



Notes de version de Solaris™ Security Toolkit 4.2

Sun Microsystems, Inc.
www.sun.com

Référence : 819-3795-10
Août 2005, révision A

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

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit décrit dans ce document. En particulier, et sans limitation aucune, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et un ou plusieurs brevets supplémentaires ou demandes de brevet en cours aux États-Unis et dans d'autres pays.

Le présent document et le produit afférent sont exclusivement distribués avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous quelque forme que ce soit, par quelque moyen que ce soit, sans l'autorisation écrite préalable de Sun et de ses bailleurs de licence, le cas échéant.

Les logiciels détenus par des tiers, y compris la technologie relative aux polices de caractères, sont protégés par copyright et distribués sous licence par des fournisseurs de Sun.

Des parties de ce produit peuvent être dérivées des systèmes Berkeley BSD, distribués sous licence par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, distribuée exclusivement sous licence par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Sun BluePrints, Solaris, SunOS, Java, JumpStart, Sun4U, SunDocs, and Solstice DiskSuite sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et désignent des marques de fabrique ou des marques déposées de SPARC International, Inc., aux États-Unis et dans d'autres pays. Les produits portant les marques déposées SPARC reposent sur une architecture développée par Sun Microsystems, Inc.

L'interface graphique utilisateur d'OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. à l'intention des utilisateurs et détenteurs de licences. Sun reconnaît les efforts de pionnier de Xerox en matière de recherche et de développement du concept des interfaces graphique ou visuelle utilisateur pour l'industrie informatique. Sun détient une licence non exclusive de Xerox sur l'interface graphique utilisateur (IG) Xerox, cette licence couvrant également les détenteurs de licences Sun qui mettent en place des IG OPEN LOOK et se conforment par ailleurs aux contrats de licence écrits de Sun.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTE AUTRE CONDITION, DÉCLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISÉE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Papier
recyclable



Adobe PostScript

Table des matières

Préface vii

Notes de version de Solaris Security Toolkit 4.2 1

Modifications apportées à la version 4.2 de Solaris Security Toolkit 1

 Modifications concernant la prise en charge du SE Solaris 10 2

 Modifications d'ordre général 3

Détails de la prise en charge du SE Solaris 10 4

 Nouvelles fonctions de structure pour Solaris Security Toolkit 4.2 4

 Nouveaux scripts pour Solaris Security Toolkit 4.2 5

 Scripts non utilisés avec le SE Solaris 10 6

 Nouvelles variables d'environnement pour Solaris Security Toolkit 4.2 6

 Nouvelles variables de structure 6

 Nouvelles variables de comportement de script 7

 Variables d'environnement non utilisées avec le SE Solaris 10 7

 Fonctions supprimées dans la version 4.2 de Solaris Security Toolkit 7

 Désactivation automatique de `rpcbind` 8

 ▼ Pour activer `rpcbind` 8

Versions de SMS prises en charge 10

Limitations connues du logiciel Solaris Security Toolkit 10

Remarques générales et problèmes connus	10
Version distribuée exclusivement sous forme de package	10
Possibilité de réadresser les packages <code>SUNWjass</code> et <code>JASScustm</code>	11
Solaris Security Toolkit et <code>CTRL+C</code>	11
Bogues relatifs au logiciel Solaris Security Toolkit 4.2	11
Possibles erreurs de contrôle suite à de multiples redémarrages lorsque le service NIS est utilisé (Bug ID 6222181)	11
<code>svcs</code> non initialisé et échec du contrôle portant sur <code>nddconfig</code> suite à de multiples redémarrages (Bug ID 6284872)	12
Bogues affectant le logiciel Solaris Security Toolkit 4.2	12
Possibilité de divergence au niveau du paramètre de <code>ip6_send_redirects</code> entre deux contrôles (Bug ID 6222001)	13
<code>/etc/motd</code> devrait être installé en tant que fichier volatile (Bug ID 6222495)	13
Dysfonctionnements de <code>svc.startd</code> avec <code>optional_all</code> (Bug ID 6223370)	14

Tableaux

[TABLEAU 1](#) Scripts Solaris Security Toolkit non utilisés avec le SE Solaris 10 6

[TABLEAU 2](#) Corrélation entre les versions de SunOS et du SE Solaris 9

Préface

Le présent document comprend les notes de version relatives au logiciel Solaris™ Security Toolkit 4.2.

Avant de lire ce document

Ce document s'adresse aux administrateurs de systèmes Solaris maîtrisant les systèmes UNIX® et, en particulier, ceux qui reposent sur le système d'exploitation Solaris (SE Solaris). Si vous ne disposez pas de ces connaissances, familiarisez-vous avec les guides de l'utilisateur et de l'administrateur système Solaris. Il est également conseillé de suivre une formation en administration système UNIX.

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. Pour en savoir plus à ce sujet, consultez les sources d'information suivantes :

- la documentation accompagnant les logiciels livrés avec votre système ;
- la documentation du système d'exploitation Solaris, disponible à l'adresse

<http://docs.sun.com>

Invites du shell

Shell	Invite
C shell	<i>nom-machine%</i>
Superutilisateur C shell	<i>nom-machine#</i>
Bourne shell et Korn shell	\$
Superutilisateur Bourne shell et Korn shell	#

Conventions typographiques

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

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

Documentation connexe

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

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

Application	Titre	Référence	Format	Emplacement
Référence	<i>Solaris Security Toolkit 4.2 Reference Manual</i>	819-1503-10	PDF HTML	En ligne
Administration	<i>Guide d'administration de Solaris Security Toolkit 4.2</i>	819-3788-10	PDF HTML	En ligne
Pages de manuel	<i>Solaris Security Toolkit 4.2 Man Page Guide</i>	819-1505-10	PDF	En ligne

Documentation, support et formation

Fonction Sun	URL	Description
Documentation	http://www.sun.com/documentation/	Téléchargez des documents aux formats PDF et HTML, et commandez des guides imprimés.
Support	http://www.sun.com/support/	Demandez le support technique et téléchargez des patches.
Formation	http://www.sun.com/training/	Informez-vous sur les formations Sun disponibles.

Sites Web tiers

Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce manuel. Sun décline toute responsabilité quant au contenu, à la publicité, aux produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et vos suggestions. Vous pouvez nous les envoyer à l'adresse suivante :

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

N'oubliez pas d'indiquer le titre et la référence du document dans votre message :

Notes de version de Solaris Security Toolkit 4.2, référence 819-3795-10.

Notes de version de Solaris Security Toolkit 4.2

Ce document contient les notes de version relatives à la version 4.2 du logiciel Solaris™ Security Toolkit, également connu sous l'appellation JumpStart™ Architecture and Security Scripts (JASS). Il aborde les sujets suivants :

- Modifications apportées à la version 4.2 de Solaris Security Toolkit
- Détails de la prise en charge du SE Solaris 10
- Systèmes matériels pris en charge
- Versions du SE Solaris prises en charge
- Versions de SMS prises en charge
- Limitations connues du logiciel Solaris Security Toolkit 4.2
- Remarques générales et problèmes connus
- Bogues relatifs au logiciel Solaris Security Toolkit 4.2
- Bogues affectant le logiciel Solaris Security Toolkit 4.2

Modifications apportées à la version 4.2 de Solaris Security Toolkit

Cette section des notes de version décrit les modifications majeures apportées à la version 4.2 du logiciel Solaris Security Toolkit. Pour plus d'informations et de détails sur ces modifications, reportez-vous au manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Remarque – Le fichier intitulé `CHANGES`, qui se trouvait dans le répertoire `Documentation` dans les versions antérieures du logiciel Solaris Security Toolkit, n'est plus fourni. Les modifications sont désormais indiquées dans le présent document.

Modifications concernant la prise en charge du SE Solaris 10

La version 4.2 du logiciel Solaris Security Toolkit prend en charge le système d'exploitation (SE) Solaris 10.

Le logiciel Solaris Security Toolkit 4.2 vous permet de durcir et de contrôler la sécurité des systèmes en procédant comme dans les versions antérieures. De même, vous pouvez toujours utiliser cette version du logiciel en mode JumpStart ou autonome, comme auparavant.

Les paragraphes qui suivent décrivent les principales modifications apportées à cette version en vue de prendre en charge le SE Solaris 10. Pour plus d'informations, reportez-vous à la section « Détails de la prise en charge du SE Solaris 10 ».

- Services prêts pour SMF - offre la possibilité à de nombreux scripts Solaris Security Toolkit d'utiliser l'interface de services SMF (Service Management Facility, dispositif de gestion de services), les FMRI (Fault Management Resource Identifiers, identificateurs de ressources de gestion des pannes) et les scripts de démarrage et d'arrêt.
- Services hérités - permet à SMF de reconnaître comme services hérités certains scripts Solaris Security Toolkit non prêts pour SMF.
- Zones - offre la possibilité de durcir et de contrôler des zones du SE Solaris 10.
- Wrappers TCP - offre des configurations de wrappers TCP (Transmission Control Protocol, protocole de contrôle des transmissions) conçues pour les pilotes Solaris Security Toolkit.
- MD5 - prend en charge la fonctionnalité d'algorithme message_digest 5 (md5) du SE Solaris 10 via la commande `digest -a md5`, rendant inutile le package SUNBEmd5 sur les systèmes exécutant le SE Solaris 10.
- Gestion du routage - fournit de nouveaux scripts permettant de gérer le routage dans le SE Solaris 10.
- Nouveau répertoire racine (root) d'accueil - offre un nouveau répertoire racine d'accueil de `/root` au lieu du `/` standard.
- Logiciel IP Filter - offre une fonctionnalité de pare-feu par le biais de l'intégration du freeware Internet Protocol (IP) Filter.
- BART - prend en charge l'outil BART (Basic Audit Reporting Tool), qui permet, entre autres, d'identifier sur les systèmes les modifications apportées au niveau des fichiers.
- Codage souple - prend en charge l'utilisation de plusieurs nouveaux réglages dans le SE Solaris 10, qui contrôlent les algorithmes utilisés pour le chiffrement des mots de passe.
- Verrouillage des comptes - prend en charge la capacité du SE Solaris 10 de verrouiller un compte après l'échec d'un nombre prédéfini de tentatives de connexion.
- Vérification paramétrée des mots de passe - prend en charge la vérification des mots de passe stricte du SE Solaris 10.

- Historique des mots de passe - prend en charge les vérifications de sécurité des mots de passe ajoutées au SE Solaris 10.
- Appel de procédure à distance (RPC) BIND - prend en charge la désactivation ou l'activation de l'appel de procédure à distance du domaine de noms Internet Berkeley (rpcbnd).
- Perl - prend en charge la création de scripts Solaris Security Toolkit en langage Perl (Practical Extraction and Report Language) à utiliser avec le SE Solaris 10.
- XFS - prend en charge la désactivation ou l'activation du serveur de polices X Font Server. Les clients XFS se connectent au serveur afin de demander un jeu de polices. Le serveur lit alors les fichiers de polices à partir du disque et les transmet aux clients. Le démon du serveur X Font Server est géré par SMF.
- GNOME - permet d'activer et de désactiver la prise en charge de l'environnement GNOME (GNU Network Object Model Environment) de même que l'environnement CDE (Common Desktop Environment).

Modifications d'ordre général

Outre les modifications relatives au SE Solaris 10, cette version se caractérise également par les changements d'ordre général suivants :

- Package réadressable - offre un package Solaris Security Toolkit 4.2 réadressable, pouvant être installé dans le répertoire de votre choix grâce aux options appropriées de la commande `pkgadd`.
- Suppression des fichiers de sauvegarde - offre la possibilité de supprimer les fichiers de sauvegarde de Solaris Security Toolkit.
- Fonctionnalités combinées de pilotes - intègre les fonctionnalités de `desktop-{secure|config|hardening}.driver`, `sunfire_15k_domain-{secure|config|hardening}.driver` et `jumpstart-{secure|config|hardening}.driver` dans le pilote `server-{secure|config|hardening}.driver`
- Paramètres par défaut sophistiqués - prend en charge les paramètres par défaut intelligents, autrement dit, l'utilisateur peut appuyer sur la touche Retour pour spécifier un paramètre par défaut lorsque cela s'y prête.
- Verbosité - prend en charge la sortie à verbosité réduite pour les commandes `jass-execute` et `jass-check-sum`.
- `IIim` - prend en charge l'activation et la désactivation de la méthode Internet-Intranet Input Method (`IIim`), qui traite les entrées en langues asiatiques pour le logiciel Solaris.
- Homogénéité des valeurs renvoyées et des pages d'aide générées - offre des valeurs de renvoi et des pages d'aide homogènes pour toutes les commandes de Solaris Security Toolkit.
- Apache 2 - offre la prise en charge d'`apache2`.

Détails de la prise en charge du SE Solaris 10

La section suivante détaille davantage les modifications relatives à la prise en charge du SE Solaris 10 que comporte cette version.

Nouvelles fonctions de structure pour Solaris Security Toolkit 4.2

Les fonctions suivantes sont disponibles pour la première fois dans cette version. Elles sont uniquement compatibles avec les systèmes exécutant le SE Solaris 10. Ces fonctions sont décrites au chapitre 2 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Ces fonctions de consignation dans le journal ont été ajoutées au logiciel Solaris Security Toolkit 4.2 :

- `logNotGlobalZone`
- `logScore`
- `logScriptFailure`
- `logServiceDisabled` and `logServiceEnabled`
- `logServiceInstalled` et `logServiceNotInstalled`
- `logServiceOptionDisabled` et `logServiceOptionEnabled`
- `logServiceProcessList`
- `logServicePropDisabled` et `logServicePropEnabled`
- `logServiceRunning` et `logServiceNotRunning`
- `logUserLocked` et `logUserNotlocked`
- `logUndoBackupWarning`

Ces diverses fonctions courantes ont été ajoutées au logiciel Solaris Security Toolkit 4.2 :

- `get_driver_report`
- `get_lists_conjunction`
- `get_lists_disjunction`

Ces fonctions de pilote public ont été développées afin de prendre en charge SMF dans la structure de Solaris Security Toolkit 4.2 :

- `add_option_to_ftpd_property`
- `change_group`
- `change_mode`
- `change_owner`
- `check_serviceDisabled`

- check_serviceEnabled
- check_serviceInstalled
- check_serviceNotInstalled
- check_serviceNotRunning
- check_serviceOptionEnabled
- check_servicePropDisabled
- check_serviceRunning
- check_serviceOptionDisabled
- check_userLocked
- check_userNotLocked
- convert_inetd_service_to_fmri
- disable_service
- enable_service
- is_service_enabled
- is_service_installed
- is_service_running
- is_user-account_extant
- is_user_account_locked
- is_user_account_login_not_set
- lock_user_account
- make_link
- set_service_property_value
- set_stored_keyword_val
- unlock_user_account
- update_inetcon_in_upgrade

Nouveaux scripts pour Solaris Security Toolkit 4.2

La liste suivante répertorie les nouveaux scripts de fin (.fin) et d'audit (.aud) conçus pour Solaris Security Toolkit 4.2 dont les fonctions sont respectivement décrites au chapitre 5 (scripts de fin) et 6 (scripts d'audit) du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

- disable-apache2.{fin|aud}
- disable-appserv.{fin|aud}
- disable-IIim.{fin|aud}
- disable-routing.{fin|aud}
- enable-account-lockout.{fin|aud}
- enable-bart.{fin|aud}
- enable-ipfilter.{fin|aud}
- enable-password-history.{fin|aud}
- set-root-home-dir.{fin|aud}
- set-strict-password-checks.{fin|aud}

Scripts non utilisés avec le SE Solaris 10

Le [TABLEAU 1](#) dresse la liste des scripts Solaris Security Toolkit non utilisés lors du durcissement du SE Solaris 10.

TABLEAU 1 Scripts Solaris Security Toolkit non utilisés avec le SE Solaris 10

Nom du script	Systèmes d'exploitation compatibles
disable-ab2	Solaris 2.5.1 à 8
disable-aspp	Solaris 2.5.1 à 8
disable-picld	Solaris 8 et 9
install-fix-modes	Solaris 2.5.1 à 9
install-newaliases	Solaris 2.5.1 à 8
install-openssh	Solaris 2.5.1 à 8
install-sadmin-options	Solaris 2.5.1 à 9
install-strong-permissions	Solaris 2.5.1 à 9
remove-unneeded-accounts	Solaris 2.5.1 à 9

Nouvelles variables d'environnement pour Solaris Security Toolkit 4.2

Cette section dresse la liste des variables d'environnement de structure et de comportement de script introduites dans cette version et uniquement compatibles avec les systèmes exécutant le SE Solaris 10. Les fonctions de ces variables d'environnement sont décrites au chapitre 7 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.

Nouvelles variables de structure

- JASS_DISPLAY_HOST_LENGTH
- JASS_DISPLAY_SCRIPT_LENGTH
- JASS_DISPLAY_TIME_LENGTH
- JASS_FILE_COPY_KEYWORD
- JASS_ROOT_HOME_DIR
- JASS_RUN_CLEAN_LOG
- JASS_RUN_VALUES
- JASS_SAVED_BACKUP
- JASS_SCRIPT
- JASS_SCRIPT_FAIL_LOG
- JASS_SCRIPT_NOTE_LOG
- JASS_SCRIPT_WARN_LOG
- JASS_UNDO_TYPE

Nouvelles variables de comportement de script

- JASS_CRYPT_ALGORITHMS_ALLOW
- JASS_CRYPT_ALGORITHMS_DEFAULT
- JASS_CRYPT_DEFAULT
- JASS_CRYPT_FORCE_EXPIRE
- JASS_PASS_DICTIONLIST
- JASS_PASS_DICTIONDBDIR
- JASS_PASS_HISTORY
- JASS_PASS_MAX_REPEATS
- JASS_PASS_MIN_ALPHA
- JASS_PASS_MINDIFF
- JASS_PASS_MINDIGIT
- JASS_PASS_MINLOWER
- JASS_PASS_MINNONALPHA
- JASS_PASS_MINSPECIAL
- JASS_PASS_MINUPPER
- JASS_PASS_NAMECHECK
- JASS_PASS_WHITESPACE
- JASS_ZONE_NAME

Variables d'environnement non utilisées avec le SE Solaris 10

Les variables d'environnement suivantes *ne sont pas* utilisées avec le SE Solaris 10 :

- JASS_ISA_CAPABILITY (*supprimée du logiciel Solaris Security Toolkit 4.2*)
- JASS_DISABLE_MODE

Fonctions supprimées dans la version 4.2 de Solaris Security Toolkit

Les fichiers et les scripts relatifs aux fonctions suivantes ont été supprimés du logiciel Solaris Security Toolkit 4.2 car ils étaient devenus inutiles :

- Installation du module de noyau `misc/klmmod` sur des domaines destinés aux systèmes haut de gamme Sun Fire
- Installation du serveur Sun ONE Web Server
- `sunfire_mf_msp-{config|hardening|secure}.driver`
- Fonctionnalité 32 bits
- Sun Enterprise™ 1000 (Starfire™), ce produit se trouvant en fin de vie

Désactivation automatique de `rpcbind`

À l'instar des versions antérieures de la boîte à outils, les pilotes `secure.driver` et `sunfire-15k_sc-secure.driver` du logiciel Solaris Security Toolkit 4.2 désactivent `rpcbind`. Or, le SE Solaris 10 dispose de services dépendant de `rpcbind` comme, par exemple, les services NIS (Network Information Services, services d'information sur le réseau), NFS (Network File System, système de fichiers réseau), de même que des gestionnaires de fenêtres tels que l'environnement CDE (Common Desktop Environment, interface graphique unifiée) et l'environnement GNOME (GNU Network Object Model Environment, environnement de modélisation d'objets réseau GNU). Par défaut, la configuration des pilotes `secure.driver` et `sunfire-15k_sc-secure.driver` désactive ces services. Par conséquent, vous devez activer `rpcbind` afin de pouvoir les utiliser.

Remarque – Les pilotes `server-secure.driver` et `suncluster3x-secure.driver` ne désactivent *pas* la commande `rpcbind`.

▼ Pour activer `rpcbind`

1. Annulez le durcissement du système.
2. Copiez les pilotes `secure.driver` et `hardening.driver` et renommez-les respectivement `new-secure.driver` et `new-hardening.driver`, `new-secure.driver` étant le nom que vous choisissez pour le nouveau pilote `secure.driver` personnalisé et `new-hardening.driver` désignant le nouveau pilote `hardening.driver` personnalisé.
3. Modifiez `new-secure.driver` en remplaçant la référence à `hardening.driver` par `new-hardening.driver`.
4. Mettez en commentaire le script `disable-rpc.fin` du pilote `new-hardening.driver`.
5. Exécutez à nouveau le durcissement à l'aide des copies de pilotes personnalisées. Pour ce faire, lancez Solaris Security Toolkit avec `new-secure.driver`.
6. Redémarrez le système.



Attention – Une fois que le service `rpcbind` est activé, il se peut que des services supplémentaires démarrent automatiquement et que les ports correspondants s'ouvrent. La fonction de contrôle (audit) de Solaris Security Toolkit interprète ces services comme des échecs.

Systèmes matériels pris en charge

Le logiciel Solaris Security Toolkit 4.2 prend en charge les systèmes SPARC® (version 64 bits *uniquement*) et x86.

Versions du SE Solaris prises en charge

Le support du logiciel Solaris Security Toolkit est assuré par Sun uniquement dans le cadre des systèmes d'exploitation Solaris 8, Solaris 9 et Solaris 10.

Remarque – Pour le logiciel Solaris Security Toolkit 4.2, le SE Solaris 10 s'utilise *exclusivement* sur les domaines de systèmes haut de gamme Sun Fire, *pas* sur le contrôleur système (SC).

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.

D'après les exemples fournis tout au long de ce document, vous observerez que lorsqu'un script vérifie la version du SE, il recherche les versions de SunOS™, autrement dit 5.x, et pas les versions du SE Solaris (2.x, 7, 8, 9 ou 10). Le [TABLEAU 2](#) montre la corrélation entre les versions de SunOS et du SE Solaris.

TABLEAU 2 Corrélation entre les versions de SunOS et du SE Solaris

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

Versions de SMS prises en charge

Si vous utilisez System Management Services (SMS) pour exécuter le contrôleur système (SC) sur des systèmes haut de gamme Sun Fire, sachez que le logiciel Solaris Security Toolkit 4.2 est pris en charge par toutes les versions du SE Solaris 8 et 9 avec les versions 1.4, 1.4.1 et 1.5 de SMS. En revanche, aucune version de SMS n'est compatible avec le SE Solaris 10 assorti du logiciel Solaris Security Toolkit 4.2.

Remarque – Pour le logiciel Solaris Security Toolkit 4.2, le SE Solaris 10 s'utilise *exclusivement* sur les domaines et *pas* sur le contrôleur système (SC).

Limitations connues du logiciel Solaris Security Toolkit

Cette section décrit les limitations connues relatives au logiciel Solaris Security Toolkit 4.2.

- Bien que le logiciel Solaris Security Toolkit 4.2 permette toujours de désactiver des comptes système (voir le script de fin `disable-system-accounts.fin`), il ne peut plus modifier le système en vue d'enregistrer les tentatives de connexion aux comptes ainsi désactivés.

Remarques générales et problèmes connus

Cette section traite des remarques générales et problèmes connus liés au logiciel Solaris Security Toolkit 4.2.

Version distribuée exclusivement sous forme de package

Le logiciel Solaris Security Toolkit 4.2 est *exclusivement* distribué sous forme de package.

Possibilité de réadresser les packages SUNWjass et JASScustm

À partir de la version 4.2 de Solaris Security Toolkit, les packages SUNWjass et JASScustm sont désormais réadressables, à l'instar des normes de conditionnement de Sun. Pour réadresser ces packages, exécutez la commande `pkgadd (1M) -R`.

Solaris Security Toolkit et CTRL+C

L'utilisation de CTRL+C lors d'opérations d'annulation (`undo`) et de durcissement par Solaris Security Toolkit peut aboutir à un état incohérent du système. Il est recommandé de mener à terme les opérations de durcissement avant d'effectuer une annulation (`undo`) plutôt que d'interrompre le durcissement en cours. *Abstenez-vous* d'utiliser la combinaison de touches CTRL+C pour la gestion des erreurs ou d'interrompre une exécution de la boîte à outils. Patientez jusqu'au terme de l'opération, puis recommencez les opérations de durcissement ou `undo`.

Bogues relatifs au logiciel Solaris Security Toolkit 4.2

Cette section présente un récapitulatif des bogues que vous êtes susceptible de rencontrer et qui n'ont *pas* été corrigés dans le logiciel Solaris Security Toolkit 4.2.

Possibles erreurs de contrôle suite à de multiples redémarrages lorsque le service NIS est utilisé (Bug ID 6222181)

`rpcbind` est désactivé par défaut dans le pilote `secure.driver`. Si le service NIS est activé, il se peut que, suite à des redémarrages répétés, le système laisse les services généralement démarrés à l'aide de `inetd` dans un état non initialisé et que les services hérités ne fonctionnent pas. Ce problème se présente dans Solaris Security Toolkit sous la forme d'une incohérence entre les résultats des contrôles effectués avant et après un redémarrage, dans les services démarrés à l'aide de `inetd`.

Ce bogue sera résolu par le Bug ID 6223370 relatif au SE Solaris 10. Vous trouverez la description de ce bogue à la section « Bogues affectant le logiciel Solaris Security Toolkit 4.2 ».

Palliatifs

- Si vous souhaitez utiliser NIS, activez `rpcbind` et redémarrez. Reportez-vous au chapitre 1 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.
- Si vous ne voulez *pas* utiliser le service NIS, désactivez-le. (Reportez-vous au document portant sur le service de dénomination du SE Solaris 10 pour connaître la procédure de désactivation du service NIS.)

svcs non initialisé et échec du contrôle portant sur `nddconfig` suite à de multiples redémarrages (Bug ID 6284872)

Des redémarrages répétés consécutifs à la procédure de durcissement entraînent la non-initialisation de `svcs` et l'échec du contrôle portant sur `nddconfig`. Autrement dit, le contrôle `nddconfig` contiendra des erreurs après de multiples redémarrages système.

Conséquence : `milestone/name-services` ne pourra pas être mis en ligne si `rpcbind` est désactivé et que le système est configuré de manière à utiliser NIS. De ce fait, `/etc/rc2.d (svc:/milestone/multi-user:default)` n'est pas exécuté et le script `nddconfig` n'est donc pas lancé.

Ce bogue sera résolu par le Bug ID 6223370 relatif au SE Solaris 10.

Palliatifs

- Si vous souhaitez utiliser NIS, activez `rpcbind` et redémarrez. Reportez-vous au chapitre 1 du manuel *Solaris Security Toolkit 4.2 Reference Manual*.
- Si vous ne voulez *pas* utiliser le service NIS, désactivez-le. Reportez-vous au document portant sur le service de dénomination du SE Solaris 10 pour connaître la procédure de désactivation du service NIS.

Bogues affectant le logiciel Solaris Security Toolkit 4.2

Cette section présente un récapitulatif des bogues que vous êtes susceptible de rencontrer et qui n'ont *pas* été corrigés dans des logiciels tiers affectant Solaris Security Toolkit.

Possibilité de divergence au niveau du paramètre de `ip6_send_redirects` entre deux contrôles (Bug ID 6222001)

Ce bogue du SE Solaris 10 risque de se répercuter sur le fonctionnement du logiciel Solaris Security Toolkit 4.2. Il peut arriver qu'un paramètre soit défini différemment pour `ip6_send_redirects` d'un contrôle à l'autre alors qu'il devrait être identique. Supposons que vous contrôliez un système qui n'a pas subi de durcissement (Contrôle n° 1). Vous procédez ensuite au durcissement du système, vous redémarrez, vous annulez le durcissement et vous redémarrez à nouveau. Vous procédez ensuite à un nouveau contrôle du système (Contrôle n° 2).

Les résultats du contrôle devraient être identiques, à l'exception de l'horodatage. Cependant, il arrive que les deux contrôles montrent une valeur différente pour le paramètre `ip6_send_redirects` situé dans le fichier `nddconfig`. Lors du premier contrôle, le message indique que la vérification a échoué, car le paramètre est différent de 0. Lors du second contrôle, le message vous informe que la vérification a réussi, car le paramètre est égal à 0, ce qui est exact.

Palliatif : aucun.

`/etc/motd` devrait être installé en tant que fichier volatile (Bug ID 6222495)

Ce bogue du SE Solaris 10 risque de se répercuter sur le fonctionnement du logiciel Solaris Security Toolkit 4.2. Le fichier `/etc/motd` est inclus dans le package `SUNWcsr` et est doté du type de fichier `f`. Les pilotes de Solaris Security Toolkit 4.2 remplacent ce fichier, ce qui peut entraîner des erreurs et des avertissements lors de l'installation de zones et de packages au sein de ces zones.

Palliatifs

Effectuez l'une des opérations suivantes :

- Supprimez le fichier de la liste `JASS_FILES` afin de *ne pas* l'installer.
- Modifiez le type du fichier en le remplaçant par `v`, ce qui éliminera cette erreur.

Dysfonctionnements de `svc.startd` avec `optional_all` (Bug ID 6223370)

Si vous désactivez `rpcbind` puis redémarrez, les services `milestone/name-services` ne sont *pas* mis en ligne, `inetd` et d'autres services risquant eux aussi de *ne pas* se mettre en ligne. Pour connaître les manières dont ce bogue du SE Solaris 10 risque d'affecter le fonctionnement du logiciel Solaris Security Toolkit 4.2, reportez-vous aux descriptions des bogues Bug ID 6284872 et Bug ID 6222181.

Palliatifs

- Si vous souhaitez utiliser NIS, activez `rpcbind` et redémarrez. Reportez-vous au chapitre 1 du manuel Solaris Security Toolkit 4.2 Reference Manual.
- Si vous ne voulez pas utiliser le service NIS, désactivez-le. Reportez-vous au document portant sur le service de dénomination du SE Solaris 10 pour connaître la procédure de désactivation du service NIS.