conventions de dénomination de fichiers d'installation sont indiquées ci-après.

Solaris, SE

Utilisez la norme de dénomination suivante pour le SE Solaris :

`Solaris_`*version os_4 chiffres de l'années_2 chiffres du mois de la version du CD-ROM*

Par exemple, le nom de répertoire pour le CD-ROM de Solaris 8 OS, daté d'avril 2001, devra être `Solaris_8_2001-04`. En séparant les mises à jour et les versions du SE Solaris, il est possible d'exercer un contrôle précis pour les tests et les déploiements.

Trusted Solaris OS

Utilisez la norme de dénomination suivante pour Trusted Solaris OS :

`Trusted_Solaris_`*version os_4 chiffres de l'années_2 chiffres du mois de la version du CD-ROM*

Par exemple, si la date de la version du logiciel Trusted Solaris était février 2000, le répertoire devra avoir le nom : `Trusted_Solaris_8_2000-02`.

Solaris OS Intel Platform Edition

Utilisez la norme de dénomination suivante pour le répertoire du SE Solaris Intel Platform Edition :

`Solaris_`*version os_4 chiffres de l'années_2 chiffres du mois de la version du CD-ROM*`_ia`

Par exemple, si la date de la version de Solaris OS Intel Platform Edition était avril 2001, le répertoire devra avoir le nom : `Solaris_8_2001-04_ia`.

Répertoire `Packages`

Ce répertoire contient les packages pouvant être installés avec un script finish. Par exemple, le package Sun Java™ System Web Server, anciennement connu sous le nom Sun™ ONE Web Server et auparavant iPlanet™ Web Server, peut être stocké dans le répertoire `Packages` de sorte que le script finish approprié puisse installer le logiciel selon les besoins.

Plusieurs scripts finish inclus dans le logiciel Solaris Security Toolkit effectuent l'installation du logiciel et des tâches de configuration de base. Les scripts qui installent le logiciel depuis le répertoire `Packages` comprennent :

- `install-fix-modes.fin`
- `install-Sun_ONE-WS.fin`
- `install-jass.fin`
- `install-md5.fin`
- `install-openssh.fin`

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 et vous évite de devoir 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, vous pouvez avoir des répertoires `2.5.1_Recommended` et `2.6_Recommended` dans le répertoire `Patches`.

Le logiciel Solaris Security Toolkit prend en charge les clusters de patchs de Solaris OS Intel Platform Edition. La convention d'attribution des noms pour ces clusters de patchs est la même que celle du service SunSolve OnLine℠.

Le format est `Solaris_<release>_x86_Recommended`. Le cluster de patchs de Solaris OS Intel Platform Edition pour Solaris 8 OS doit se trouver dans un répertoire nommé `Solaris_8_x86_Recommended`.

Répertoire `Profiles`

Ce répertoire contient tous les profils JumpStart. Ces profils renferment des informations de configuration utilisées par le logiciel JumpStart pour déterminer les clusters Solaris pour l'installation (par exemple, Core, End User, Developer ou Entire Distribution), la configuration du disque d'installation et le type d'installation (par exemple, autonome) à effectuer.

Les profils JumpStart sont listés et utilisés dans le fichier `rules` pour définir comment les systèmes spécifiques ou les groupes de systèmes sont construits.

Répertoire `Sysidcfg`

Le répertoire `Sysidcfg`, similaire au répertoire `Profiles`, contient des fichiers qui ne sont utilisés que 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 répertoire séparée.

Chaque version du SE Solaris possède son propre répertoire. Le répertoire contenant chaque version est nommé `Solaris_`*Version SE*. Le logiciel Solaris Security Toolkit contient des exemples de fichiers `sysidcfg` pour les versions 2.5.1 à 9 du SE Solaris.

Les exemples de fichiers `sysidcfg` peuvent être étendus à d'autres types de fichiers (par ex. par réseau, hôte, etc.). Le logiciel Solaris Security Toolkit prend en charge des 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

Le référentiel de données est une variable d'environnement dans le répertoire `JASS_REPOSITORY` qui prend en charge les annulations Solaris Security Toolkit, enregistre les données relatives à chaque exécution, maintient un ensemble de fichiers modifiés par le logiciel et enregistre les données pour le journal d'exécution. La fonction d'annulation se base sur les informations enregistrées sans le référentiel de données.

Maintien du contrôle de version

Il est vital de garder le contrôle de la version pour tous les fichiers et scripts utilisés par le logiciel Solaris Security Toolkit pour deux raisons. D'abord, l'un des objectifs de cet environnement est de pouvoir recréer une installation du système. Cet objectif serait impossible sans un instantané de toutes les versions de fichiers utilisées pendant une installation. Ensuite, vu que ces scripts remplissent des fonctions de sécurité—ce qui est un facteur critique pour de nombreuses entreprises—, il faut faire extrêmement attention à n'implémenter que des modifications appropriées et testées.

Un package de contrôle de version Source Code Control System (SCCS) est inclus dans le package Solaris OS `SUNWsprot`. Vous pouvez utiliser un autre logiciel de contrôle de version disponible en freeware ou en vente dans le commerce pour gérer les informations relatives à la version. Quel que soit le produit de contrôle de version utilisé, établissez une procédure de gestion des mises à jour et capturez les informations de la version pour toute nouvelle création future éventuelle.

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 peuvent ne pas avoir recours au système de contrôle de version, ils ne peuvent pas facilement éviter d'utiliser 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, parce que les bases de données locales pourraient être modifiées par malveillance.

Exécution de versions de Solaris OS prises en charge

Le support du logiciel Solaris Security Toolkit est assuré par Sun uniquement dans le cadre des systèmes d'exploitation Solaris 8 et Solaris 9. Bien que le logiciel fonctionne sur les systèmes d'exploitation Solaris 2.5.1, Solaris 2.6 et Solaris 7, le support Sun est uniquement disponible pour les systèmes d'exploitation susmentionnés.

Le logiciel Solaris Security Toolkit détecte automatiquement la version du système d'exploitation Solaris installée, puis exécute les tâches adaptées à cette version.

Exécution des versions de SMS prises en charge

Si vous disposez de System Management Services (SMS) pour gérer votre contrôleur système (SC), le support Sun est disponible pour le logiciel Solaris Security Toolkit 4.1 à condition que vous utilisiez les versions 1.3 à 1.4.1 de SMS.

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 implémentent toutes les indications de sécurité dans 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 les articles Sun BluePrints OnLine concernant la sécurité. Ces paramètres ne conviennent pas à tous les systèmes ; vous devez donc personnaliser le logiciel Solaris Security Toolkit pour remplir les conditions de sécurité requises pour 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. 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 modèles de fichiers.

La plupart des utilisateurs n'ont pas besoin de modifier le code de Solaris Security Toolkit. Toute modification pourrait avoir des conséquences négatives sur les prises en charge et les mises à jour. S'il est absolument nécessaire de modifier le code pour utiliser le logiciel Solaris Security Toolkit dans votre environnement, copiez ce code vers un fichier unique ou un nom de fonction, afin de pouvoir ensuite retrouver facilement les modifications (voir « Instructions générales », page 14).

Vous trouverez tout au long de ce document des indications et des instructions pour la personnalisation du logiciel Security Toolkit. Vous trouverez des informations utiles sur la personnalisation des pilotes dans le manuel le *Solaris Security Toolkit 4.1 Reference Manual*. La personnalisation comporte la modification et la création de fichiers et de variables.

Les chapitres suivants donnent 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 bonne planification pour obtenir un résultat conforme aux attentes de votre entreprise et s'assurer que la configuration de la plate-forme est correcte.

En phase de planification, veillez à recueillir le maximum de données, y compris sur les politiques et les normes de sécurité, les réglementations et normes industrielles ainsi que les pratiques préférées des vendeurs.

En plus de ces informations, il est essentiel d'examiner les conditions de fonctionnement et d'application de manière à s'assurer que la configuration résultante n'aura aucune conséquence négative sur la capacité de la plate-forme à remplir les fonctions commerciales prévues.

Instructions générales

Pour la personnalisation du logiciel Solaris Security Toolkit, respectez les instructions générales suivantes. La compréhension et le respect de ces instructions 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 d'origine empêchera toute évolution vers les versions supérieures du logiciel Solaris Security Toolkit, étant donné que les changements seront écrasés par les nouvelles versions de fichiers. (Tous les changements de personnalisation seraient perdus et la configuration de votre système pourrait 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 y a toutefois trois exceptions à ces instructions : les fichiers `sysidcfg`, les modèles dans le répertoire Files et à chaque indication contraire dans les articles Sun BluePrints OnLine.

- Donnez 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 ou d'un type d'application constitue un excellent système d'attribution de nom. Le TABLEAU 1-1 donne plusieurs exemples de noms standard.

TABLEAU 1-1 Normes d'attribution de noms pour les fichiers personnalisés

Fichier personnalisé	Norme de dénomination
`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.

- Si nécessaire, modifiez les fichiers originaux suivants. Ces fichiers sont les *seuls* fichiers originaux de Solaris Security Toolkit que vous pouvez modifier directement.

`Sysidcfg/*/sysidcfg`	Utilisé pour la configuration automatique JumpStart.
`Files/*`	Utilisés comme modèles de fichiers et copiés sur les systèmes.

Remarque – Sachez que si vous supprimez `SUNWjass` à l'aide de la commande `pkgrm`, les fichiers `user.init` et `user.run`, s'ils existent, ne seront pas supprimés. Ce comportement a lieu pour tous les fichiers du client qui sont ajoutés à la structure du répertoire Solaris Security Toolkit et qui ne sont pas inclus dans la distribution. Les fichiers dans le répertoire Files inclus dans la distribution de Solaris Security Toolkit et les fichiers`sysidcfg` existent et seront donc supprimés.

CHAPITRE 2

Sécurisation de systèmes : application d'une méthodologie

Ce chapitre décrit une méthodologie pour la sécurisation de systèmes. Il propose une méthode à appliquer avant de sécuriser des systèmes à l'aide du logiciel Solaris Security Toolkit.

Ce chapitre traite des points suivants :

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, basé sur les stratégies et les normes de sécurité de l'entreprise, ainsi que sur les conditions de fonctionnement et d'application du système. Cette phase comprend les tâches suivantes :

Même si elles ne sont pas décrites dans cet ouvrage, il est bon de faire certaines considérations sur la compréhension des risques, la maîtrise de l'infrastructure et de ses besoins en matière de sécurité, l'imputabilité, le logging et l'audit de l'usage.

Prise en compte des risques et des avantages

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

Pour le durcissement de systèmes, vous devez prendre certaines précautions afin d'assurer le fonctionnement du système après l'implémentation du logiciel Solaris Security Toolkit. De plus, il est important d'optimiser la procédure pour limiter au minimum les temps d'arrêt.

Remarque – Lors de la sécurisation d'un système déployé, il est parfois plus rapide et efficace de reconstruire le système, de le durcir au moment de l'installation puis de recharger tout le logiciel nécessaire au fonctionnement.

---

1. Description des besoins des services et des applications sur le système.

   Vous devez identifier les services et les applications exécutés sur un système avant d'exécuter le logiciel Solaris Security Toolkit. Toutes 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 l'implémentation 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. Selon l'importance vitale du système, les services qu'il fournit et la disponibilité d'une fenêtre de maintenance, l'implémentation 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 arrêt de l'activité par rapport aux risques encourus si la sécurité n'est pas augmentée.

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

   Dans la mesure du possible, effectuez toutes les modifications sur des systèmes hors production avant d'implémenter les systèmes dans une configuration stratégique. Ceci n'est pas toujours possible ; 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'installation du logiciel Solaris Security Toolkit. Des dépendances non identifiées nécessitant un dépannage après le durcissement 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.

En cas de problèmes de fonctionnement après l'installation du logiciel Solaris Security Toolkit, il peut être 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 supporter et d'activer les fonctionnalités manquantes.

4. La sécurisation d'une plate-forme ne se limite pas au durcissement et à la réduction.

   Si vous envisagez la mise à niveau de la configuration de votre système pour améliorer sa sécurité, il est essentiel de comprendre que le durcissement et la réduction d'une plate-forme ne représente qu'une fraction des tâches nécessaires à la sécurisation d'un système, de services et de données. Ce document ne traite pas des mesures et contrôles additionnels ; il est toutefois conseillé de considérer des questions telles que la gestion des comptes, la gestion des privilèges, l'intégrité des systèmes de fichiers et des données, les contrôles d'accès basés sur les hôtes, la détection des intrusions, l'exploration et l'analyse de la vulnérabilité et la sécurité des applications.

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

   La plate-forme en cours de durcissement pourrait déjà avoir fait l'objet d'une attaque. Le logiciel Solaris Security Toolkit a probablement été implémenté trop tard pour assurer une protection contre les vulnérabilités exploitables. Dans ce cas, réinstallez le système puis installez et utilisez le logiciel Solaris Security Toolkit pour le sécuriser.

Vérification de la stratégie, des normes et de la documentation en matière de sécurité

Le premier pas pour la sécurisation d'un système est la compréhension des principales stratégies de sécurité, des normes et des documents de référence adoptés par votre entreprise en matière de sécurité de plate-forme. Déterminez le profil de Solaris Security Toolkit à partir de ces documents, qui décrivent les besoins et les mesures à mettre en oeuvre pour tous les systèmes de votre entreprise. Si votre entreprise ne dispose pas de documentation, sa préparation augmentera votre capacité à personnaliser le logiciel Solaris Security Toolkit (SST).

Remarque – Lorsque vous recherchez ces documents, n'oubliez pas que vous pouvez trouver du matériel dans les exercices pratiques ou autre documentation.

Pour de plus amples informations sur les stratégies en matière de sécurité, reportez-vous à l'article Sun BluePrints OnLine « Developing a Security Policy ». Ce document vous permettra de mieux comprendre le rôle des stratégies de sécurité à l'échelle de l'entreprise.

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

Exemple 1

- **Stratégie** – Une entreprise doit utiliser des protocoles de gestion qui prennent en charge une puissante authentification des utilisateurs et le chiffrement des données transmises.
- **Impact sur le profil**– Les protocoles utilisant un texte en clair, tels que Telnet, FTP, SNMPv1 et autres, ne doivent pas être utilisés. Par défaut, le 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 supporter une authentification et un chiffrement plus puissant en utilisant des extensions telles que Kerberos. Ces services sont toutefois cités à titre d'exemple parce que leurs configurations par défaut ne supportent pas ces niveaux de sécurité supplémentaires.

Exemple 2

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

Impact du profil – Le logiciel Solaris Security Toolkit peut être configuré pour permettre le vieillissement du mot de passe. Par défaut, le logiciel Solaris Security Toolkit accepte les mots de passe pendant une période maximale de 8 semaines (56 jours). Pour se conformer à la stratégie, il faut changer le profil du logiciel Solaris Security Toolkit. Reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

Même si, par défaut, le logiciel Solaris Security Toolkit permet le vieillissement du mot de passe lorsqu'il est exécuté sur un système, cette modification n'affecte pas les utilisateurs existants. Pour permettre le vieillissement du mot de passe des utilisateurs existants, utilisez la commande `passwd`(1) sur chaque compte utilisateur.

Détermination des besoins de l'application et du service

Cette tâche permet d'assurer que les services restent fonctionnels après le durcissement du système. Cette tâche comprend les étapes suivantes :

- « Inventaire des applications et des services opérationnels », page 21
- « Détermination des besoins du service », page 21

Inventaire des applications et des services opérationnels

Inventaire des applications, services et fonctions opérationnelles ou de gestion. Cet inventaire est nécessaire pour déterminer quel logiciel est 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 logiciels installés sur les systèmes doivent autant que possible être réduits au minimum. En effet, les logiciels non utilisés pour la prise en charge d'une fonction de l'entreprise ne doivent pas être installés. Les applications inutiles augmentent d'autant les failles du système et donc ses vulnérabilités exploitables. Par ailleurs, davantage de logiciels sur un système équivaut généralement à davantage de patchs à appliquer. Pour de plus amples informations sur la réduction du SE Solaris, reportez-vous à l'article Sun BluePrints OnLine « Minimizing the Solaris Operating Environment for Security ».

Lors de l'inventaire des logiciels, pensez 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 besoins du service

Après avoir terminé un inventaire des applications et des services, déterminez si des composants quelconques ont des dépendances qui pourraient avoir une incidence sur le durcissement. De nombreuses applications tierce partie n'utilisent pas directement les services fournis par le SE Solaris. Vous trouverez, dans les sections qui suivent, des informations utiles sur ces applications.

- « Bibliothèques partagées », page 21
- « Fichiers de configuration », page 24
- « Structures des services », page 25

Bibliothèques partagées

Il est important de comprendre quelles bibliothèques sont nécessaires pour la prise en charge d'une application. Ceci est surtout utile en cas de débogage, mais l'est également pour la préparation d'un système avant son durcissement. Si vous ne connaissez pas l'état d'un système, recueillez autant d'informations que possible de manière à bien comprendre certains faits, tels que les dépendances logicielles.

Pour déterminer quelles bibliothèques sont utilisées par une application, vous avez le choix entre trois méthodes, selon la version du SE Solaris installée :

- La première s'utilise contre un objet système de fichiers (par exemple, binaire d'application).
- La seconde s'utilise pendant l'analyse d'une application en cours d'exécution.
- La troisième s'utilise pour le suivi d'un programme à son démarrage.

Prenons un exemple : détermination des bibliothèques nécessaires au support du logiciel d'un serveur DNS.

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

EXEMPLE DE CODE 2-1 Collecte d'informations sur les objets 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
```

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

EXEMPLE DE CODE 2-2 Collecte d'informations depuis 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
```

La commande `pldd` montre les bibliothèques partagées qui sont chargées de manière dynamique par l'application, en plus des bibliothèques par rapport auxquelles est reliée l'application. Cette information peut également être obtenue en utilisant 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
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. En utilisant la valeur renvoyée, il est clair que l'appel système réussit à trouver et ouvrir la librairie partagée.

Après avoir pris connaissance des bibliothèques partagées, utilisez la commande suivante pour savoir à quels packages du SE Solaris 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 réduction 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 durci du fait que les fichiers de configuration peuvent être renommés ou supprimés pour désactiver des services. Pour plus d'informations, reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

Pour savoir 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 Déterminer l'état d'utilisation d'un fichier de configuration

```
# 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("/etc/services", 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 y ait un problème. Une documentation attentive des résultats avant et après le durcissement peut contribuer à l'accélération de l'ensemble du processus de validation.

Structures des services

Cette catégorie comprend des structures ou des métaservices sur lesquels sont construites des applications plus grosses et plus complexes. Les structures types appartenant à cette catégorie sont les services d'attribution de noms (par exemple, NIS, NIS+ et LDAP), les services d'authentification (par exemple, Kerberos et LDAP) et des services tels que le portmapper utilisé par les RPC.

On ne sait pas toujours avec précision quand une application dépend de ces types de services. Lorsque des ajustements particuliers sont nécessaires pour configurer une application, par exemple lorsqu'il faut l'ajouter à un domaine Kerberos, on connaît parfaitement la dépendance. Dans certains cas, les dépendances des applications ne nécessitent aucune tâche supplémentaire ce qui fait que la dépendance actuelle peut ne pas être documentée par le vendeur.

Le RPC portmapper en est un exemple type. Par défaut, le logiciel Solaris Security Toolkit désactive le RPC portmapper. Cette opération peut donner lieu à des comportements inattendus dans d'autres services reposant sur ce service. D'après les expériences passées, l'abandon, l'interruption ou l'échec des services dépend de la qualité d'écriture du code de l'application pour gérer les exceptions. Pour savoir si une application utilise le RPC portmapper, utilisez la commande `rpcinfo`. Par exemple :

EXEMPLE DE CODE 2-5 Identification des applications utilisant le 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` et/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.

Par exemple, prenons la commande `rusers`. Cette commande repose sur le service RPC portmapper. Si le RPC portmapper n'est pas en cours d'exécution, il semble que la commande `rusers` s'interrompt. 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 RPC portmapper depuis `/etc/init.d/rpc`, le programme renvoie immédiatement son résultat.

Comme autre exemple, prenons le cas où le service RPC portmapper 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>
```

Vu 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. Cette hypothèse est validée en regardant 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 uniquement disponible sur les SE Solaris versions 7 à 9. 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 d'utiliser 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, avec le nom de fichier, que ce service repose sur le RPC portmapper.

En plus du RPC portmapper, les applications peuvent également reposer sur d'autres services OS courants, tels que FTP, SNMP ou 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 donnée 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 on ne sait pas quels ports appartiennent à quels services ou quelles applications. Pour le savoir, on peut inspecter les processus à l'aide de la commande `pfiles` (disponible sur les SE Solaris versions 8 et 9).

EXEMPLE DE CODE 2-8 Identification des ports appartenant aux services ou applications

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

Ces dépendances peuvent être déterminées plus efficacement en utilisant la commande `lsof` (pour obtenir la liste des fichiers ouverts). Cette commande permet de savoir quels processus utilisent quels fichiers et quels ports. Par exemple, pour savoir quels processus de l'exemple précédent utilisent le port 35047, lancez la commande suivante.

EXEMPLE DE CODE 2-9 Identification des processus utilisant 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`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`.

Vous pouvez télécharger le programme `lsof` depuis l'adresse :

`ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/`

Remarque – Il peut arriver que les méthodes décrites pour la détermination des dépendances ne trouvent pas les éléments qui sont rarement utilisés. En plus de l'utilisation de ces méthodes, consultez la documentation et la documentation du fournisseur.

Développement et implémentation d'un profil Solaris Security Toolkit

Une fois la phase de planification et de préparation terminée, développez et implémentez un profil de sécurité. Un profil de sécurité consiste en un pilote de durcissement comme, par exemple, *nom*-`hardening.driver`, et tous les pilotes, scripts et fichiers nécessaires pour l'implémentation des stratégies de sécurité spécifiques à votre site.

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

Pour personnaliser le logiciel Solaris Security Toolkit, 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.

Vous trouverez de plus amples informations dans les chapitres suivants :

- Pour des directives importantes sur la personnalisation du logiciel, reportez-vous au Chapitre 1, « Configuration et personnalisation du logiciel Solaris Security Toolkit », page 13.
- Pour un exemple de création de profil de sécurité, consultez le Chapitre 7, « Création d'un profil de sécurité », page 96.
- Pour plus d'informations sur la personnalisation des pilotes, reportez-vous au manuel *Solaris Security Toolkit 4.1 Reference Manual*.

  Si nécessaire, consultez les chapitres relatifs aux scripts, aux fonctions de structure, aux variables d'environnement et aux fichiers du *Solaris Security Toolkit 4.1 Reference Manual*. Parmi les variables d'environnement, vous pouvez vouloir personnaliser `JASS_FILES` et `JASS_SCRIPTS`.

Pour l'application de normes communes à la majorité des plates-formes, tout en préservant des différentes spécifiques à chaque plate-forme, utilisez une technique connue comme profils de sécurité imbriqués ou hiérarchiques. Pour plus d'informations, reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*. Comparez le profil de sécurité résultant des stratégies, normes et besoins de votre entreprise pour éviter que des modifications ne soient 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, consultez le 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 durcissement, mais sur les tâches qui précèdent et suivent l'installation.

Exécution des tâches de préinstallation

Avant le durcissement d'un système déployé, vous devez étudier et planifier deux tâches importantes—sauvegarde et vérification. Ces tâches facilitent la détermination de l'état du système déployé et la résolution des problèmes de configuration pouvant se poser avant le durcissement du système.

Sauvegarde des données

Cette tâche est centrée sur la planification prévisionnelle. 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 sauvegarder le système, vous assurer que la copie de sauvegarde peut être lue et confirmer que son contenu peut être récupéré. Cette opération doit être accomplie 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 l'implémentation de modifications de configuration, telles que les modifications introduites par le processus de durcissement. Ce processus de vérification comporte une réinitialisation suivie de tests positifs des applications ou services. Bien qu'il soit préférable d'avoir un programme de test et d'acceptation bien défini, la documentation peut ne pas être toujours disponible. Dans ce cas, testez raisonnablement le système en fonction de son type d'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'affiche à l'initialisation du système ou au démarrage d'une application. Si vous n'arrivez 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 durcissement. Lorsque vous examinez les fichiers journaux, n'oubliez pas d'inclure les journaux de système, service et application 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'anomalies inconnues (toutes les erreurs ou anomalies connues sont documentées). Le système doit redémarrer dans un état connu et stable. Au cours d'une vérification, si vous découvrez que les configurations en cours d'utilisation et stockées ne sont pas les mêmes, réévaluez les stratégies et processus de contrôle des changements de votre entreprise pour identifier le problème à l'origine de cette situation.

Exécution des tâches suivant l'installation

Les tâches suivant l'installation sont un prolongement des tâches préalables à l'installation. Leur objectif est d'assurer que le processus de durcissement 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 le durcissement et la réinitialisation doivent être similaires à ceux qui avaient été collectés avant le durcissement 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, parce que certaines applications pourraient rencontrer des problèmes sans consigner de messages dans le fichier journal. Consultez la section suivante pour des informations détaillées sur la vérification.

Vérification du fonctionnement 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 implémenté en conformité avec les stratégies de l'entreprise en matière de sécurité. Effectuez cette tâche avec soin et immédiatement après la réinitialisation de la plate-forme durcie, 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 du fonctionnement 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 et sans erreurs, examinez le fichier journal de l'installation. Ce fichier est installé dans `JASS_REPOSITORY/jass-install-log.txt`.

Remarque – Examinez ce fichier journal pour comprendre ce que le logiciel Solaris Security Toolkit a fait au système. Pour chaque exécution sur le système, un nouveau fichier journal est enregistré dans un répertoire en fonction de l'heure 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 pour automatiser le processus.

Vérification du fonctionnement des applications et des services

Pour vérifier les applications et les services du processus, lancer un plan de test et d'acceptation. Il teste les différents composants d'un système ou d'une application et s'assure de leur disponibilité et de leur bon état de marche. En l'absence d'un tel plan, testez raisonnablement le système en vous basant sur la manière dont il est utilisé. L'objectif est de s'assurer que le durcissement n'a pas altéré le fonctionnement des applications ou services.

Si vous découvrez qu'une application ou un service ne fonctionne pas correctement après le durcissement du système, recherchez la cause du problème en examinant les fichiers journaux de cette application. 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

Une erreur commune à de nombreuse entreprises est de considérer la sécurité qu'au moment de l'installation, et d'y revenir 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 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. Par exemple, les failles du systèmes deviennent connues. Les indications ci-après vous serviront de guide pour la maintenance de la sécurité.

- Les patchs du SE Solaris peuvent installer des packages supplémentaires et écraser des fichiers de configuration de votre système. Vérifiez le niveau de sécurité de votre système avant d'installer un patch quelconque. Il est également important que toujours maintenir vos systèmes à jour en applications les patchs les plus récents.

  Le logiciel Solaris Security Toolkit peut vous assister lors de l'application de patchs, parce qu'il supports les exécution répétées sur un système de sorte que vous pouvez sécuriser le système après l'application de patchs. Exécutez le logiciel après l'installation de chaque patch, en utilisant les pilotes appropriés, pour toujours assurer la cohérence de votre configuration avec vos stratégies en matière de sécurité. Effectuez également un examen manuel du système, parce que la version de Solaris Security Toolkit utilisée pourrait ne pas prendre en charge les nouvelles fonctionnalités ajoutées par les patchs installés.
- Contrôlez le système à intervalles réguliers pour éviter l'apparition de comportements anormaux. Vérifiez les comptes du système, les mots de passe et les types d'accès ; il peuvent vous apporter de précieuses informations sur ce qui ce passe dans 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 collectant et examinant ces journaux.
- Instituez une puissante stratégie d'audit et de lutte contre la vulnérabilité pour le contrôle et la maintenance des configurations du système. Cette stratégie joue un rôle fondamental pour assurer aux systèmes des configurations sûres avec le temps.

- Mettez périodiquement vos systèmes à jour en installant la dernière version du logiciel Solaris Security Toolkit.

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

CHAPITRE 3

Installation et exécution du logiciel de sécurité

Ce chapitre explique comment télécharger, installer et exécuter le logiciel Solaris Security Toolkit et d'autres logiciels ayant trait à la sécurisation. Il explique également comment configurer votre environnement en mode autonome ou JumpStart et comment bénéficier d'un support technique.

Suivez les instructions contenues dans cette section pour installer, configurer et exécuter le logiciel. Ces instructions comprennent le téléchargement de composants logiciels complémentaires, d'exemples utiles et de directives.

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

Cette section décrit les tâches suivantes :

Exécution des tâches de planification et de préinstallation

Une bonne planification est essentielle à la réussite de la sécurisation de systèmes à l'aide du logiciel Solaris Security Toolkit. Avant d'installer le logiciel, consultez le Chapitre 2 qui fournit des informations détaillées sur la planification.

Si vous installez le logiciel sur un système déployé, reportez-vous à la section « Exécution des tâches de préinstallation », page 30, qui contient une description des tâches à effectuer avant l'installation sur les systèmes déployés.

Dépendances

Le logiciel Solaris Security Toolkit 4.1 dispose de peu de dépendances.

Dépendances matérielles

Reportez-vous à la section « Exécution de versions de Solaris OS prises en charge », page 12 pour de plus amples informations sur les versions du système d'exploitation Solaris prises en charge.

Dépendances logicielles

Le logiciel Solaris Security Toolkit 4.1 dépend du package SUNWloc. L'absence de ce package entraîne l'échec de Solaris Security Toolkit.

Reportez-vous à la section « Exécution des versions de SMS prises en charge », page 13 pour de plus amples informations sur les versions du logiciel System Managements Services (SMS) prises en charge.

Détermination du mode à utiliser

Durcissez les systèmes pendant ou immédiatement après leur installation, afin de limiter leur durée d'exposition aux attaques sans être sécurisés. 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 pour utiliser JumpStart ultérieurement. Si vous utilisez JumpStart, vous bénéficiez des capacités du logiciel Solaris Security Toolkit de s'intégrer dans les architectures JumpStart existantes.

Les sections suivantes décrivent les modes autonome et JumpStart.

Mode autonome

Le logiciel Solaris Security Toolkit se lance directement depuis 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 pour la réinstallation du système d'exploitation à partir du fichier de travail. Toutefois, pour sécuriser les systèmes, ils doivent si possible être réinstallés à partir du fichier de travail.

Le mode autonome est particulièrement utile pour le durcissement de systèmes après l'installation de patchs. Vous pouvez exécuter plusieurs fois le logiciel Solaris Security Toolkit sur un système sans aucun risque. Les patchs peuvent écraser ou modifier des fichiers qui avaient été modifiés par Solaris Security Toolkit ; en réexécutant le logiciel Solaris Security Toolkit, vous pouvez réimplémenter les modifications de sécurité qui ont été changées 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 est l'une des meilleures options et des plus rapides pour le durcissement d'un système déployé. Aucune opération spéciale n'est requise pour intégrer le logiciel Solaris Security Toolkit dans une architecture sans JumpStart, à part les opérations décrites au point « Téléchargement des packages de sécurité », page 38 relatives aux 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 de 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*.

Pour une utilisation dans un environnement JumpStart, copiez la source Solaris Security Toolkit dans `JASS_HOME_DIR` (pour les téléchargements au format`tar`) ou `/opt/SUNWjass` (pour les téléchargements au format `pkg`) contenus dans le répertoire de base du serveur JumpStart. Le répertoire par défaut est `/jumpstart` sur le serveur JumpStart. `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 savoir comment configurer un serveur JumpStart.

Téléchargement des packages de sécurité

Pour le durcissement d'un système, il faut d'abord télécharger les packages de sécurité complémentaires sur le système que vous souhaitez 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 MD5 sont essentiels. Au lieu d'OpenSSH, vous pouvez utiliser une version commerciale de shell sécurisé, disponible dans de nombreux points de vente. Installez et utilisez un shell sécurisé sur tous les systèmes. Avec Solaris 9 OS, utilisez la version de shell sécurisé inclue.

Téléchargement du logiciel Solaris Security Toolkit

Téléchargez d'abord le logiciel Solaris Security Toolkit, puis installez-le sur le serveur où vous entendez utiliser Solaris Security Toolkit 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 depuis le 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. Si vous installez le logiciel Solaris Security Toolkit à partir de l'archive `tar`, `JASS_HOME_DIR` est défini pour être le chemin jusqu'à `jass-`*n.n* compris. Si vous installez la version `tar` de la distribution dans le répertoire `/opt`, la variable d'environnement `JASS_HOME_DIR` est définie comme `/opt/jass-`*n.n*.

Le logiciel Solaris Security Toolkit est distribué au format de package du SE Solaris, en plus du format traditionnel de l'archive `tar` compressée. Le même logiciel est inclus dans les deux archives.

Choisissez le format le plus approprié à votre situation. Le format `pkg` convient le mieux pour les clients, tandis que`tar` est plus approprié pour les systèmes JumpStart et pour le développement de packages personnalisés.

Les sections qui suivent contiennent une description des procédures à suivre pour le téléchargement et l'installation de deux types différents d'archives.

▼ Téléchargement de la version `tar`

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

   Le fichier source est disponible sur le site Web suivant :

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

2. **Extrayez le fichier de distribution du logiciel dans un répertoire sur le serveur en utilisant les commandes** `zcat` **et** `tar` **comme illustré**:

```
# zcat jass-n.n.tar.Z | tar xvf -
```

   Où *n.n* est la version téléchargée la plus récente.

   L'exécution de cette commande crée le sous-répertoire `jass-`*n.n* dans le répertoire de travail courant. Ce sous-répertoire contient tous les répertoires Solaris Security Toolkit et les fichiers associés.

▼ Téléchargement de la version `pkg`

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

   Le fichier source se trouve à l'adresse :

   `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.Z
```

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

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

   Où *n.n* est 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 d'assurer l'installation de la dernière version du cluster de patchs recommandés et de sécurité pour le SE Solaris, cette section décrit comment télécharger le 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.

▼ Téléchargement d'un cluster de patchs recommandé

Avant d'installer un cluster de patchs, lisez les fichiers README qui accompagne chaque patch et toute autre documentation fournie. Ces documents contiennent souvent des conseils et des informations utiles avant d'installer un cluster de patchs.

1. **Téléchargez le dernier cluster de patchs depuis le site Web SunSolve OnLine à :**

   `http://sunsolve.sun.com`

2. **Cliquez sur le lien Patches en haut de la barre de navigation de gauche.**
3. **Cliquez sur le lien Recommended Patch Clusters.**

   Le contrat de licence s'affiche.

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

   Dans notre exemple, nous sélectionnons Solaris 8 OS.

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

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

6. **Enregistrez le fichier sur votre ordinateur.**
7. **Déplacez le fichier en toute sécurité sur le système en cours de durcissement.**

   Exécutez la commande `scp` (`scp(1)` – secure copy (programme de copie à distance)) ou utilisez toute autre méthode offrant un transfert de fichiers sécurisé.

   Utilisez la commande `scp` comme suit :

```
# scp 8_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 dans lequel le fichier a été enregistré/8_Recommended.zip.
# unzip 8_Recommended.zip
Archive:     8_Recommended.zip
  creating:  8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

Le cluster de patchs s'installera automatiquement une fois que vous aurez 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 package FixModes

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

Remarque – Avec la version Solaris 9 OS, des modifications ont été effectuées pour augmenter les autorisations d'objets précédemment altérés par le package FixModes. Toutefois, FixModes est encore nécessaire parce qu'il est nécessaire de renforcer les autorisations des fichiers et répertoires avec des logiciel tiers et non fourni en standard.

▼ Téléchargement de logiciels FixModes

1. **Téléchargez les fichiers binaires précompilés de FixModes depuis :**

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

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

2. **Déplacez le fichier en toute sécurité sur le système en cours de durcissement à l'aide de la commande `scp` ou en utilisant une autre méthode garantissant un transfert sûr du fichier.**

   Utilisez la commande `scp` comme suit :

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

3. **Décompressez et enregistrez le fichier intitulé** `SUNBEfixm.pkg.Z` **dans le répertoire** `Packages` **de Solaris Security Toolkit** `/opt/SUNWjass/Packages`**, avec les commandes suivantes :**

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

Le cluster de patchs s'installera automatiquement quand vous aurez téléchargé les autres packages de sécurité et exécuté le logiciel Solaris Security Toolkit.

Téléchargement du package OpenSSH

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

L'outil le plus souvent utilisé pour l'implémentation du chiffrement est le shell sécurisé, en version intégrée dans le SE Solaris, en version commerciale de tiers ou en version freeware. Pour implémenter toutes les modifications de sécurité introduites par le logiciel Solaris Security Toolkit, vous devez inclure un shell sécurisé.

Remarque – Avec Solaris 9 OS, utilisez la version du shell sécurisé fournie avec le logiciel. Cette version de shell sécurisé s'intègre à d'autres fonctions de sécurité du SE Solaris, telles que le Basic Security Module (BSM) ainsi que son support par le service d'assistance de Sun.

Pour savoir où obtenir des versions commerciales du shell sécurisé, reportez-vous à la section « Ressources connexes », page xx.

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

Le shell sécurisé vous permet d'accéder au système comme vous le feriez en utilisant Telnet et FTP.

▼ Téléchargement du logiciel OpenSSH

Remarque – Si le serveur exécute Solaris 9 OS, vous pouvez utiliser le shell sécurisé intégré et sauter les étapes d'installation d'OpenSSH décrites dans cette section.

- **Recherchez l'article Sun BluePrints OnLine et suivez les instructions qu'il contient pour télécharger le logiciel.**

  Un article Sun BluePrints OnLine expliquant comment compiler et déployer OpenSSH et intitulé « Building and Deploying OpenSSH on the Solaris Operating Environment » est disponible à l'adresse :

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

  Vous pouvez également acheter en librairie l'ouvrage Sun BluePrint *Secure Shell in the Enterprise*.

  OpenSSH s'installera automatiquement quand vous aurez téléchargé les autres packages de sécurité et exécuté le logiciel Solaris Security Toolkit.

Attention – Ne compilez pas OpenSSH sur le système en cours de durcissement et n'installez par les compilateurs sur le système en cours de durcissement. Pour compiler OpenSSH, utilisez un système SE Solaris distinct, exécutant la même version de Solaris, la même architecture et le même mode (par exemple, Solaris 8 OS, Sun4U (`sun4u`) et 64 bits). Si vous implémentez une version commerciale de SSH, aucune compilation n'est requise. L'objectif est de limiter la disponibilité des compilateurs à des intrus potentiels. Toutefois, s'abstenir d'installer des compilateurs sur un système local ne constitue pas une protection significative contre certains piirates informatiques 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 durcissement. Générez les empreintes digitales numériques, puis comparez-les avec ce que Sun indique comme correct dans ses publications afin de détecter les fichiers binaires du système altérés ou *attaqués par un cheval de Troie* (caché à l'intérieur de quelque chose apparemment sûr) par des utilisateurs non autorisés. En modifiant les fichiers binaires du système, les attaquants ouvrent une porte dérobée sur le système cible ; ils cachent leur présence et pourraient causer des instabilités dans le système.

▼ Téléchargement de MD5

1. **Téléchargez les fichiers binaires de MD5 depuis le site Web suivant :**

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

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

2. **Déplacez le fichier** `SUNBEmd5.pkg.Z` **en toute sécurité sur le système en cours de durcissement à l'aide de la commande** `scp` **ou en utilisant une autre méthode garantissant un transfert sûr du fichier.**

   Utilisez la commande `scp` comme suit :

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

3. **Décompressez et déplacez le fichier dans le répertoire** `Packages` **de Solaris Security Toolkit situé au sein du répertoire** `/opt/SUNWjass/Packages`**, à l'aide d'une commande de ce type :**

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

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

   Après l'installation des fichiers binaires MD5, vous pouvez les utiliser pour vérifier l'intégrité des exécutables sur le système au moyen de la base de données d'empreintes digitales de Solaris. Vous trouverez de plus amples informations sur celle-ci dans l'article Sun BluePrints OnLine intitulé « The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files ».

4. **(Facultatif) Téléchargez et installez Solaris Fingerprint Database Companion et Solaris Fingerprint Database Sidekick depuis le site Web Sun BluePrint à :**

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

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

   Vous pouvez télécharger ces outils et leurs instructions depuis l'article Sun BluePrints OnLine 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 composants logiciels de sécurité supplémentaires, validez leur intégrité à l'aide des sommes de contrôle de 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. Comme mentionné dans le chapitre précédent, le profil de sécurité par défaut et les modifications apportées par ces pilotes peuvent ne pas être appropriés pour vos systèmes. Les profils de sécurité implémentés par ces pilotes désactivent les services non requis et activent les fonctions de sécurité optionnelles qui sont désactivées par défaut.

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 directives pour la personnalisation des profils de sécurité dans le manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

Installation et exécution du logiciel

Il est important de compléter les tâches préliminaires avant l'exécution du logiciel Solaris Security Toolkit. Une grande partie du durcissement est effectuée automatiquement quand vous exécutez le logiciel Solaris Security Toolkit.

- Téléchargez le logiciel de sécurité supplémentaire et le logiciel Solaris Security Toolkit sur le système que vous souhaitez durcir ou sur le serveur JumpStart. Reportez-vous à la section « Téléchargement des packages de sécurité », page 38.
- Configurez votre système pour le mode autonome ou JumpStart. Reportez-vous à la section « Détermination du mode à utiliser », page 37.
- Le cas échéant, personnalisez Solaris Security Toolkit pour votre environnement.
- Avant l'installation et l'exécution de Solaris Security Toolkit et des composants logiciels de sécurité supplémentaires, validez leur intégrité à l'aide des sommes de contrôle de MD5.

Vous pouvez lancer le logiciel Solaris Security Toolkit directement depuis la ligne de commande ou depuis un serveur JumpStart.

Pour les options de ligne de commande et d'autres informations sur l'exécution du logiciel, reportez-vous à l'un des points suivants :

- « Exécution du logiciel en mode autonome », page 47
- « Exécution du logiciel en mode JumpStart », page 55

Exécution du logiciel en mode autonome

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

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

```
# ./jass-execute -h

usage:

Pour appliquer ce Toolkit (cette boîte à outils) à un système à
l'aide de la syntaxe :
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente de Toolkit sur un système :
   jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

Pour vérifier si un système est conforme à un profil prédéfini :
   jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
      [ -m e-mail_address ]

Pour afficher l'historique des applications de Toolkit sur un
système :
   jass-execute -H

Pour afficher la dernière application de Toolkit sur un système :
   jass-execute -l

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

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

#
```

Le TABLEAU 3-1 dresse la liste et la description des options de ligne de commande disponibles.

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

Option	Description
`-a`	Détermine si un système est en conformité avec le profil de sécurité associé.
`-b`	Utilisée avec l'option –u. Sauvegarde tout fichier ayant été modifié manuellement depuis la dernière session de durcissement, puis rétablit l'état initial du système.
`-d`	Indique le pilote à exécuter en mode autonome.
`-f`	Utilisée avec l'option –u. Annule les modifications effectuées lors d'une session de durcissement sans vous proposer d'exceptions, même si les fichiers ont été modifiés manuellement après une session de durcissement.
`-h`	Affiche le message d'aide de `jass-execute`, qui présente les options disponibles.
`-H`	Affiche l'historique du logiciel Solaris Security Toolkit sur le système.
`-k`	Utilisée avec l'option –u. Conserve les modifications manuelles apportées depuis la dernière session de durcissement.
`-l`	Affiche la dernière application de Solaris Security Toolkit sur le système.
`-m`	Envoie la sortie à une adresse e-mail spécifique.
`-o`	Dirige la sortie vers un fichier spécifique.
`-p`	Utilisée avec l'option `-r` *répertoire_racine*. Indique la version du SE (système d'exploitation) Solaris. Le format utilisé est identique à celui de l'option `uname -r`.
`-q`	Empêche l'affichage de la sortie à l'écran. Également appelée option silencieuse.
`-r`	Doit s'utiliser avec `-p` *version_se*. Indique le répertoire racine utilisé lors des sessions `jass-execute`. Par défaut, le système de fichiers racine est `/`. Ce répertoire racine est défini par la variable d'environnement Solaris Security Toolkit (JASS), `JASS_ROOT_DIR`. Le SE Solaris sécurisé est disponible via `/`. Par exemple, si vous souhaitez sécuriser un répertoire SE distinct, monté temporairement sous `/mnt`, utilisez l'option `-r` afin de spécifier `/mnt`.
`-u`	Exécute l'option d'annulation (undo) en vous présentant des invites interactives vous demandant ce que le programme doit faire s'il détecte des exceptions. Impossible à utiliser avec les options –d, –a, –h, –l ou –H.
`-v`	Affiche des informations sur la version de ce programme.
`-V`	Indique le niveau de détail de la sortie générée.
`-?`	Affiche le message d'aide de `jass-execute`, qui présente les options disponibles.

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

Pour une liste complète des pilotes disponibles, consultez le répertoire Drivers. Les dernières versions du logiciel sont susceptibles de contenir des pilotes supplémentaires.

▼ Exécution du logiciel en mode autonome

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

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

```
# cd /opt/SUNWjass
# ./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: 4.1.0
Node name:                        ufudu
```

EXEMPLE DE CODE 3-3 Exécution du logiciel en mode autonome *(suite)*

```
Host ID:                                8085816e
Host address:                           10.8.31.115
MAC address:                            8:0:20:85:81:6e
OS version:                             5.9
Date:                                   Tue May 4 16:28:24 EST 2004
================================================================
[...]
```

Pour une liste complète des pilotes disponibles, consultez le répertoire Drivers. Les dernières versions du logiciel sont susceptibles de contenir des pilotes supplémentaires.

2. **Une fois le logiciel Solaris Security Toolkit exécuté sur un système, redémarrez ce dernier afin de prendre en compte les modifications.**

   Lors du durcissement, diverses modifications sont apportées à la configuration du client. Il peut s'agir, entre autres, de la désactivation de scripts de démarrage pour les services, de la désactivation d'options de services et de l'installation de nouveaux fichiers binaires ou de nouvelles bibliothèques à partir de patchs. Tant que le client n'est pas redémarré, ces modifications risquent de ne pas prendre effet.

3. **Une fois le système redémarré, assurez-vous que les modifications sont correctes et toutes intégrées.**

   Reportez-vous à la section « Validation des modifications du système », page 56.

4. **Si des erreurs sont détectées, corrigez-les et réexécutez le logiciel Solaris Security Toolkit en mode autonome.**

Option d'audit

L'option `-a` permet au logiciel Solaris Security Toolkit d'effectuer un audit visant à déterminer si un système est conforme à son profil de sécurité. Cette session a pour objet non seulement de vérifier que les modifications apportées au fichiers système sont toujours actives, mais aussi de contrôler si des processus auparavant désactivés sont en cours d'exécution ou si des packages de logiciels supprimés ont été réinstallés. Pour plus d'informations sur cette fonction, reportez-vous au Chapitre 6.

Exemple d'utilisation pour l'audit d'un système en fonction d'un profil de sécurité :

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

Option Display Help

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

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

EXEMPLE DE CODE 3-4 Exemple de sortie de l'option `-h`

```
# ./jass-execute -h
Pour appliquer ce Toolkit (cette boîte à outils) à un système à
l'aide de la syntaxe :
   jass-execute [-r root_directory -p os_version ]
      [ -q | -o output_file ] [ -m e-mail_address ]
      [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente de Toolkit sur un système :
   jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
      [ -m e-mail_address ] [ -V [3|4] ]

Pour vérifier si un système est conforme à un profil prédéfini :
   jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
      [ -m e-mail_address ]

Pour afficher l'historique des applications de Toolkit sur un
système :
   jass-execute -H

Pour afficher la dernière application de Toolkit sur un système :
   jass-execute -l

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

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

Vous observerez qu'il suffit de spécifier le nom du pilote avec les
options -d ou -a. Il est inutile d'indiquer un chemin car le script
est supposé exister dans le répertoire Drivers.

L'option -u (undo) et les options -d et -a s'excluent mutuellement.
Le comportement d'annulation par défaut est de demander à
l'utilisateur en cas
de détection d'un fichier à restaurer qui a été modifié puisque
la somme de contrôle est incorrecte.

L'option -u est être combinée avec -k, -b ou -f afin d'écraser
le comportement interactif par défaut. Il est nécessaire d'utiliser
```

EXEMPLE DE CODE 3-4 Exemple de sortie de l'option `-h` *(suite)*

```
l'une de ces options lors d'une exécution en mode silencieux ('-q').

L'option -k permet de conserver en permanence le fichier actif et
la sauvegarde si la somme de contrôle est incorrecte. b permet de
sauvegarder le
file actif et de restaurer l'original si la somme de contrôle est
incorrecte.
L'option f a toujours priorité sur l'original si la somme de contrôle
est incorrecte, sans enregistrer l'original modifié.
```

Option de pilote (driver)

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

Vous devez définir un pilote à l'aide de l'option `-d`. Le logiciel Solaris Security Toolkit ajoute `Drivers/` au début du nom du script ajouté. Vous devez uniquement saisir le nom du script sur la ligne de commande.

Remarque – Vous ne pouvez pas utiliser l'option `-d` avec les options `-u, -H, -h` ou `-a`.

Une session de durcissement `jass-execute` utilisant l'option `-d` *driver* génère une sortie similaire à l'exemple suivant :

EXEMPLE DE CODE 3-5 Exemple de sortie de l'option `-d` *driver*

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

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

============================================================
Solaris Security Toolkit Version: 4.1.0
Node name:                        ufudu
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.9
Date:                             Tue Oct 4 16:28:24 EST 2004
============================================================
[...]
```

Option de notification par e-mail

L'option `-m` *email-address* est un mécanisme selon lequel le logiciel Solaris Security Toolkit envoie automatiquement par e-mail le durcissement autonome et la sortie d'annulation, une fois la session terminée. Le rapport e-mail est fourni en plus des journaux éventuellement générés sur le système à l'aide d'autres options.

Une session Solaris Security Toolkit appelant `sunfire_15k_sc-config.driver` à l'aide de l'option de notification par e-mail ressemble à ceci :

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

Option de l'historique des exécutions

L'option `-H` offre un mécanisme simple permettant de déterminer le nombre de fois que le logiciel Solaris Security Toolkit a été exécuté sur un système. Toutes les exécutions sont répertoriées, qu'elles aient été annulées ou non.

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

EXEMPLE DE CODE 3-6 Exemple de sortie de l'option `-H`

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

La liste qui suit recense les applications de Solaris Security
Toolkit sur ce système. Elle est présentée par 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 sur ce système trois fois et que la dernière session a été annulée.

Option de l'exécution la plus récente

L'option `-l` option offre un mécanisme permettant d'identifier l'exécution la plus récente. Il s'agit toujours de la dernière exécution recensée par l'option `-H`.

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

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

```
# ./jass-execute -l

Remarque : Ces informations concernent uniquement les applications
de Solaris Security Toolkit depuis la version 4.1.0.

La dernière application de Solaris Security Toolkit a eu lieu le :

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
```

Option de sortie de fichier

L'option `-o` *output-file* redirige la sortie de console de `jass-execute` vers un fichier distinct intitulé *output-file*.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Cette option est extrêmement pratique lorsqu'elle est utilisée sur une connexion de terminal lente, car Solaris Security Toolkit génère une quantité significative de données de sortie.

Cette option peut s'utiliser en combinaison avec les options `-d`, `-u` ou `-a`.

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

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

```
# ./jass-execute -o jass-output.txt -d 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 sur le flux d'entrée/sortie standard (`stdio`) pendant l'exécution d'un durcissement.

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 lorsque Solaris Security Toolkit est exécuté via une tâche cron ou sur une connexion réseau bas débit.

Cette option peut s'utiliser en combinaison avec les options `-d`, `-u` ou `-a`.

L'option -q génère une sortie du type suivant :

EXEMPLE DE CODE 3-9 Exemple de sortie de l'option -q

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

Option de répertoire racine

L'option -r *root-directory* permet de spécifier le répertoire racine utilisé au cours d'exécutions jass-execute. L'option -r nécessite par ailleurs l'utilisation de l'option -p afin d'indiquer la version de la plate-forme (du SE). Le format de l'option -p équivaut à celui généré par uname -r.

Par défaut, le répertoire du système de fichiers racine est /. Ce répertoire racine est défini par la variable d'environnement Solaris Security Toolkit JASS_ROOT_DIR. Le SE Solaris sécurisé est disponible via /. Par exemple, si vous souhaitez sécuriser un répertoire SE distinct, monté temporairement sous /mnt, utilisez l'option -r afin de spécifier /mnt. Tous les scripts sont appliqués à cette image du SE.

Option d'annulation

L'option -u (undo) permet au logiciel Solaris Security Toolkit d'annuler des modifications système effectuées au cours du durcissement. Il est ainsi possible d'annuler chaque script finish à l'aide de l'option -u. De plus, la fonction d'annulation de Solaris Security Toolkit est étroitement intégrée aux sommes de contrôle générées lors de chaque exécution. Pour plus d'informations sur cette fonction, reportez-vous au Chapitre 4.

Exemple d'utilisation de la ligne de commande pour une commande d'annulation :

```
# jass-execute -u [ -b | -f | -k ] [ -q | -o fichier_de_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 manière à utiliser le mode JumpStart, reportez-vous au Chapitre 5.

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

▼ Exécution du logiciel en mode JumpStart

Pour exécuter le logiciel Solaris Security Toolkit en mode JumpStart, assurez-vous qu'il est intégré à votre environnement JumpStart et appelé à partir des scripts finish associés à une installation JumpStart. Pour de plus amples informations sur l'intégration du logiciel Solaris Security Toolkit à votre environnement, reportez-vous au Chapitre 5.

1. **Lorsque toutes les modifications requises ont été apportées aux pilotes, installez le client à partir de l'infrastructure JumpStart.**

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

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

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

   celui-ci devrait ensuite être configuré correctement. Lors du durcissement, diverses modifications sont apportées à la configuration du client. Il peut s'agir, entre autres, de la désactivation de scripts de démarrage pour les services, de la désactivation d'options de services et de l'installation de nouveaux fichiers binaires ou de nouvelles bibliothèques à partir de patchs. Tant que le client n'est pas redémarré, ces modifications risquent de ne pas prendre effet.

2. **Une fois le système redémarré, assurez-vous que les modifications sont correctes et toutes intégrées.**

   Reportez-vous à la section « Validation des modifications du système », page 56.

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

Validation des modifications du système

Une fois le système redémarré, vérifiez si les modifications apportées sont correctes et complètes en suivant les directives des sections qui suivent.

Contrôles qualité (QA) des services

L'un des défis majeurs inhérents à la sécurisation des systèmes est l'identification des services du SE devant rester activés afin que le système puisse fonctionner correctement. Certains services du SE Solaris sont nécessaires de par leur utilisation directe comme, par exemple, le shell sécurisé qui permet de se connecter à un système. Ils peuvent aussi être utilisés de manière indirecte tel le démon RPC (Remote Procedure Call) utilisé par l'interface utilisateur d'outils de gestion de logiciels tiers.

Il est préférable de déterminer la plupart des conditions requises avant d'exécuter le logiciel Solaris Security Toolkit. (Reportez-vous à la section « Détermination des besoins de l'application et du service », page 20). Toutefois, la seule méthode fiable consiste à installer et à sécuriser le système, puis à effectuer des tests complets des fonctionnalités requises à l'aide d'un contrôle qualité (QA, quality assurance). Il est vivement conseillé de mettre en place un plan de QA pour tout nouveau système à déployer après le durcissement du système. De même, dans le cas des systèmes déployés en cours de durcissement, il est recommandé de conduire des tests complets afin de s'assurer que toutes les fonctionnalités requises et attendues sont installées et opérationnelles.

Si le contrôle qualité révèle des disparités, procédez comme suit :

1. Identifiez la zone posant problème en vous référant aux directives du Chapitre 2.
2. Validez l'exécution de l'application dans la configuration modifiée.
3. Annulez la session Solaris Security Toolkit.
4. Modifiez le profil (pilote) de sécurité en fonction de la résolution du problème.
5. Exécutez à nouveau le logiciel Solaris Security Toolkit.

Résultat : vous devriez disposer d'un profil de sécurité exécutable sur le système sans impacts négatifs sur les fonctionnalités requises.

Évaluation de la sécurité de la configuration

Outre la vérification complète des fonctions que le système doit pouvoir exécuter, pensez également à évaluer la configuration de sécurité afin de déterminer si le système bénéficie du niveau de protection voulu. Selon le degré de durcissement ou de réduction appliqué au système, différents aspects sont concernés.

Au minimum, vous devriez vérifier la configuration du système sur les plans suivants :

- Assurez-vous que tous les patchs de sécurité et autres recommandés sont installés.
- Assurez-vous que seuls les processus requis et appropriés fonctionnement et qu'ils sont exécutés avec les arguments appropriés.
- Assurez-vous que seuls les démons requis fonctionnement et qu'ils sont exécutés avec les arguments appropriés.
- Assurez-vous que seuls les ports requis sont ouverts sur le système en vérifiant localement (par exemple, `netstat -a`) et à distance à l'aide d'un scanner de port tel que Nmap, qui identifie les ports disponibles sur une interface réseau.
- Assurez-vous que seuls les packages du SE Solaris nécessaires ont été installés si le système a été réduit.

Considérez ce type de vérification comme minimal dans le cas de systèmes qui viennent d'être construits et sécurisés. Lors du durcissement de systèmes existants, il est recommandé de vérifier le SE sous-jacent afin de détecter la présence de modifications non autorisées. Pour effectuer des contrôles d'intégrité de cette nature, il est conseillé de monter le système de fichiers du système en mode lecture seule et d'exécuter le logiciel de contrôle de l'intégrité à partir d'une instance connue du SE. Les outils décrits dans l'article Sun BluePrints OnLine intitulée « The Solaris Fingerprint Database—A Security Tool for Solaris Software and Files » sont utiles dans ce cas de figure.

Validation du profil de sécurité

Une fois qu'un système est sécurisé et que vous avez validé les services et fonctions requises afférents, faites appel à la fonction d'audit pour vous assurer que le profil de sécurité a été appliqué correctement et entièrement. Cette tâche est essentielle à deux titres. Premièrement, elle permet de vous assurer que le durcissement du système est conforme aux conditions requises. Deuxièmement, elle garantit que le profil de sécurité défini pour le système est reproduit correctement dans la configuration de Solaris Security Toolkit. Cette vérification est cruciale, car les informations de configuration servent à conserver le profil de sécurité du système tout au long du cycle de vie du déploiement.

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

Exécution des tâches suivant l'installation

Si vous avez installé le logiciel sur un système déployé, reportez-vous à la section « Exécution des tâches suivant l'installation », page 31, pour en savoir plus sur les tâches à effectuer après l'installation sur les systèmes déployés.

CHAPITRE 4

Annulation de modifications du système

Ce chapitre explique comment rétablir le système en annulant les modifications introduites par le logiciel Solaris Security Toolkit pendant l'exécution des opérations de durcissement. Cette option fournit un mécanisme automatisé permettant de restaurer un système dans l'état où il se trouvait avant une ou plusieurs sessions de durcissement.

Ce chapitre traite des points suivants :

Consignation et annulation des changements effectués

Chaque session de durcissement de Solaris Security Toolkit crée un répertoire d'exécution dans `JASS_REPOSITORY`. Les noms de ces répertoires se basent sur la date et l'heure de début d'exécution. En plus de 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 l'enregistrement des opérations.

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

Attention – Le contenu des fichiers dans `JASS_REPOSITORY` ne doit jamais être modifié par un administrateur.

Quand vous utilisez le logiciel Solaris Security Toolkit pour le durcissement 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 d'annulation utilise pour revenir en arrière. Le fichier contient des informations sur les opérations de durcissement implémentées 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 personnalisées, qui sont requises quand on annule des modifications plus complexes, telles les installations de packages. Un fichier `jass-manifest.txt` séparé est créé pour chaque session de durcissement.

Remarque – La fonction d'annulation du logiciel Solaris Security Toolkit annule uniquement les modifications qui correspondent à des entrées dans les fichiers globaux.

L'annulation est exécutée par l'intermédiaire des fichiers globaux générés pendant une session de Solaris Security Toolkit et stockés dans `JASS_REPOSITORY`. L'exécution restaure les fichiers de sauvegarde à leurs emplacements d'origine. Si des fichiers n'avaient pas été sauvegardés, la fonction d'annulation n'est pas disponible.

L'annulation d'une session de Solaris Security Toolkit n'entraîne pas la suppression du répertoire associé. En revanche, deux fichiers sont créés dans le répertoire `JASS_REPOSITORY`: `jass-undo-log.txt` et `reverse-jass-manifest.txt`. Ensuite, la session qui a été annulée n'apparaîtra plus dans la liste à la prochaine exécution de `jass-execute -u`. Une session de durcissement 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 4.1 de Solaris Security Toolkit, vous pouvez utiliser la fonction d'annulation pour des sessions exécutées en mode autonome ou JumpStart. Toutefois, vous ne pouvez annuler des modifications qu'en mode autonome. La fonction d'annulation ne peut pas être utilisée pendant une installation JumpStart.
- Si vous sélectionnez l'option Solaris Security Toolkit pour 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` a été réglé sur `0`.
- Une session ne peut être annulée qu'une seule fois.

- Si vous développez un nouveau script finish qui n'utilise pas les fonctions de structure de Solaris Security Toolkit, vous devez créer un script audit approprié et ajouter des entrées dans le fichier global en utilisant 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 altérer le contenu et causer des erreurs imprévisibles ou la corruption du système quand vous utiliser 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 entreprise tout en vous facilitant la gestion de la configuration de systèmes pendant leurs cycles de vie.

Lors de la personnalisation de scripts, il est important de comprendre l'effet de chacune de vos 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 d'annulation utilise le contenu des fichiers globaux pour annuler les sessions de durcissement). Dans la plupart des cas, ces fonctions auxiliaires fournissent ce dont vous avez besoin pour personnaliser les scripts pour votre organisation.

Vous trouverez une liste de fonctions auxiliaires et des explications sur leur utilisation dans le *Solaris Security Toolkit 4.1 Reference Manual*. Utilisez ces fonctions auxiliaires à la place des commandes équivalentes du système, afin que les annulations se réfèrent aux 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 avoir à 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 lorsque voulez ajouter des packages qui ne sont pas au format Sun `pkg`. Dans cet exemple, vous devrez dire à la fonction d'annulation comment supprimer les packages qui avaient été ajoutés dans un autre format lors de la session de durcissement.

Avec les fonctions auxiliaires et la fonction spéciale `add_to_manifest`, le logiciel Solaris Security Toolkit met à disposition un outil simple et flexible pour personnaliser des scripts et étendre les modifications aux sessions d'annulation.

Si vous modifiez le comportement de scripts finish sans utiliser ces fonctions, le logiciel Solaris Security Toolkit ne pourra pas savoir quelles modifications ont été apportées. Par conséquent, vous devrez annuler manuellement les modifications qui ne sont pas référencées dans les fichiers globaux.

Autre exemple : avant de modifier un fichier sur le système, il faut 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, Solaris Security Toolkit n'aura 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 `JASS_SUFFIX` et ajoute une entrée globale indiquant au logiciel Solaris Security Toolkit qu'une copie du fichier a été faite. 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 modifiés manuellement après une session de durcissement, il est parfois plus indiqué de faire appel à la commande `jass-check-sum` pour lister et vérifier les fichiers modifiés.

Cette commande vous permet de revoir le contenu de `JASS_REPOSITORY` et d'effectuer les sommes de contrôle sur tous les fichiers listés dans les fichiers globaux afin de déterminer quels fichiers ont été modifiés depuis l'enregistrement de leurs sommes de contrôle pendant la session de durcissement. Effectué avant de lancer une session d'annulation forcée, ce contrôle permet d'obtenir de précieuses informations qui vous éviteront de perdre des heures inutiles pour le dépannage.

Ci-dessous, un exemple de sortie.

EXEMPLE DE CODE 4-1 Exemple 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 l'exécution du durcissement.

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 session d'annulation.

Remarque – Vous ne pouvez pas utiliser les options `-d`, `-a`, `-h`, `-l` ou `-H`avec la fonction d'annulation. Vous devez fournir les options `-b`, `-k` ou `-f` lors de l'exécution de la fonction d'annulation `undo` en mode silencieux.

`jass-execute -u` est la commande standard pour l'exécution d'une session d'annulation. Cette commande détecte automatiquement les fichiers qui ont été modifiés manuellement depuis la dernière session de durcissement. Si le logiciel Solaris Security Toolkit détecte des fichiers qui ont été modifiés manuellement après une session de durcissement, il vous demande de choisir une réponse :

1. Effectuez une copie de sauvegarde du fichier le plus récent avant de restaurer l'original (le fichier qui existait avant le durcissement).
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 être perdues) et restaurez le fichier original.

Si vous voulez changer le comportement par défaut de l'annulation, utilisez les options `-b`, `-k` et `-f` quand 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. Vous trouverez des informations détaillées sur chaque option dans les sections ci-après.

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

Option	Description
`-b`	Sauvegarde tout fichier ayant été modifié manuellement depuis la dernière session de durcissement, puis restaure le système dans son état d'origine.
`-f`	Annule les modifications effectuées lors d'une session de durcissement sans vous proposer d'exceptions, même si les fichiers ont été modifiés manuellement après une session de durcissement.
`-k`	Conserve toute modification manuelle apportée aux fichiers après une session de durcissement.

TABLEAU 4-1 Utilisation des options de ligne de commande avec la commande d'annulation *(suite)*

Option	Description
`-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 `JASS_REPOSITORY/jass-undo-log.txt`.

Option de sauvegarde

L'option `-b` sauvegarde automatiquement les fichiers qui ont été modifiés manuellement depuis la dernière session de durcissement, puis restaure les fichiers dans leur état d'origine avant la session de durcissement. Pour implémenter les modifications manuelles, vous devez comparer les fichiers restaurés avec les fichiers sauvegardés et ajuster les différences à la main. Un fichier sauvegardé en utilisant cette option sera similaire à l'exemple suivant.

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

Option de forçage

L'option `-f` annule les modifications apportées pendant une session de durcissement sans aucune exception, même si les fichiers avaient été modifiés manuellement après la session de durcissement. La session d'annulation ne compare pas les sommes de contrôle des fichiers enregistrés avec les versions actuelles des fichiers. En conséquence, si vous avez modifié des fichiers manuellement après une session de durcissement, les modifications seront écrasées et perdues après la session d'annulation.

Il peut être nécessaire de réimplémenter les modifications manuellement après l'exécution d'une session d'annulation. De plus, il peut être nécessaire d'ajuster les différences entre des groupes de fichiers, suivant les types de modifications apportées. Pour éviter ces problèmes, utilisez la commande `jass-check-sum` ou l'option de ligne de commande `-b` précédemment citée.

Option de maintien

L'option `-k` maintient automatiquement toute modification manuelle apportée aux fichiers après une session de durcissement 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 sauvegardées dans le fichier `jass-checksums.txt` sont valides.

Cette option n'est pas sans inconvénients. Par exemple, un système peut être placé dans un état incohérent si un sous-ensemble de fichiers modifiés par un script finish sont ultérieurement modifiés.

Prenons 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 un durcissement, 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 maintien, seul le fichier `/etc/passwd` sera copié à son état d'origine. Le fichier `/etc/shadow` conserve sa forme actuelle. Les deux fichiers ne sont plus cohérents.

Option de sortie de fichier

L'option `-o` *output-file* redirige la sortie de la console de commandes `jass-execute` vers un fichier séparé, *output-file*.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Cette option est particulièrement utile si elle est utilisée sur une connexion lente de terminal, parce qu'une session d'annulation Solaris Security Toolkit génère une quantité de données en sortie.

Option de sortie silencieuse

L'option `-q` empêche le logiciel Solaris Security Toolkit d'envoyer une sortie sur 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 sur des connexions réseau bas débit.

Option de notification par e-mail

Avec l'option `-m` *email-address*, le logiciel Solaris Security Toolkit envoie par e-mail une copie de l'exécution complète à une adresse e-mail. La notification par e-mail est en plus des journaux générés sur le système en utilisant d'autres options.

Annulation de modifications du système

Il est parfois nécessaire d'annuler les modifications apportées pendant une ou plusieurs sessions de durcissement de Solaris Security Toolkit. Si vous estimez que les modifications apportées pendant une session de durcissement ont des conséquences négatives sur votre système, vous pouvez les annuler.

Par exemple, si après une session de durcissement vous découvrez qu'un service requis, tel que NFS, a été désactivé, annulez la session de durcissement. Ensuite, activez NFS et répétez la session de durcissement avec le profil de sécurité révisé.

Cette section explique comment annuler les modifications apportées pendant une ou plusieurs sessions de durcissement. Remarquez que l'annulation d'une session de durcissement est soumise à certaines restrictions et conditions. Reportez-vous à la section « Conditions requises pour l'annulation de modifications du système », page 60.

▼ Annulation d'une session Solaris Security Toolkit

1. **Sauvegardez et réinitialisez votre système.**

   Réinitialisez et sauvegardez le système avant chaque session d'annulation pour s'assurer qu'il retournera ou pourra être ramené dans un état connu et fonctionnant.

2. **Déterminez les options que vous voulez utiliser avec la commande** `jass-execute -u`**.**

   Reportez-vous à la section « Utilisation d'options avec la fonction d'annulation », page 63.

   Pour les instructions qui suivent, on suppose que vous utilisez la commande `jass-execute -u`.

3. **Pour annuler une ou plusieurs sessions en utilisant l'option standard** `-u`**, tapez la commande suivante depuis** `JASS_HOME_DIR`**:**

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

   Le logiciel Solaris Security Toolkit collecte des informations sur chaque session de durcissement 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 cette session d'annulation n'est pas

exécutée. De plus, si le répertoire du fichier global contient également un fichier appelé `jass-undo-log.txt`, le logiciel suppose que la session d'annulation a déjà été exécutée et ne la répète donc pas. Une fois toutes les informations collectées, les résultats s'affichent. Ci-dessous, un exemple de sortie.

EXEMPLE DE CODE 4-2 Sortie de test des sessions disponibles pour l'annulation

```
# ./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 sessions différentes de durcissement ont été trouvées. Ces sessions ont apporté des modifications au système et n'ont pas été annulées. La liste des sessions de durcissement est toujours présentée par ordre chronologique inverse. La première entrée dans la liste correspond à la session de durcissement la plus récente.

4. **Vérifiez la sortie pour déterminer quelle(s) session(s) annuler, puis entrez le numéro correspondant.**

   Pour chaque entrée sélectionnée, le logiciel Solaris Security Toolkit annule chaque session de numéro égal ou inférieur à la valeur sélectionnée. Ainsi, la session d'annulation annule les modifications dans l'ordre inverse de leur réalisation, c'est-à-dire en commençant par la plus récente pour terminer par celle que vous avez sélectionnée. En utilisant l'exemple précédent comme référence, si vous sélectionnez la session 3, puis `undo run`, vous annulez d'abord les modifications de la session 1, puis les modifications de la session 2 et enfin celles de la session 3.

L'exemple suivant illustre la sortie générée quand la session d'annulation porte sur deux entrées de fichier global.

EXEMPLE DE CODE 4-3 Sortie de test d'une session d'annulation portant sur plusieurs entrées de fichier global

```
[...]

================================================================
undo.driver: Performing UNDO of
//var/opt/SUNWjass/run/20030124135727.
================================================================

[...]

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

[NOTE] Undoing operation COPY.
cp -p /etc/cron.d/cron.allow.JASS.20030125223417
/etc/cron.d/cron.allow
rm -f /etc/cron.d/cron.allow.JASS.20030125223417

[NOTE] Removing a JASS-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 session de durcissement. La sortie d'une session d'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.

La session d'annulation continue jusqu'au traitement de toutes les sessions et de tous les fichiers globaux correspondants et à l'annulation de toutes les modifications.

En plus de la collecte d'informations sur chaque session de durcissement en recherchant tous les fichiers globaux contenus dans `JASS_REPOSITORY`, le logiciel Solaris Security Toolkit compare la somme de contrôle de chaque fichier modifié. Chaque fois qu'une anomalie est détectée dans les fichiers des sommes de contrôle, un avertissement est généré et consigné. Pour ces fichiers, la session d'annulation vous demande quelle action vous souhaitez mettre en oeuvre.

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

   L'exemple de sortie suivant illustre une exception et les choix possibles pour gérer cette exception.

EXEMPLE DE CODE 4-4 Sortie de test d'une exception d'annulation

```
[...]

================================================================
undo.driver: Undoing Finish Script: install-templates.fin
================================================================

[NOTE] Undoing operation COPY.
cp -p /etc/skel/local.login.JASS.20030125223413
/etc/skel/local.login
rm -f /etc/skel/local.login.JASS.20030125223413

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]    filename = /etc/.login
[WARN]    current = 3198795829:585, saved = 1288382808:584

Please select the course of action:

1. Backup.  Save current file before restoring original.
2. Keep.    Keep the current file, making no changes.
3. Force.   Ignore manual changes and overwrite current file.

Enter 1, 2, or 3:
```

Dans notre exemple, en choisissant 1, on obtient la sortie suivante.

EXEMPLE DE CODE 4-5 Sortie de test du choix d'une option de sauvegarde pendant une annulation

```
Enter 1, 2, or 3: 1

[NOTE] BACKUP specified, creating backup copy of /etc/.login.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /etc/.login to /etc.login.BACKUP.JASS.20030125224926
cp -p /etc/.login.JASS.20030125223413 /etc/.login
rm -f /etc/.login.JASS.20030125223413

[...]
```

Effectuez l'opération appropriée pour les fichiers qui ont été modifiés manuellement après des sessions de durcissement.

Quand une session d'annulation rencontre des fichiers modifiés et que vous décidez de ne pas les écraser, ajustez ces fichiers avant de réinitialiser le système.

Remarque – Dans notre exemple, le fichier modifié a été sauvegardé sous un nouveau nom : `/etc/.login.BACKUP.JASS.20030125224926`. Après la session d'annulation, comparez ce fichier à `/etc/.login` pour établir si d'autres ajustements sont nécessaires.

---

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

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

   Il est indispensable de réinitialiser le système pour qu'il puisse arrêter et démarrer les services disponibles avant son durcissement.

CHAPITRE 5

Configuration et gestion de serveurs JumpStart

Ce chapitre explique comment configurer et administrer les serveurs JumpStart pour utiliser le 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 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 standardisation de systèmes. Il s'agit d'une solution permettant l'installation et le déploiement de systèmes avec rapidité.

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 contribue à assurer la standardisation de la sécurisation des systèmes et son adressage au moment de l'installation du système. 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 traite des points suivants :

Configuration de serveurs et d'environnements JumpStart

Pour l'utilisation dans un environnement JumpStart, vous devez copier la source Solaris Security Toolkit contenue dans `JASS_HOME_DIR` (pour les téléchargements `tar`) ou `/opt/SUNWjass` (pour les téléchargements `pkg`) à l'intérieur du 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.

▼ Configuration pour le mode JumpStart

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

   Par exemple, si l'archive de Solaris Security Toolkit a été extraite dans `JASS_REPOSITORY` et que le répertoire racine du serveur JumpStart est `/jumpstart`, la commande suivante copie la source Solaris Security Toolkit :

   ```
   # pwd
   /opt/SUNWjass
   # tar cf - . | (cd /jumpstart; tar xf -)
   ```

   Normalement, 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 système d'exploitation Solaris 2.5.1, apportez ces modifications dans le fichier contenu dans le répertoire `JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1`.**

   Si vous utilisez Solaris 2.5.1 OS, 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-répertoires séparés. Pour répondre à cette restriction sur Solaris 2.5.1 OS, le logiciel Solaris Security Toolkit dispose d'un répertoire `SI_CONFIG_DIR/sysidcfg`, 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/Drivers
# cp user.init.SAMPLE user.init
```

4. **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`**.**

5. **Si vous voulez installer le logiciel Solaris Security Toolkit dans un sous-répertoire de** `SI_CONFIG_DIR`**, comme** `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
```

6. **Sélectionnez ou créez un pilote Solaris Security Toolkit (par exemple, le pilote par défaut** `secure.driver`**).**
   - Si vous entendez utiliser tous les scripts listés dans `hardening.driver` et `config.driver`, ajoutez le chemin `Drivers/secure.driver` au fichier `rules`.
   - Si vous ne devez utiliser que les scripts sélectionnés, faites des copies de ces fichiers, puis modifiez les copies.

7. **Après avoir complété le pilote, vous devez modifier le fichier** `rules`**.**

   L'entrée ajoutée au fichier doit être similaire à :

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

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.

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

8. **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 quelconque lors de l'analyse syntaxique du fichier `sysidcfg`, le contenu du fichier sera 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 sur le client et de durcir ou minimiser avec succès le système d'exploitation pendant le processus d'installation.

Utilisation de modèles de profils JumpStart

Les modèles de profils JumpStart sont des fichiers qui sont exclusivement utilisés avec le mode JumpStart. Le contenu des profils obligatoires et optionnels 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 pour déterminer quelles sont les modifications éventuelles à apporter pour une utilisation dans votre environnement.

Faites 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 :

- `32-bit-minimal.profile`
- `core.profile`
- `end-user.profile`
- `developer.profile`
- `entire-distribution.profile`
- `oem.profile`
- `minimal-Sun_ONE-WS-Solaris*.profile`
- `minimal-SunFire_Domain*.profile`

Ces profils sont décrits ci-après.

32-bit-minimal.profile

Ce profil JumpStart est relativement générique pour un système minimisé 32 bits. Il représente un point de départ raisonnable pour le développement de systèmes minimisés et a été utilisé comme point de départ pour les scripts de minimisation `minimal-Sun_ONE-WS-Solaris* .profile`.

core.profile

Ce profil JumpStart installe le plus petit cluster du SE Solaris, à savoir `SUNWCreq`. Il se limite à spécifier 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 de Solaris, `SUNWCuser`, et les deux packages Solaris requis pour que le relevé du 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 Solaris requis pour que le relevé du processus fonctionne correctement. Comme dans la définition de `core.profile`, les seules définitions supplémentaires apportées à la configuration, en plus du cluster du SE Solaris, concernent le partitionnement du disque pour inclure les partitions racine et swap.

entire-distribution.profile

Ce profil JumpStart installe le cluster de distribution complète de SE Solaris, à savoir `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 de SE Solaris, à savoir `SUNWCXall`. Ce cluster est un jeu complet du cluster de distribution qui installe le logiciel OEM fourni.

minimal-Sun_ONE-WS-Solaris*.profile

Tous les profils suivants se réfèrent à l'article Sun BluePrints OnLine intitulé « *Minimizing the Solaris Operating Environment for Security* ». Toutes les versions du SE Solaris mentionnées dans cet article ont des profils spécifiques. Les profils mentionnés dans l'article sont les profils JumpStart suivants :

- `minimal-Sun_ONE-WS-Solaris.26.profile`
- `minimal-Sun_ONE-WS-Solaris7-32bit.profile`
- `minimal-Sun_ONE-WS-Solaris7-64bit.profile`
- `minimal-Sun_ONE-WS-Solaris8-32bit.profile`
- `minimal-Sun_ONE-WS-Solaris8-64bit.profile`
- `minimal-Sun_ONE-WS-Solaris9-64bit.profile`

minimal-SunFire_Domain*.profile

Les profils suivants se réfèrent à l'article Sun BluePrints OnLine intitulé *Minimizing Domains for Sun Fire V1280, 12K, and 15K Systems*. Les profils mentionnés dans l'article sont les profils JumpStart suivants :

- `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

Ce point décrit les scripts pouvant être utilisés en mode JumpStart. Le mode 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 manière à utiliser le mode JumpStart, reportez-vous à la section « Configuration de serveurs et d'environnements JumpStart », page 72.

Script `add-client`

Pour simplifier l'ajout de clients depuis des serveurs JumpStart, utilisez ce script 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`, qui accepte les arguments suivants.

Exemple d'utilisation :

```
# 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`

Valeur	Description
-c *client*	Nom d'hôte résolvable du client JumpStart.
-h	Affiche des informations sur l'utilisation. S'utilise sans être accompagnée d'autres options. Toute option supplémentaire sera ignorée.
-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 machine du client JumpStart. Cette valeur a le même format que la sortie de la commande `uname -m`.
-o *Se-client*	Révision du SE Solaris, disponible dans le répertoire `JASS_HOME_DIR/OS`, qui n'est pas installé 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*	Le nom optionnel du chemin d'accès 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 réglée sur le répertoire `JASS_HOME_DIR/Sysidcfg/Solaris_version/`, où la version est extraite du OS spécifié pour ce client. Si spécifié, il faut utiliser un nom de chemin relatif au répertoire `JASS_HOME_DIR`. Spécifiez uniquement le chemin d'accès au fichier `sysidcfg`.
-v	Affiche des informations sur la version de ce programme.
-?	Affiche des informations sur l'utilisation. S'utilise sans être accompagnée d'autres options. Toute option supplémentaire sera ignorée.

Pour ajouter un client JumpStart appelé `jordan` à un serveur JumpStart intitulé `nomex` à l'aide de Solaris 8 (4/01) sur une interface appelée `nomex-jumpstart`, exécutez la commande `add-client` suivante :

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart
updating /etc/bootparams
```

Pour ajouter le même client JumpStart (`jordan`) en utilisant l'option`sysidcfg`, vous devez utiliser la commande suivante :

```
#./add-client -c jordan -o Solaris_8_2001-04 -m sun4u -i nomex-jumpstart -s
Hosts/jordan
updating /etc/bootparams
```

Script `rm-client`

Pour simplifier la suppression de clients depuis des serveurs JumpStart, utilisez ce script 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 *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` de manière similaire à `add-client`:

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

Où *`client`* est le 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`

Valeur	Description
`-c` *client*	Nom d'hôte résolvable du client JumpStart.
`-h`	Affiche des informations sur l'utilisation. S'utilise sans être accompagnée d'autres options. Toute option supplémentaire sera ignorée.
`-v`	Affiche des informations sur la version de ce programme.
`-?`	Affiche des informations sur l'utilisation. S'utilise sans être accompagnée d'autres options. Toute option supplémentaire sera ignorée.

Pour supprimer un client JumpStart appelé `jordan`, exécutez la commande `rm-client` suivante :

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

CHAPITRE 6

Audit de sécurité de systèmes

Ce chapitre explique comment contrôler (valider) la sécurité d'un système à l'aide du logiciel Solaris Security Toolkit. Utilisez les indications et les procédures figurant dans ce chapitre pour maintenir un profil de sécurité donné après le durcissement. Pour les systèmes déjà déployés, référez-vous aux informations contenues dans ce chapitre pour évaluer les mesures da sécurité existantes avant de procéder au durcissement.

Remarque – Le terme *audit* est utilisé dans ce chapitre et dans cet ouvrage pour définir le processus automatique de validation d'une politique de sécurité en la comparant à un profil de sécurité prédéfini. L'utilisation de ce terme dans cet ouvrage ne signifie pas que le système sera entièrement sécurisé après l'activation de l'option d'audit.

Ce chapitre traite des points suivants :

Maintenance de la sécurité

La maintenance de la sécurité est un processus permanent devant être vérifié et révisé de manière régulière. La maintenance d'un système sécurisé requiert le maximum d'attention, car 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 », page 33).

En nous référant à l'expérience et aux exigences des utilisateurs, nous avons conçu une méthode d'audit automatisée permettant au logiciel Solaris Security Toolkit de contrôler la politique de sécurité d'un système en déterminant le niveau de conformité à un profil de sécurité spécifié.

Remarque – Cette méthode est uniquement disponible en mode autonome via la commande `jass-execute -a`. Elle ne peut pas être utilisée pendant une installation JumpStart.

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

La fréquence de contrôle 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 chaque jour et d'autres encore une fois par mois. Certains utilisateurs 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.

Vérifiez un composant essentiel afin de maintenir la politique de sécurité des systèmes déployés. Si la politique de sécurité n'est pas vérifiée à intervalle régulier, les configurations dérivent souvent avec le temps par entropie ou suite à des modifications apportées par inadvertance ou par malveillance. En l'absence de contrôles périodiques, ces changements ne seront pas détectés et aucune mesure corrective n'est prise. Résultat : le système devient de moins en moins sûr et de plus en plus vulnérable.

En plus des 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 le durcissement

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

Personnalisation des audits de sécurité

L'option d'audit est un mécanisme extrêmement flexible et modulable visant à évaluer l'état d'un système. Comme pour les scripts de durcissement, vous pouvez personnaliser les actions des scripts d'audit. Par exemple, vous pouvez personnaliser les variables d'environnement, la structure et les fonctions d'aide, de même qu'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 servir de modèles pour la personnalisation de l'audit de leurs environnements. Dans ce cas de figure, on utilise les pilotes, les scripts finish, les variables d'environnement et les modèles de fichiers pour personnaliser les scripts d'audit. Vous pouvez apporter des modifications de personnalisation avec un minimum d'efforts, sans devoir toucher le code. Quelles que soient les modifications introduites pour le durcissement, le logiciel Solaris Security Toolkit les détecte automatiquement lorsque vous exécutez l'audit.

Parfois, certains utilisateurs veulent ajouter des contrôles ou des fonctionnalités qui ne sont pas prévus par le logiciel Solaris Security Toolkit. Pour cela, il faut ajouter les contrôles ou les nouvelles fonctionnalités dans le script d'audit. (Vous pouvez aussi apporter les modifications dans le script finish correspondant.) Dans certains cas, il peut s'avérer nécessaire de modifier le code. Si vous ajoutez ou modifiez un code, faites extrêmement attention à ne pas introduire de bogues ou de failles.

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, les scripts finish, les variables et les fonctions spécifiques au site ne sont *pas* reconnus automatiquement pas le logiciel Solaris Security Toolkit lorsque 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 avec seulement le script d'audit, vous devez créer le script finish correspondant.

Pour personnaliser ou créer de nouveaux pilotes, scripts, variables et fonctions, reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

Vous devrez peut-être ajouter un patch que le logiciel Solaris Security Toolkit n'installe pas automatiquement. Vous pouvez utiliser l'un des modèles standard ou spécifiques au produit ou bien en créer un. Si vous définissez vos propres modèles, commencez par créer un script finish pour ajouter le patch, puis rédigez le script d'audit correspondant afin de contrôler l'installation du patch.

Préparation d'un audit de sécurité

Pour utiliser les instructions contenues dans ce chapitre, vous devez disposer d'un profil de sécurité. Pour plus d'informations sur le développement et l'implémentation d'un profil de sécurité, reportez-vous au Chapitre 2.

De nombreux modèles de profils de sécurité sont inclus sous forme de pilotes dans le logiciel Solaris Security Toolkit. Comme indiqué précédemment dans cet ouvrage, le profil de sécurité par défaut et les modifications apportées par ces pilotes ne s'appliquent pas à tous les systèmes. En général, les profils de sécurité mis en œuvre par ces pilotes constituent des limites supérieures de sécurité. Par là, nous entendons des limites qui désactivent les services inutiles et activent les fonctions de sécurité facultatives, désactivées pas défaut.

Pour de nombreux utilisateurs du logiciel Solaris Security Toolkit, les modèles de profils de sécurité standard et spécifiques au produit sont acceptables pour leurs environnements. Si tel est votre cas, déterminez le profil de sécurité correspondant le mieux au type de politique de sécurité voulu, puis utilisez-le pour l'évaluation et le durcissement des systèmes.

Vérifiez et personnalisez les modèles de profils de sécurité pur votre environnement ou développez-en de nouveaux. Vous trouverez des techniques et des directives pour la personnalisation des profils de sécurité dans le manuel le *Solaris Security Toolkit 4.1 Reference Manual*. Cette approche permet de sécuriser votre système selon les besoins de votre entreprise et de minimiser la quantité des 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 faille lors de l'évaluation de la sécurité. Par exemple, un site utilisant Telnet avec Kerberos, pour l'authentification et le chiffrement, ne considère pas l'utilisation de Telnet comme une faille.

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 traite des points suivants :

Options de ligne de commande.

Exemple d'utilisation pour l'audit d'un système en fonction d'un profil de sécurité :

```
# jass-execute -a driver [ -V [0-4]] [ -q | -o output-file ]
[ -m adresse-email ]
```

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 Audit

Option	Description
`-a`	Détermine si un système est en conformité avec le profil de sécurité associé.
`-h`	Affiche le message d'aide de `jass-execute`, qui présente les options disponibles.
`-m`	Envoie la sortie à une adresse e-mail.
`-o`	Dirige la sortie dans un fichier.
`-q`	Désactive l'affichage de la sortie sur la console. Également appelée option silencieuse.
`-V`	Spécifie le niveau de verbosité pour un audit.

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

- « Option Display Help », page 83
- « Option de notification par e-mail », page 84
- « Option de sortie de fichier », page 85
- « Option Quiet », page 85
- « Option Verbosity », page 85

Option Display Help

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

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

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

```
# ./jass-execute -h

Pour appliquer ce Toolkit (cette boîte à outils) à un système à
l'aide de la syntaxe :
  jass-execute [-r root_directory -p os_version ]
  [ -q | -o output_file ] [ -m e-mail_address ]
  [ -V [3|4] ] [ -d ] driver

Pour annuler une application précédente de Toolkit sur un système :
  jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
     [ -m e-mail_address ] [ -V [3|4] ]

Pour vérifier si un système est conforme à un profil prédéfini :
  jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
     [ -m e-mail_address ]

Pour afficher l'historique des applications de Toolkit sur un
système :
  jass-execute -H

Pour afficher la dernière application de Toolkit sur un système :
  jass-execute -l

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

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

Option de notification par e-mail

L'option -m *email-address* est un mécanisme selon lequel le logiciel Solaris Security Toolkit envoie automatiquement la sortie par e-mail une fois la session terminée. Le rapport e-mail est en plus des journaux éventuellement générés sur le système à l'aide d'autres options.

Une session Solaris Security Toolkit appelant sunfire_15k_sc-config.driver à l'aide de l'option de notification par e-mail ressemble à ceci :

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

Option de sortie de fichier

L'option `-o` *output-file* redirige la sortie de console de `jass-execute` vers un fichier distinct intitulé *output-file*.

Cette option n'a aucun effet sur les journaux conservés dans le répertoire `JASS_REPOSITORY`. Cette option est extrêmement pratique lorsqu'elle est utilisée sur une connexion de terminal lente, car Solaris Security Toolkit génère une quantité significative de données de sortie.

Cette option peut s'utiliser en combinaison avec les options `-d`, `-u` ou `-a`.

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

EXEMPLE DE CODE 6-2 Exemple 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 Quiet

L'option `-q` désactive la sortie de Solaris Security Toolkit sur le flux d'entrée/sortie standard (`stdio`) pendant l'exécution d'un durcissement.

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 lorsque Solaris Security Toolkit est exécuté via une tâche cron ou sur une connexion réseau bas débit.

Cette option peut s'utiliser en combinaison avec les options `-d`, `-u` ou `-a`.

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

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

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

Option Verbosity

L'option `-V` spécifie le niveau de verbosité d'une session d'audit. Cette option n'est disponible que pour les audits. Les niveaux de verbosité offrent une haute flexibilité d'affichage des résultats d'un audit. Par exemple, si vous avez 100 machines à contrôler, il peut être plus pratique de limiter la sortie à une seule ligne pour chaque

machine afin de savoir quelles machines sont correctes et lesquelles ne le sont pas. Ensuite, vous pouvez choisir de lancer un audit uniquement sur les machines incorrectes et de générer 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	Une ligne indique la réussite ou l'échec.
1	Pour chaque script, une ligne indique la réussite ou l'échec. Une ligne indique le total général des résultats après les lignes de script.
2	Pour chaque script, indique les résultats de tous les contrôles.
3	Plusieurs lignes avec une sortie complète, y compris les messages de bannière et d'en-tête.
4	Plusieurs lignes (toutes les données depuis le niveau 3) plus toutes les entrées 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 au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

Sortie de bannières et de messages

Vous pouvez configurer l'option d'audit de Solaris Security Toolkit pour sortir ou omettre les bannières et les messages. La variable `JASS_LOG_BANNER` n'est pas compatible avec les niveaux de verbosité 0 à 2. Ces options de sortie s'appliquent aux niveaux de verbosité 3 et 4. Par exemple, il est parfois souhaitable de supprimer les messages de passage (variable `JASS_LOG_SUCCESS`) de la sortie afin que le rapport contienne uniquement les messages relatifs aux échecs (variable `JASS_LOG_FAILURE`).

Le TABLEAU 6-3 dresse 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 au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.) Si la variable de consignation est définie sur `0`, aucune sortie ne sera générée pour les messages de ce type. Inversement, si la

variable de consignation est définie sur 1, les messages seront affichés. Par défaut, ces variables sont configurées de manière à afficher les messages. Le TABLEAU 6-3 décrit les variables de consignation.

TABLEAU 6-3 Affichage des bannières et des messages en 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 des bannières. Ces messages sont généralement entourés de séparateurs de type signe égal (« = ») ou tiret (« - »).
JASS_LOG_ERROR	[ERR]	Ce paramètre contrôle l'affichage des messages d'erreur. S'il est défini sur 0, aucun message d'erreur ne sera généré.
JASS_LOG_FAILURE	[FAIL]	Ce paramètre contrôle l'affichage des messages d'échec. S'il est défini sur 0, aucun message d'échec ne sera généré.
JASS_LOG_NOTICE	[NOTE]	Ce paramètre contrôle l'affichage des messages d'avis. S'il est défini sur 0, aucun message d'avis ne sera généré.
JASS_LOG_SUCCESS	[PASS]	Ce paramètre contrôle l'affichage des messages de succès. S'il est défini sur 0, aucun message de succès ne sera généré.
JASS_LOG_WARNING	[WARN]	Ce paramètre contrôle l'affichage des messages d'avertissement. S'il est défini sur 0, aucun message d'avertissement ne sera généré.

Ces options se révèlent très pratiques lorsque vous souhaitez uniquement afficher des messages spécifiques. En les configurant, vous pouvez minimiser les messages générés et vous concentrer sur les zones que vous estimez critiques. Par exemple, en configurant toutes les variables de consignation sur 0 à l'exception de JASS_LOG_FAILURE (en conservant sa valeur par défaut de 1), seuls les rapports d'audit concernant des failles seront générés par la fonction logFailure.

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

```
# JASS_LOG_FAILURE=1
# export JASS_LOG_FAILURE
[setting of other parameters to 0 omitted]
# ./jass-execute -a secure.driver -V 2
update-at-deny        [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
update-at-deny        [FAIL] Audit Check Total : 1 Error(s)
update-inetd-conf     [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
update-inetd-conf     [FAIL] Audit Check Total : 3 Error(s)
```

Nom d'hôte, nom de script et horodatage en sortie

Vous pouvez configurer l'option d'audit de Solaris Security Toolkit de manière à inclure le nom d'hôte, le nom de script et l'horodatage pour les niveaux de verbosité 0 à 2. Par exemple, si vous disposez d'un nombre élevé de machines à contrôler, vous pouvez trier la sortie par nom d'hôte, par nom de script ou par horodatage. Le TABLEAU 6-4 dresse 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 configuré sur 1, le logiciel Solaris Security Toolkit ajoute chaque entrée de journal avec le nom d'hôte du système. Cette information repose sur le paramètre JASS_HOSTNAME. Par défaut, ce paramètre est vide et la boîte à outils Toolkit n'affiche donc pas cette information.
JASS_DISPLAY_SCRIPTNAME	Par défaut, ce paramètre est configuré sur 1 et le logiciel Solaris Security Toolkit ajoute chaque entrée de journal avec le nom d'hôte du script d'audit en cours d'exécution. En configurant ce paramètre sur une autre valeur, la boîte à outils Toolkit n'affiche pas cette information.
JASS_DISPLAY_TIMESTAMP	Lorsque ce paramètre est configuré sur 1, le logiciel Solaris Security Toolkit ajoute chaque entrée de journal avec l'horodatage associé à l'audit. Cette information repose sur le paramètre JASS_TIMESTAMP. Par défaut, ce paramètre est vide et le logiciel n'affiche donc pas cette information.

En configurant le logiciel Solaris Security Toolkit afin qu'il ajoute le nom d'hôte, le nom de script et l'horodatage, vous pouvez combiner de nombreux audits depuis un seul système ou un groupe de systèmes et les trier ensuite à partir de ces données. Vous pouvez 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 failles.

Par exemple, en configurant le paramètre JASS_DISPLAY_TIMESTAMP sur 1 et le paramètre JASS_DISPLAY_SCRIPTNAME sur 0, on obtient en sortie un message similaire au suivant.

EXEMPLE DE CODE 6-5 Exemple d'entrées de journal d'audit

```
# JASS_DISPLAY_SCRIPTNAME=0
# JASS_DISPLAY_TIMESTAMP=1
# export JASS_DISPLAY_SCRIPTNAME JASS_DISPLAY_TIMESTAMP
# ./jass-execute -a secure.driver -V 2
20030101233525 [FAIL] User test is not listed in
   /etc/cron.d/at.deny.
20030101233525 [FAIL] Audit Check Total : 1 Error(s)
20030101233525 [FAIL] Service ftp is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service telnet is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Service rstatd is enabled in
   /etc/inet/inetd.conf.
20030101233525 [FAIL] Audit Check Total : 3 Error(s)
```

Exécution d'un audit de sécurité

L'évaluation périodique de la sécurité de votre système permet savoir jusqu'à quel point la sécurité correspond au profil de sécurité que vous avez implémenté. Le plus souvent l'évaluation de la sécurité d'un système est- similaire à une tâche de maintenance parfois exécutée après le durcissement de nouvelles installations. Nous avons conçu l'option d'évaluation de la sécurité de sorte que vous puissiez exécuter le(s) même(s) pilote(s) de durcissement que ceux utilisés pour le durcissement du système, mais utiliser à présent l'option `-a` pour contrôler l'état actuel par rapport au profil de sécurité implémenté pendant l'opération. Cette solution élimine la complexité tout en offrant un grande flexibilité. Par exemple, quand vous mettez à jour votre profil de sécurité, les évaluations de sécurité suivantes utilisent le profil de sécurité mis à jour.

Dans un autre scénario possible, vous pourriez être responsable de la sécurisation de systèmes qui sont déjà déployés. Avant de passer à leur durcissement, vous voulez effectuer une évaluation de sécurité. Dans ce scénario, vous définissez votre 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.

▼ Exécution d'un audit de sécurité

Avant d'effectuer un audit, vous devez définir ou choisir un profil de sécurité. Pour plus d'informations, reportez-vous à la section « Préparation d'un audit de sécurité », page 82.

Attention – Si vous évalué la politique de sécurité appliquée à un système déployé jamais durci auparavant, commencez par sauvegarder la machine, puis réinitialisez-la afin de vérifier que sa configuration est connue, homogène et opérationnelle. Les erreurs ou les avertissements détectés lors de la réinitialisation 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 durcissement) à utiliser :**
   - Si vous avez précédemment durci le système, utilisez le même profil de sécurité.

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

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

   Pour une liste complète et à jour des pilotes disponibles, téléchargez la dernière version du logiciel Solaris Security Toolkit sur le site Web suivant :

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

   Consultez le *Solaris Security Toolkit 4.1 Reference Manual* pour de plus amples informations sur les pilotes standard et spécifiques au produit. Les pilotes les plus récents se trouvent dans le répertoire Drivers.

2. **Déterminez les options de ligne de commande que vous voulez utiliser et comment vous souhaitez contrôler la sortie.**

   Reportez-vous à la section « Utilisation d'options et contrôle de la sortie des audits », page 82.

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

   L'exemple suivant illustre un audit exécuté à l'aide du script `sunfire_15k_sc-secure.driver`.

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

```
# ./jass-execute -a sunfire_15k_sc-secure.driver
[NOTE] Executing driver, sunfire_15k_sc-secure.driver

[...]

================================================================
sunfire_15k_sc-secure.driver: Audit script: enable-rfc1948.aud
================================================================

#----------------------------------------------------------------
# RFC 1948 Sequence Number Generation
#
# Rationale for Audit:
#
# The purpose of this script is to audit that the system is
# configured and is in fact using RFC 1948 for its TCP sequence
# number generation algorithm (unique-per-connection ID). This is
# configured by setting the 'TCP_STRONG_ISS' parameter to '2' in
# the /etc/default/inetinit file.
#
# Determination of Compliance:
#
[...]
#----------------------------------------------------------------

[PASS] TCP_STRONG_ISS is set to '2' in /etc/default/inetinit.
[PASS] System is running with tcp_strong_iss=2.

# The following is the vulnerability total for this audit script.

[PASS] Audit Check Total : 0 Error(s)

================================================================

# The following is the vulnerability total for this driver profile.

[PASS] Driver Total : 0 Error(s)

================================================================
sunfire_15k_sc-secure.driver: Driver finished.
================================================================

[PASS] Grand Total : 0 Error(s)
```

Après le démarrage d'une session d'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, ils n'ont pas les mêmes suffixes. Le script `driver.run`traduit automatiquement les scripts finish définis par la variable `JASS_SCRIPTS` dans des scripts d'audit, en changeant leurs suffixes de `.fin` à `.aud`.

L'audit démarre et initialise l'état du logiciel Solaris Security Toolkit. Chaque pilote auquel on 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 sa réussite ou son 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. Par ailleurs, la valeur totale de vulnérabilité pour chaque pilote est affichée une fois l'évaluation du pilote terminée. Un total général de tous les résultats 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 a commencé. Le logiciel Solaris Security Toolkit contrôle l'état stocké du système en inspectant les fichiers de configuration et l'état en cours du système en inspectant les informations sur la table du processus, le pilote de périphérique et ainsi de suite. Le logiciel Solaris Security Toolkit contrôle l'existence de chaque fichier ou service et vérifie qu le logiciel associé avec un service est installé, configuré, activé et en cours d'exécution. Cette méthode fournit un instantané précis de l'état courant d'un système.

CHAPITRE 7

Sécurisation d'un système

Ce chapitre décrit comment appliquer les informations contenues dans les chapitres précédents à un scénario réaliste pour l'installation et la sécurisation d'un nouveau système. Ce chapitre explique comment déployer le logiciel Solaris Security Toolkit avec un Check PointFirewall-1 NG pour le SE Solaris 8.

Utilisez les informations contenues dans ce chapitre comme guide et scénario pour sécuriser un nouveau système et des applications.

Les ouvrages et les articles Sun BluePrint accessibles en ligne peuvent vous guider au cours du processus de réduction et de durcissement de nombreux systèmes Sun. Vous trouverez les versions les plus récentes de ces documents à l'adresse suivante :

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

Ce chapitre traite des points suivants :

Planification et préparation

Pour bien déployer des systèmes réduits et sécurisés tels que décrit dans 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 de systèmes doivent être définis et communiqués. Pour de plus amples informations sur la planification et la

préparation, reportez-vous au Chapitre 2. Le scénario décrit dans ce chapitre documente les procédures et les tâches qu'un administrateur système doit effectuer afin d'obtenir une image réduite et durcie du SE Solaris pour un système de pare-feu.

Dans ce scénario, l'administrateur système doit créer une solution automatisée et évolutive pour la construction et le déploiement de systèmes Check PointFirewall-1 NG pour un fournisseur d'accès (xSP) qui souhaite offrir un service pare-feu à ses clients. Pour ce scénario, les exigences et les considérations du xSP sont les suivantes :

- Vu que le xSP a prévu de déployer un nombre important de ces systèmes, le temps employé pour construire et déployer chacun de ces systèmes est un facteur critique 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 n'est utilisé que par le personnel du xSP 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 de pare-feu déployés.

Sur la base de ces facteurs, l'administrateur système décide d'automatiser l'installation, la réduction et le durcissement des images OS en utilisant la technologie JumpStart et le logiciel Solaris Security Toolkit.

Suppositions et restrictions

Ce chapitre suppose que nous utilisons un logiciel Solaris Security Toolkit déjà fonctionnel et une installation en technologie JumpStart. D'autres chapitres de cet ouvrage contiennent des instructions et des directives pour l'installation du logiciel ; reportez-vous aux chapitres correspondants.

Ce chapitre suppose que nous développons une configuration personnalisée pour la réduction et le durcissement d'une application spécifique. Le logiciel Solaris Security Toolkit ne possède pas de pilotes ou de profils JumpStart spécifiques à l'application. Par conséquent, nous devons 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.

Pour ce scénario, l'administrateur système doit :

- Avoir suffisamment de connaissances et d'expérience pour configurer le système d'exploitation et les applications.
- Savoir comment tester et ajuster la configuration.
- Savoir comment construire un environnement JumpStart à partir duquel installer le système client. Reportez-vous à l'ouvrage Sun BluePrint *JumpStart Technology : Effective Use in the Solaris Operating Environment*.

- Maîtriser les techniques de réduction du système d'exploitation. Reportez-vous à *Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*.
- Maîtriser les bases du logiciel Solaris Security Toolkit et être en mesure de construire une configuration personnalisée en utilisant les techniques et directives de réduction et de durcissement. Reportez-vous au Chapitre 1.

Environnement du système

L'exemple de scénario se base sur l'environnement matériel et logiciel suivant :

- Check PointFirewall-1 NG
- SE Solaris 8
- JumpStart, technologie
- Cluster SE Solaris (`SUNWCreq`)
- Logiciel Solaris Security Toolkit
- Plate-forme reposant sur la technologie SPARC
- Au moins deux interfaces Ethernet

Sécurité requise

Pour ce scénario, le haut niveau requis et les packages ont été identifiés, mais pas les composants et les services spécifiques de tous les packages. Il faut également identifier les capacités du SE Solaris nécessaires pour administrer et gérer les systèmes.

La liste suivante précise comment les composants logiciels sont utilisés :

- Shell sécurisé pour l'administration à distance
- FTP pour copier des fichiers
- Solstice DiskSuite™ pour la mise en miroir de disques
- Messages SYSLOG transmis à un référentiel central

Vous pouvez développer un profil de sécurité à partir de cette liste. Pour des informations détaillées sur le développement de profils de sécurité et l'utilisation de modèles de profils, reportez-vous à la section « Développement et implémentation d'un profil Solaris Security Toolkit », page 29.

Création d'un profil de sécurité

Un profil de sécurité définit les modifications introduites par le logiciel Solaris Security Toolkit lors du durcissement et de la réduction 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 pour les systèmes Check PointFirewall-1 NG réduits. Par conséquent, vous devez créer un profil de sécurité personnalisé pour implémenter les modifications du système appropriées.

La méthode de création d'un profil de sécurité pour ce scénario est décrite en divers points de ce chapitre. D'abord, nous créons de nouveaux fichiers de pilotes à partir des pilotes existants. Ensuite, nous modifions les nouveaux pilotes afin de les conformer aux conditions de sécurité précédemment précisées. La réduction est décrite au point « Installation du logiciel », page 96, et les modifications de la configuration de durcissement au point « Personnalisation de la configuration de durcissement », page 104.

Installation du logiciel

Cette section décrit comment installer le logiciel. La description est effectuée en tenant compte de toutes les exceptions et instructions spécifiques à cet exemple de scénario. Vous trouverez des instructions générales sur l'installation du logiciel dans d'autres parties de ce guide.

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 sécurisation

Téléchargez et installez Solaris Security Toolkit et les composants logiciels de sécurisation additionnels, y compris les patchs, sur le serveur JumpStart en procédant comme suit.

▼ Procédures de téléchargement et d'installation du logiciel de sécurisation

1. **Téléchargez le logiciel Solaris Security Toolkit et les composants de sécurisation additionnels.**

   Reportez-vous à la section « Téléchargement des packages de sécurité », page 38.

2. **Installez le logiciel Solaris Security Toolkit et les composants de sécurisation additionnels.**

   Reportez-vous à la section « Installation et exécution du logiciel », page 46.

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 aspects de disponibilité, des défauts au niveau des performances ou d'autres aspects d'un système. Quand vous installez un nouveau système d'exploitation puis à intervalles réguliers, vérifiez que les patchs appropriés sont appliqués.

Le logiciel Solaris Security Toolkit fournit un mécanisme pour l'installation du cluster de patchs de sécurité et recommandés disponibles sur SunSolve Online. Ce cluster de patchs spécifiques au système d'exploitation contient les patchs les plus souvent requis.

▼ Installation des patchs

1. **Vous devez au minimum télécharger le cluster de patchs recommandés de sécurité et dans le répertoire** `Patches` **et le décomprimer.**

   Si le script `install-recommended-patches.fin` est inclus dans le pilote de durcissement, ce cluster de patchs sera installé automatiquement.

   Un point supplémentaire porte sur Check PointFirewall-1 NG. Cette application nécessite des patchs spécifiques non fournis dans le cluster des patchs de sécurité et recommandés. Le Check PointFirewall-1 NG requiert les patchs suivants :

   - 108434
   - 108435

2. **Pour automatiser l'installation des patchs 108434 et 108435, téléchargez les dernières versions des patchs depuis 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 d'aide `add_patch`, avec le nom de chaque patch.**

   Ce script finish appelle les fonctions d'aide appropriées 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

La première tâche requise après la définition de l'organisation du disque pour l'installation du système d'exploitation est de spécifier quel cluster du SE Solaris doit être installé. Choisissez l'un des cinq clusters d'installation fournis avec le SE Solaris : `SUNWCreq`, `SUNWCuser`, `SUNWCprog`, `SUNWCall` et`SUNWCXall`.

▼ Indication et installation du cluster du système d'exploitation

1. **Spécifiez le cluster du système d'exploitation à installer.**

   L'objectif de cet exemple de scénario étant de construire un pare-feu réduit et dédié, à savoir le plus petit des clusters de SE Solaris disponibles, `SUNWCreq`, ce package est également connu en tant que Noyau.

   Ce cluster contenant un nombre relativement petit de packages, d'autres packages seront probablement requis. Ces autres packages doivent être inclus dans le profil avec la définition du cluster de Solaris.

   La définition du profil de la ligne de référence ajoute ce qui suit au profil précédemment défini.

```
cluster           SUNWCreq
```

   Le cluster d'installation `SUNWCreq` comprend des packages qui ne sont pas nécessaire 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 OnLine « Minimizing the Solaris Operating Environment for Security : Updated for the Solaris 9 Operating Environment ».

2. **Exploitez une installation avec le profil de sécurité correctement défini pour déterminer la présence éventuelle de problèmes de dépendance de packages.**

   Certaines dépendances de packages sont rencontrées pendant l'installation et nous déterminons que les packages Solaris suivants sont requis pour Check PointFirewall-1 NG :

   - `SUNWter` – Informations sur le terminal
   - `SUNWadmc` – Bibliothèques de noyau 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 dans le profil est la suivante :.

```
cluster          SUNWCreq
package          SUNWter          add
package          SUNWlibC         add
package          SUNWlibCx        add
package          SUNWlibC         add
package          SUNWlibC         add
```

   Bien que cette liste soit complète pour cette étude de cas, d'autres packages peuvent être ajoutés ou supprimés dans l'environnement où cette configuration est déployée.

   Des modifications pourront encore être apportées à liste finale des packages tant que le fonctionnement et la sécurité du système n'auront pas été vérifiés (voir « Test d'assurance qualité », page 110). Si tel est le cas, modifiez le profil, réinstallez le système et répétez 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 explique comment configurer le serveur et le client JumpStart afin d'utiliser un profil de sécurité pour la réduction. Pour des informations détaillées 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.

▼ Préparation de l'infrastructure

1. **Configurez votre serveur et 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 jordan -o Solaris_8_2002-02 -m sun4u
-s nomex-jumpstart
cleaning up preexisting install client "jordan"
removing jordan 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 jordan - 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 avant de pouvoir terminer avec succès l'étape suivante. Initialement, ces fichiers peuvent être des copies de fichiers distribués avec le logiciel Solaris Security Toolkit. Ne modifiez jamais les fichiers originaux distribués avec le logiciel Solaris Security Toolkit. L'exemple suivant illustre comment créer les 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/Profiles
# cp minimal-Sun_ONE-WS-Solaris8-64bit.profile \
     xsp-minimal-firewall.profile
```

   Cet exemple utilise une configuration de serveur Web dédié, parce qu'il s'agit d'une bonne base de départ pour le développement d'un pare-feu dédié.

5. **Après la création des fichiers de profil et de pilote, modifiez ces fichiers 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 à votre script finish (par exemple,** `fw1-patch-install.fin`**).**

      Le script modifié doit être similaire au suivant.

EXEMPLE DE CODE 7-3 Exemple 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.
```

À ce stade, il doit être possible de commencer l'installation JumpStart sur le client, `jordan` dans cet exemple. Utilisez la configuration JumpStart et les pilotes Solaris Security Toolki, 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 », page 103.**

8. **Depuis 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 ne se construit pas, vérifiez la configuration et modifiez-la jusqu'à ce qu'il 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 correctement 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 réduction et son durcissement.

Validation et vérification du fichier Rules

Lors de la validation du fichier `rules`, vous pouvez rencontrer toute une série de problèmes. Certains de ces problèmes les plus fréquents sont décrits dans cette section.

La première exécution du fichier `rules` donne la sortie suivante.

EXEMPLE DE CODE 7-5 Exemple de sortie pour le fichier `rules`

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/xsp-minimal-firewall.profile...
Error in file "rules", line 20
hostname jordan - 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`jordan` n'existe pas. Le profil `xsp-minimal-firewall.profile` n'était pas présent dans le répertoire des profils. Normalement, cette erreur est générée à cause d'une faute de frappe dans le nom de fichier, de l'omission du répertoire pour les profils ou simplement parce le profil n'a pas encore été créé. Résolvez le problème et effectuez une nouvelle vérification.

Le second contrôle détecte deux autres problèmes. Le premier problème se réfère au pilote appelé dans `xsp-firewall-secure.driver`. Au lieu d'appeler `xsp-firewall-hardening.driver`, `xsp-firewall-secure.driver` appelle encore `hardening.driver`.

Le second problème se réfère à la variable `JASS_SCRIPTS` qui est réglée sur `minimize-Sun_ONE-WS.fin` et non sur `minimize-firewall.fin`.

Le script suivant est incorrect.

EXEMPLE DE CODE 7-6 Exemple 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 Exemple 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 durcissement

La configuration de durcissement du pare-feu proposé est prête pour sa personnalisation et son réglage précis. Les scripts initiaux se basent sur `hardening.driver`. Ceci signifie que tous les services du système sont désactivés.

Vu que Solaris 8 OS ne contient pas de Shell client sécurisé, vous devez faire des modifications pour permettre l'administration à distance via le réseau des pare-feux. Pour le pare-feu dans cet exemple de scénario, il est spécifié que les services FTP doivent rester activés et qu'un Shell client sécurisé 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 autres interfaces réseau. Vous trouverez des informations sur la restriction de ces services dans l'article Sun BluePrints OnLine intitulé « Solaris Operating Environment Security : Updated for the Solaris 9 Operating Environment ».

Laissez non seulement ces deux services activés, mais encore les services RPC de manière à pouvoir utiliser l'interface graphique (IG) pour configurer Solstice DiskSuite et effectuer la mise en miroir du disque. Si l'interface graphique de Solstice DiskSuite ne doit pas être utilisée, les services RPC sont inutiles. Dans cet exemple, l'interface graphique est requise et les services RPC sont laissés 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 xSP. Ce fichier `syslog.conf` personnalisé doit être installé sur chacun des systèmes de pare-feu.

Ces modifications requièrent des changements dans un grand nombre d'options de configuration de Solaris Security Toolkit. Chacune des modifications nécessaires est décrite en détails dans les sections suivantes.

Activation du service FTP

Pour le pare-feu dans cet exemple de scénario, laissez les services FTP activés.

▼ Procédure d'activation du service FTP

1. **Pour laisser le service FTP activé, modifiez le comportement pas défaut du fichier `update-inetd-conf.fin` en réglant les variables `JASS_SVCS_DISABLE` et `JASS_SVCS_ENABLE`.**

   Pour désactiver tous les services standard Solaris sauf FTP, la meilleure méthode dans notre exemple de scénario est de définir `JASS_SVCS_ENABLE` sur `ftp`, tout en s'assurant que `JASS_SVCS_DISABLE` conserve sa valeur par défaut obtenue via le script `finish.init`. Reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

2. **Pour implémenter le changement à l'aide des variables d'environnement, ajoutez une entrée du type ci-dessous à `xsp-firewall-secure.driver` avant l'appel à `xsp-firewall-hardening.driver`.**

   ```
   JASS_SVCS_ENABLE="ftp"
   ```

3. **Vérifiez que FTP n'est disponible que sur le réseau de gestion du xSP en l'implémentant via le logiciel du pare-feu.**

   Parmi les autres conditions, il fallait que FTP ne soit disponible que sur le réseau de gestion du xSP. Sur le SE Solaris 8, vous pouvez implémenter cette condition en incorporant des wrappers TCP sur le système ou par l'intermédiaire du logiciel du pare-feu. Dans cet exemple de scénario, implémentez cette conditions via le logiciel du pare-feu.

Installation du logiciel Shell sécurisé

Vu que Solaris 8 n'incorpore pas un Shell client sécurisé, vous devez installer un Shell client sécurisé pour l'administration à distance.

Vous pouvez configurer le logiciel Solaris Security Toolkit pour installer l'outil OpenSSH. Utilisez le script `install-openssh.fin`, listé dans le fichier`config.driver` utilisé par `xsp-firewall-secure.driver`.

▼ Installation d'un shell sécurisé

1. **Copiez le** `config.driver` **par défaut sur** `xsp-firewall-config.driver`**.**
2. **Dans la copie du fichier, annuler le commentaire relatif à** `install-openssh.fin`**.**
3. **Modifiez l'entrée dans** `xsp-firewall-secure.driver` **qui appelle**`config.driver` **pour qu'elle appelle** `xsp-firewall-config.driver` **à sa place.**
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 dernière version, accédez aux pages Web d'OpenSSH :

   `http://www.openssh.org`
5. **Compilez le dernier package OpenSSH, attribuez-lui un nom correct et installez-le dans le répertoire** `Packages`**.**

   Pour de plus amples informations sur ce package, reportez-vous à l'article Sun BluePrints OnLine intitulé « Configuring OpenSSH for the Solaris Operating Environment ».
6. **Actualisez le script** `install-openssh.fin` **en mettant à jour le nom du package OpenSSH.**

   Il peut être nécessaire de modifier le script `install-openssh.fin`. Ce script définit le nom de package 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 xSP en l'implémentant via le logiciel du pare-feu.**

   Parmi les autres conditions, il fallait que le Shell sécurisé ne soit disponible que sur le réseau de gestion du xSP. Avec Solaris 8, vous pouvez implémenter cette condition en incorporant des wrappers TCP sur le système ou par l'intermédiaire du logiciel du pare-feu. Dans cet exemple de scénario, nous l'implémentons via le logiciel du pare-feu. Notez que cette condition peut également être implémentée en modifiant la configuration du serveur Shell sécurisé.

Activation du service RPC

Laissez les services RPC activés afin de pouvoir utiliser SDS pour la mise en miroir du disque, qui nécessite RPC.

Cette modification est relativement immédiate grâce à la disponibilité d'un script finish `disable-rpc.fin` qui désactive les services RPC pendant une session de Solaris Security Toolkit.

Remarque – L'accès à distance aux services RPC sur un système doit être explicitement interdit par la configuration de pare-feu du système.

▼ Activation de l'appel RPC

- **Commentez l'entrée pour** `disable-rpc.fin` **dans** `xsp-firewall-hardening.driver`**.**

  Désactivez les scripts depuis les pilotes en les commentant au lieu de les supprimer. Faites attention en commentant les entrées dans la définition `JASS_SCRIPTS`, parce que seules certaines combinaisons de commentaires sont acceptées.

  L'exemple suivant est un commentaire inclus dans le script `driver.funcs` concernant les données que le logiciel Solaris Security Toolkit accepte comme indicateurs de commentaires dans la définition de `JASS_SCRIPTS`.

```
#Gestionnaire de commentaires très rudimentaire. Ce code
reconnaîtra les
#commentaires à condition qu'un seul signe # soit placé devant le
nom du fichier
#(séparé par un espace ou non). Il ne tiendra pas compte alors
#de l'argument qui suit immédiatement.
```

Personnalisation du fichier `syslog.conf`

La modification finale pour ce client consiste en un fichier personnalisé `syslog.conf` qui utilise le serveur SYSLOGcentral du xSP. Ce fichier `syslog.conf` personnalisé doit être installé sur chacun des systèmes de pare-feu.

▼ Personnalisation du fichier `syslog.conf`

1. **Copiez le fichier `syslog.conf` standard du xSP, renommez-le `syslog.conf.jordan` et placez-le dans le répertoire `Files/etc`.**

   Le logiciel Solaris Security Toolkit permet de copier des fichier selon plusieurs méthodes. L'option 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` est uniquement copié sur `jordan`, parce qu'il a des modifications uniques spécifiques au pare-feu. Dans notre cas, le client est appelé `jordan`, de sorte que le nom de fichier utilisé dans `Files/etc` est `syslog.conf.jordan`. Il est important de noter que la définition de `JASS_FILES` ne doit pas avoir de suffixe. Pour de plus amples informations, reportez-vous au manuel le *Solaris Security Toolkit 4.1 Reference Manual*.

2. **Si le fichier xSP standard `syslog.conf` n'est pas disponible, créez un fichier `syslog.conf` personnalisé en procédant comme suit :**

   a. **Copiez le fichier `syslog.conf` livré avec le logiciel Solaris Security Toolkit, renommez-le `syslog.conf.jordan` et placez-le dans le répertoire `Files/etc`.**

   b. **Modifiez `syslog.conf.jordan` pour le conformer au standard xSP pour `SYSLOG`.**

3. **Vérifiez que le fichier** `/etc/syslog.conf` **est listé dans la définition** `JASS_FILES` **du** `xsp-firewall-hardening.driver`**.**

   Par défaut, la définition modifiée `JASS_FILE` dans `xsp-firewall-hardening.driver` est la suivante.

EXEMPLE DE CODE 7-8 Exemple de sortie de `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
"
```

À ce stade, toutes les modifications requises ont été faites. L'installation du système d'exploitation, la réduction et le durcissement sont entièrement automatisés et personnalisés en fonction de l'application spécifique. Les seules tâches qui ne sont pas entièrement automatisées sont la configuration et l'installation du logiciel 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.

▼ Procédure d'installation du client

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

   Tapez la commande suivante à l'invite `ok` du client.

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

2. **Si vous rencontrez des erreurs, corrigez-les et réinstallation 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 tous correctement. Cette tâche permet aussi de vérifie que le profil de sécurité a correctement implémenté 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 durcie et réduite, afin d'assurer la détection des anomalies ou problèmes éventuels et leur rapide correction. Cette procédure comporte deux tâches : Vérification de l'installation du profil et du fonctionnement des applications et des services.

▼ Vérification de l'installation du profil

Pour vérifier que le logiciel Solaris Security Toolkit a installé correctement le profil de sécurité et sans erreurs, contrôlez et évaluez ce qui suit :

1. **Vérifiez le fichier journal de l'installation.**

   Ce fichier est installé dans `JASS_REPOSITORY/jass-install-log.txt`.

   Remarque – Ce fichier journal peut être utilisé comme référence pour comprendre exactement ce que le logiciel Solaris Security Toolkit a fait au système. Pour chaque exécution sur le système, un nouveau fichier journal est enregistré dans un 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 audit pour évaluer la configuration de sécurité du système.**

   Pour des informations détaillées sur l'option audit, reportez-vous au Chapitre 6. Pour ce scénario, nous utilisons la commande suivante du répertoire où le logiciel Solaris Security Toolkit a été installé 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:   4.1.0
[...]
```

   Si la vérification de Solaris Security Toolkit rencontre des incohérences, celles-ci seront 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`.

▼ Vérification du 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 s'utilise pour tester les différents composants d'un système ou d'une application et s'assurer qu'ils sont disponibles et en bon état de marche. En l'absence d'un tel plan, testez raisonnablement le système en vous basant sur la manière dont il est utilisé. L'objectif est de s'assurer que le durcissement 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 le durcissement du système, utilisez les techniques décrites dans le chapitre Chapitre 2 pour rechercher le problème.**

   Par exemple, utilisez la commande `truss`. Cette commande peut souvent être utilisée pour déterminer à quel point une application rencontre un problème. Une fois ceci déterminé, il est possible de cibler de problème et de remonter à la modification effectuée par le logiciel Solaris Security Toolkit.

   Remarque – D'après l'expérience collective des personnes qui ont développé le 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 qui suit définit les abréviations et acronymes utilisés dans le 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

BIND (Berkeley Internet Name Domain) Domaine de noms Internet Berkeley

BSD (Berkeley Software Distribution) Distribution logicielle Berkeley

BSM (Basic Security Model) Modèle de sécurité de base sous *Solaris*

C

CD (Compact Disc) Disque compact

CD-ROM Compact Disc–Read-Only Memory

CDE (Common Desktop Environment) Interface graphique unifiée

`cp`**(1)** copy files (copier les fichiers)

`cron`**(1M)** clock daemon (démon de l'horloge)

D

DHCP (Dynamic Host Configuration Protocol) Protocole d'attribution dynamique des adresses sur un réseau IP

DMI (Desktop Management Interface) Interface d'administration du bureau

DMTF (Distributed Management Task Force) Groupe DMTF

DNS (Domain Name System) Service de conversion des noms de domaines

E

EEPROM (Electronically Erasable Programmable Read-Only Memory) Mémoire en lecture seule programmable électroniquement effaçable

F

FTP (File Transfer Protocol) Protocole de transfert de fichiers

G

GID (Group Identifier) Identificateur de groupe

H

HTTP (HyperText Transfer Protocol) Protocole de transfert hypertexte

I

ID Identificateur

IETF (Internet Engineering Task Force) Groupe IETF

INETD (Internet service Daemon) Démon Internet

IP (Internet Protocol) 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 Kerberos

L

LDAP (Lightweight Directory Access Protocol) Protocole LDAP

`lp`**(1)** line printer *(envoyer la requête d'imprimante)*

M

MAN Management Network *(réseau I1 interne des systèmes haut de gamme Sun Fire)*

MD5 (Message-Digest 5 Algorithm) Algorithme de hachage MD5

MIP (Mobile Internet Protocol) Protocole MIP

MSP (Midframe Service Processor) Processeur de service midframe

`mv`**(1)** move files (déplacer les fichiers)

N

NFS (Network File System) Système de fichiers réseau

NG (Next Generation) Prochaine génération

NIS, NIS+ (Network Information Services) Services d'informations sur le réseau

NSCD (Name Service Cache Daemon) Démon cache de service de dénomination

O

OE (Operating Environment) Environnement d'exploitation, *anciennement utilisé pour Solaris*

OEM (Original Equipment Manufacturer) Fabricant de matériel

SE Système d'exploitation, *désormais utilisé pour Solaris*

P

PAM (Pluggable Authentication Module) Module d'authentification enfichable

PDF (Portable Document Format) Format de document portable

PICL (Platform Information and Control Library) Bibliothèque d'informations et de contrôle de plate-forme

PPP (Point-to-Point Protocol) Protocole point-à-point

PROM (Programmable Read-Only Memory) Mémoire en lecture seule programmable

Q

QA (Quality Assurance) Contrôle qualité

R

RBAC (Role-Based Access Control) Contrôle d'accès basé sur le rôle

rc run-control *(exécuter et contrôler un fichier ou un script)*

`rlogin`**(1)** remote login (se connecter à distance)

RFC (Remote Function Call) Appel de fonction à distance

RPC (Remote Procedure Call) Appel de procédure à distance

`rsh`**(1)** remote shell (shell à distance)

S

SA (System Administrator) Administrateur système

SC (System Controller) *Contrôleur système pour les systèmes haut de gamme et milieu de gamme Sun Fire*

`scp`**(1)** secure copy (programme de copie de fichiers sécurisée à distance)

SCCS (Source Code Control System) Système de contrôle du code source

SLP (Service Location Protocol) Protocole d'emplacement de service

SMA (System Management Agent) Agent de gestion système

SMC (Solaris Management Console) Console de gestion Solaris

SNMP (Simple Network Management Protocol) Protocole SNMP

SP (Service Provider) Fournisseur de services

SPARC (Scalable Processor Architecture) Architecture SPARC

SPC (SunSoft Print Client) Client SPC

SSH Secure Shell *(Solaris)*

SSP (System Service Processor) *(processeur de services système pour serveurs Sun Enterprise 10000)*

`stdio` (Standard Input/Output) Entrée/sortie standard

Sun ONE Sun Open Network Environment, *actuellement* Sun Java System, *anciennement* iPlanet

T

TCP (Transmission Control Protocol) Protocole TCP

`tftp`**(1)** (trivial file transfer program) Programme de transfert de fichiers trivial

`ttl` (time-to-live) Temps de session en direct

U

U.S. (United States) États-Unis

UDP (User Diagram Protocol) Protocole UDP

UID ID utilisateur

UUCP (UNIX-to-UNIX Copy) Copie UNIX sur UNIX

V

VOLD (Volume Management Daemon) Démon de gestion de volumes

W

WBEM (Web-based Enterprise Management) Gestion d'entreprise Web

Index

Symboles

Numériques

A

B

C

D

E

F

G

H

I

N

O

S

T

U

V

W

Z