Directives de sécurité d'Oracle® Solaris 11

Référence: E53924-02
Septembre 2014

Table des matières

Liste des tableaux

Utilisation de la présente documentation

- **Présentation** – Offre une vue d'ensemble des fonctions de sécurité d'Oracle Solaris et fournit des instructions pour leur utilisation en vue de sécuriser un système installé et ses applications.
- **Public visé** – Les administrateurs système, les administrateurs de sécurité, les développeurs d'application et les auditeurs qui développent, déploient ou évaluent la sécurité sur les systèmes Oracle Solaris 11.
- **Connaissances requises** – Exigences en matière de sécurité.

Bibliothèque de documentation produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=E56338.

Accès aux services de support Oracle

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

Commentaires

Faites part de vos commentaires sur cette documentation à la page suivante : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

A propos de la sécurité d'Oracle Solaris

Oracle Solaris est un système d'exploitation professionnel robuste et de qualité qui offre des fonctions de sécurité éprouvées. Doté d'un système de sécurité sophistiqué s'étendant à l'ensemble du réseau et contrôlant la manière dont les utilisateurs accèdent aux fichiers, protègent les bases de données du système et utilisent les ressources système, Oracle Solaris 11 répond aux besoins de sécurité à tous les niveaux. Alors que les systèmes d'exploitation traditionnels peuvent présenter des failles de sécurité inhérentes, la flexibilité d'Oracle Solaris 11 lui permet de remplir des objectifs de sécurité divers, pour des serveurs d'entreprise comme pour des clients de bureau. Oracle Solaris est intégralement testé et pris en charge par une multitude de systèmes SPARC et x86 d'Oracle ainsi que par des plates-formes matérielles de fournisseurs tiers.

Nouveautés Oracle Solaris 11.2 en termes de fonctions de sécurité

Cette section contient des informations destinées aux clients existants sur les nouvelles fonctions de sécurité de cette version.

- Vous pouvez évaluer la conformité de vos systèmes aux normes de sécurité à l'aide de la nouvelle commande de sécurité `compliance`. Elle vous permet d'évaluer et de présenter sous forme de rapport la conformité de votre système aux normes de sécurité standard de l'industrie, y compris la norme PCI-DSS. Pour plus d'informations, reportez-vous au manuel

“ Guide de conformité à la sécurité d’Oracle Solaris 11.2 ”, ainsi qu'à la page de manuel `compliance`(1M).

- La fonction Structure cryptographique d'Oracle Solaris est validée à FIPS 140-2, niveau 1 pour les fonctions utilisateur et noyau dans les versions Oracle Solaris 11.1 SRU 5.5 et Oracle Solaris 11.1 SRU 3.
  - Pour consulter une liste des produits Oracle certifiés FIPS, voir Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html).
  - Pour plus d'informations sur l'activation du Mode FIPS 140 sur votre système, reportez-vous à “ Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ”.
- Oracle Solaris 11.1 est certifié conforme à la norme canadienne Critères communs. Voir “Certification EAL4+ d'Oracle Solaris 11 selon les Critères communs” à la page 30.
- Le service d'audit peut utiliser Oracle Audit Vault pour stocker, passer en revue et analyser des enregistrements d'audit. Voir la section “ Utilisation du coffre d’audit Oracle et du pare-feu de base de données pour le stockage et l’analyse des enregistrements d’audit ” du manuel “ Gestion de l’audit dans Oracle Solaris 11.2 ”.
- Verified Boot protège le processus d'initialisation contre les menaces perpétrées à l'encontre des serveurs de la série Oracle SPARC T5 et des serveurs de la série Oracle SPARC T7. Pour plus d'informations, reportez-vous à la section “ Utilisation de Verified Boot ” du manuel “ Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 ”.
- Vous pouvez sécuriser les installations automatiques (AI) à l'aide de certificats et de clés destinés au serveur d'installation, à des systèmes client spécifiques, à tous les clients d'un service d'installation spécifique et à tout autre client AI. La sécurisation des AI protège le transfert des packages Oracle Solaris vers vos systèmes. Voir la section “ Augmentation de la sécurité pour des installations automatisées ” du manuel “ Installation des systèmes Oracle Solaris 11.2 ”.
- Un nouveau package d'installation de groupe est disponible : `pkg:/group/system/solaris-minimal-server`. Pour obtenir une description et un comparatif des contenus des packages de groupe, reportez-vous au document “ Oracle Solaris 11.2 Package Group Lists ”.
- Vous pouvez installer des clients Kerberos à l'aide du système AI, de sorte à ce que le client soit un système utilisant Kerberos dès la première initialisation. Voir la section “ Configuration des clients Kerberos à l’aide de l’AI ” du manuel “ Installation des systèmes Oracle Solaris 11.2 ”.
- Dans cette version, les zones physiques globales (appelées zones globales immuables) et les zones globales virtuelles (appelées zones de noyau Oracle Solaris) sont en lecture seule. Si les zones globales immuables sont légèrement plus puissantes que les zones de noyau, aucune d'elles ne peut modifier de manière permanente le matériel ou la configuration du système. Les zones en lecture seule s'initialisent plus rapidement et sont plus sécurisées que les zones autorisant les écritures.

  Dans le cadre d'une maintenance, les zones globales immuables définissent un ensemble spécial de processus appelé TCB (base informatique sécurisée). Cette base peut être

configurée via une connexion sécurisée appelée Trusted Path (chemin de confiance). Pour plus d'informations, reportez-vous au Chapitre 12, “ Configuration et administration de zones immuables ” du manuel “ Création et utilisation des zones Oracle Solaris ”. Pour plus d'informations sur les ressources de configuration des zones, reportez-vous à la section “ Présentation d’Oracle Solaris Zones ”. Reportez-vous également aux pages de manuel `mwac`(5) et `tpd`(5).

Les zones noyau Oracle Solaris sont utiles pour déployer un système conforme. Par exemple, vous pouvez configurer un système conforme, créer une archive d'ensemble et déployer l'image en tant que zone noyau. Pour plus d'informations, consultez les références suivantes : page de manuel `solaris-kz`(5), “ Création et utilisation des zones de noyau d’Oracle Solaris ”, “ Présentation d’OracleÂ Solaris Zones ” du manuel “ Présentation des environnements de virtualisation d’Oracle Solaris 11.2 ” et “ Utilisation de Unified Archives pour la récupération du système et le clonage dans Oracle Solaris 11.2 ”.

- Les nouvelles fonction des droits d'utilisateur et de processus sont les suivantes :
  - Contrôle de l'accès aux services PAM en fonction du temps et de l'emplacement
  - Rôles d'autorisation gérés à partir de rôles RBAC (ARMOR) prédéfinis
  - Profils de droits d'accès contraignant les utilisateurs à saisir un mot de passe avant d'exécuter une action privilégiée
  - Les profils de droits Capacité d'observation du réseau et Capacité d'observation du système pour l'exécution des commandes de diagnostic `ipstat`, `tcpstat`, `snoop` et `intrstat` avec privilèges et sans être `root`

  Pour plus d'informations, reportez-vous à la section “ Nouveautés relatives aux droits dans OracleÂ SolarisÂ 11.2 ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.
- La version 2 d'IKE (IKEv2) fournit le dernier protocole IKE permettant la gestion automatique par clés des paquets du réseau protégés par IPsec. Pour plus d'informations, reportez-vous à la section “ Nouveautés concernant la sécurité du réseau dans Oracle Solaris 11.2 ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”.
- Oracle Hardware Management Pack (HMP) fournit des outils de ligne de commande pour configurer et mettre à jour les microprogrammes. Pour plus d'informations sur l'utilisation sécurisée de HMP associée à d'autres produits matériels Oracle, tels que des commutateurs réseau et des cartes d'interface réseau, reportez-vous au manuel “ Guide de sécurité d’Oracle Hardware Management Pack pour Oracle Solaris ”.

Sécurité d'Oracle Solaris 11 après l'installation

Oracle Solaris est installé de manière "sécurisée par défaut" (SBD). Cette sécurisation protège le système contre les intrusions et surveille les tentatives de connexion, entre autres fonctions de sécurité.

Accès au système limité et surveillé

Comptes de l'utilisateur initial et du rôle `root` : le compte de l'utilisateur initial peut se connecter à partir de la console. Le rôle `root` est affecté à ce compte. Lors de l'installation, le mot de passe de l'utilisateur initial est identique à celui des comptes `root`.

- Une fois la connexion établie, l'utilisateur initial peut prendre le rôle `root` pour poursuivre la configuration du système. Au moment où il prend ce rôle, l'utilisateur est invité à modifier le mot de passe `root`. Notez que ni le rôle `root`, ni aucun autre rôle ne peut se connecter directement.
- Des valeurs par défaut provenant du fichier `/etc/security/policy.conf` sont assignées à l'utilisateur initial. Les valeurs par défaut incluent les profils de droits Basic Solaris User (Utilisateur de base Solaris) et Console User (Utilisateur de la console). Ces profils de droits d'accès permettent aux utilisateurs de lire ou d'écrire sur un CD ou un DVD, d'exécuter n'importe quelle commande dépourvue de privilège sur le système, et d'arrêter et de redémarrer leur système depuis la console.
- Le profil de droits System Administrator (administrateur système) est également attribué au compte de l'utilisateur initial. Sans prendre le rôle `root`, l'utilisateur initial dispose donc de certains droits d'administration, tels que le droit d'installer des logiciels et de gérer le service de noms.

Exigences relatives au mot de passe : les mots de passe utilisateur doivent comporter six caractères au minimum et comprendre au moins deux caractères alphabétiques et un caractère non alphabétique. Les mots de passe sont hachés à l'aide de l'algorithme `SHA256`. Tous les utilisateurs, y compris le rôle `root`, doivent respecter ces exigences relatives au mot de passe.

Accès au réseau limité : après l'installation, le système est protégé contre les intrusions via le réseau. La connexion à distance par l'utilisateur initial est autorisée par le biais d'une connexion chiffrée authentifiée à l'aide du protocole `ssh`. Ce protocole est le seul protocole réseau acceptant les paquets entrants. La clé `ssh` est encapsulée à l'aide de l'algorithme `AES128`. Une fois le chiffrement et l'authentification en place, l'utilisateur peut accéder au système sans interception, modification ou usurpation.

Tentatives de connexion enregistrées : le service d'audit est activé pour tous les événements `login/logout` (connexion, déconnexion, changement d'utilisateur, démarrage et arrêt d'une session `ssh` et verrouillage de l'écran) et pour toutes les connexions non attribuables (ayant échoué). Dans la mesure où le rôle `root` ne peut pas se connecter, le nom de l'utilisateur prenant un rôle `root` est enregistré dans la piste d'audit. L'utilisateur initial peut consulter les journaux d'audit grâce à un droit accordé par le biais du profil de droits System Administrator (Administrateur système).

Les protections du noyau, du fichier et du bureau sont en place

Une fois l'utilisateur initial connecté, le noyau, les systèmes de fichiers, les fichiers système et les applications du bureau sont protégés par des autorisations de fichier, des privilèges et des droits d'utilisateur. Les droits de l'utilisateur sont également appelés *contrôle d'accès basé sur les rôles* (RBAC).

Protections du noyau : de nombreux démons et commandes d'administration se voient attribuer uniquement les privilèges qui leur permettent d'aboutir. De nombreux démons sont exécutés à partir de comptes d'administration spéciaux qui ne disposent pas de privilèges `root` (`UID=0`) et qui ne peuvent pas être détournés pour effectuer d'autres tâches. Ces comptes d'administration spéciaux ne peuvent pas se connecter. Les périphériques sont protégés par des privilèges.

Systèmes de fichiers : par défaut, tous les systèmes de fichiers sont des systèmes de fichiers ZFS. La valeur `umask` de l'utilisateur est `022`. Ainsi, lorsqu'un utilisateur crée un nouveau fichier ou répertoire, seul cet utilisateur est autorisé à le modifier. Les membres du groupe de l'utilisateur sont autorisés à lire et à effectuer une recherche dans le répertoire ainsi qu'à lire le fichier. Les connexions externes au groupe de l'utilisateur peuvent lister le répertoire et lire le fichier. Les autorisations du répertoire par défaut sont `drwxr-xr-x` (`755`). Les autorisations du fichier sont `-rw-r--r--` (`644`).

Fichiers système : les fichiers de configuration système sont protégés par des autorisations de fichier. Seul le rôle `root` ou un utilisateur disposant du droit de modifier un fichier système spécifique peut modifier un fichier système.

Applets de bureau : les applets de bureau sont protégés par une gestion des droits. Par conséquent, les actions d'administration, telles que l'ajout d'imprimantes distantes dans le gestionnaire d'impression, sont limitées aux utilisateurs et aux rôles disposant de droits d'administration pour l'impression.

Oracle Hardware Management Package

Oracle Hardware Management Package fournit un ensemble d'utilitaires de configuration, de gestion et de contrôle des serveurs Oracle. Cet ensemble d'outils à valeur ajoutée adaptés au matériel Oracle est toujours disponible. Il peut automatiquement fournir à ILOM certaines informations relatives au matériel afin de compléter sa vue du matériel du système. Pour plus d'informations sur les utilitaires et la sécurité, voir Systems Management and Diagnostics Documentation" (http://www.oracle.com/goto/ohmp/docs).

Sécurité configurable d'Oracle Solaris

Outre les bases solides fournies par les paramètres de sécurité par défaut d'Oracle Solaris, la sécurisation d'un système Oracle Solaris est hautement configurable afin de répondre à une palette d'exigences en matière de sécurité.

Les sections suivantes constituent une brève introduction aux fonctions de sécurité d'Oracle Solaris. Les descriptions contiennent des renvois à des explications plus détaillées et à des procédures figurant dans ce guide et dans d'autres guides d'administration système d'Oracle Solaris, lesquels présentent les fonctions concernées.

Protection des données

Oracle Solaris empêche les données de s'initialiser lors de l'installation, de l'utilisation et de l'archivage.

Autorisations de fichier et entrées de contrôle d'accès

Les autorisations UNIX par défaut affectées à chaque objet d'un système de fichiers constituent la première ligne de défense pour la protection des objets de ce système de fichiers. Les autorisations UNIX prennent en charge l'affectation de droits d'accès uniques au propriétaire d'un objet, à un groupe affecté à l'objet et à toute autre personne. En outre, le système de fichiers par défaut ZFS prend en charge les listes de contrôle d'accès (ACL). Ces dernières contrôlent de manière plus détaillée l'accès aux objets individuels ou aux groupes d'objets des systèmes de fichiers.

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour obtenir un aperçu des autorisations de fichier, reportez-vous à la section " Utilisation des autorisations UNIX pour protéger les fichiers " du manuel " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 ".
- Pour obtenir une vue d'ensemble et des exemples de protection de fichiers ZFS, reportez-vous au Chapitre 7, " Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ", ainsi qu'aux pages de manuel correspondantes.
- Pour obtenir des instructions sur la configuration des ACL sur des fichiers ZFS, reportez-vous à la page de manuel `chmod`(1).

Services cryptographiques

Les fonctions de structure cryptographique et de structure de gestion des clés (KMF) d'Oracle Solaris fournissent des référentiels centralisés pour les services cryptographiques et la gestion des clés. Le matériel, les logiciels et les utilisateurs finaux ont directement accès à des algorithmes optimisés. KMF fournit une interface unifiée pour différents mécanismes de stockage, utilitaires d'administration et interfaces de programmation de diverses infrastructures de clé publique (PKI).

La structure cryptographique fournit un magasin d'algorithmes et de bibliothèques PKCS #11 commun pour traiter les exigences en matière de cryptographie. Les bibliothèques PKCS #11 sont implémentées conformément à la norme RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). Les services cryptographiques, tels que le chiffrement et le déchiffrement de fichiers, sont accessibles aux utilisateurs standard.

KMF offre des outils et des interfaces de programmation permettant la gestion centralisée des objets de clé publique tels que les certificats X.509 et les paires de clés publique/privée. Les formats de stockage de ces objets peuvent varier. KMF offre également un outil de gestion des stratégies qui définissent l'utilisation de certificats X.509 par des applications. KMF prend en charge des plug-ins de fournisseurs tiers.

Pour plus d'informations, reportez-vous aux références suivantes :

- Pages de manuel connexes : `cryptoadm`(1M), `encrypt`(1), `mac`(1), `pktool`(1) et `kmfcfg`(1).
- Pour obtenir un aperçu des services cryptographiques, reportez-vous au Chapitre 1, “ Structure cryptographique ” du manuel “ Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 ” et au Chapitre 4, “ Structure de gestion des clés ” du manuel “ Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 ”.
- Pour obtenir des exemples d'utilisation de la structure cryptographique, reportez-vous au Chapitre 3, “ Structure cryptographique ” du manuel “ Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 ”, ainsi qu'aux pages de manuel correspondantes.
- Pour activer le fournisseur FIPS 140 de structure cryptographique, reportez-vous à la section “ Création d’un environnement d’initialisation compatible FIPS 140 ” du manuel “ Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 ”.

Système de fichiers ZFS Oracle Solaris

Le système de fichiers ZFS est le système de fichiers par défaut dans Oracle Solaris 11. Le système de fichiers ZFS modifie radicalement la manière dont les systèmes de fichiers Oracle Solaris sont administrés. Le système ZFS est robuste, évolutif et facile à administrer. En raison de la légèreté des systèmes de fichiers créés dans le système ZFS, vous pouvez facilement définir des quotas et des espaces réservés. Les autorisations UNIX et les ACL protègent les fichiers. Vous pouvez chiffrer l'intégralité du jeu de données dès sa création. La gestion des droits Oracle Solaris prend en charge l'administration déléguée des jeux de données ZFS.

Autrement dit, les utilisateurs disposant d'un ensemble limité de privilèges peuvent gérer les jeux de données ZFS.

Pour plus d'informations, reportez-vous aux références suivantes :

- " Utilisateur Rights Management " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- Chapitre 1, " Système de fichiers Oracle Solaris ZFS (introduction) " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 "
- " Différences entre les systèmes de fichiers Oracle Solaris ZFS et classiques " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 "
- Chapitre 5, " Gestion des systèmes de fichiers Oracle Solaris ZFS " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 "
- " Administration à distance de ZFS avec le shell sécurisé " du manuel " Gestion de l'accès au shell sécurisé dans Oracle Solaris 11.2 "
- Pages de manuel connexes : `zfs`(1M) et `zfs`(7FS).

Java Cryptography Extension

Java fournit l'application Java Cryptography Extension (JCE), destinée aux développeurs d'applications Java. Pour plus d'informations, voir Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

Protection et isolation des applications

Les applications peuvent constituer des points d'entrée pour les programmes et utilisateurs malveillants. Dans Oracle Solaris, ces menaces sont atténuées par l'utilisation de privilèges et le confinement d'applications au sein de zones. Les applications peuvent être exécutées uniquement avec les privilèges nécessaires. Ainsi, un utilisateur malveillant ne dispose pas de privilèges root pour accéder au reste du système. Les zones peuvent limiter la portée d'une attaque. Les attaques perpétrées contre des applications situées dans une zone non globale peuvent uniquement affecter les processus de cette zone, et non le système hôte de la zone.

La randomisation du format d'espace d'adressage (ASLR) et l'utilitaire de gestion des services (SMF) sont d'autres fonctions protégeant les applications. La fonction ASLR complique la tâche des intrus tentant de pirater un exécutable, tandis que les fonctions SMF permettent aux administrateurs de limiter le démarrage, l'arrêt et l'utilisation d'une application.

Privilèges dans Oracle Solaris

Les privilèges sont des droits détaillés et discrets liés à des processus et sont appliqués dans le noyau. Oracle Solaris en définit plus de 80, allant de privilèges élémentaires tels que `file_read`

à des privilèges plus spécialisés tels que `proc_clock_highres`. Ces privilèges sont accordés à un processus, un utilisateur, ou un rôle. De nombreux commandes et démons Oracle Solaris fonctionnent uniquement avec les privilèges nécessaires pour leur permettre d'accomplir leur tâche. Des programmes prenant en charge les étiquettes peuvent empêcher les intrus d'obtenir plus de privilèges que le programme lui-même n'en utilise.

L'utilisation de privilèges est également appelée *gestion des droits de processus*. Les privilèges permettent aux entreprises de préciser (et ainsi limiter) les privilèges accordés aux services et aux processus qui s'exécutent sur leurs systèmes.

Pour plus d'informations, reportez-vous aux références suivantes :

- " Processus Rights Management " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- Chapitre 2, " Developing Privileged Applications " du manuel " Developer's Guide to Oracle Solaris 11 Security "
- Pages de manuel connexes : `ppriv`(1) et `privileges`(5).

Oracle Solaris Zones

La technologie de partitionnement du logiciel Oracle Solaris Zones permet de conserver le modèle de déploiement d'une application par serveur tout en partageant les ressources matérielles.

Les zones sont des environnements d'exploitation virtualisés permettant à plusieurs applications de s'exécuter indépendamment les unes des autres sur le même matériel physique. Cet isolement empêche que des processus qui s'exécutent dans une zone ne surveillent ou n'affectent des processus qui s'exécutent dans d'autres zones ; il empêche également les processus de voir leurs données réciproques ou de manipuler le matériel sous-jacent. En outre, les zones fournissent une couche d'abstraction qui sépare les applications des attributs physiques du système sur lequel elles sont déployées, telles que les chemins d'accès aux périphériques physiques et les noms d'interface réseau.

Vous pouvez configurer dans Oracle Solaris 11.2 des systèmes de fichiers root immuables.

Pour plus d'informations, reportez-vous aux références suivantes :

- " Configuration des zones en lecture seule " du manuel " Création et utilisation des zones Oracle Solaris "
- " Présentation d'Oracle Solaris Zones "
- Pages de manuel connexes : `brands`(5), `zoneadm`(1M) et `zonecfg`(1M).

Randomisation du format d'espace d'adressage

La randomisation du format d'espace d'adressage (ASLR) crée de manière aléatoire les adresses utilisées par un programme donné. La fonction ASLR peut parer certains types d'attaques basées sur la connaissance de l'emplacement exact de certains intervalles de mémoire et peut détecter l'opération lorsque le programme est arrêté. Pour plus d'informations, reportez-vous à la section " Randomisation du format d'espace d'adressage " du manuel " Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 " et à la section "Vérification de l'activation de la fonction ASLR" à la page 33.

Utilitaire de gestion des services

Les *services* sont des applications constamment en cours d'exécution. Un service peut représenter une application en cours d'exécution, l'état du logiciel d'un périphérique ou un ensemble d'autres services. L'utilitaire de gestion des services (SMF) d'Oracle Solaris permet d'ajouter, de supprimer, de configurer et de gérer les services. La fonction SMF utilise la gestion des droits pour contrôler l'accès aux fonctions de gestion des services sur le système. En particulier, SMF se sert d'autorisations pour déterminer qui peut gérer un service et quelles fonctions cette personne peut exécuter.

SMF permet aux entreprises de contrôler l'accès aux services ainsi que de contrôler la façon dont ces services sont démarrés, arrêtés et actualisés.

Pour plus d'informations, reportez-vous aux références suivantes :

- " Gestion des services système dans Oracle Solaris 11.2 "
- " Procédure d'assignation de privilèges propres au shell Apache du serveur Web " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- Pages de manuel connexes : `svcadm`(1M), `svcs`(1) et `smf`(5).

Protection des utilisateurs et assignations de droits supplémentaires

Les utilisateurs se voient attribuer un ensemble basique de privilèges, de profils de droits et d'autorisations provenant du fichier `/etc/security/policy.conf`, à l'instar de l'utilisateur initial décrit dans la section "Accès au système limité et surveillé" à la page 14. Ces droits sont configurables. Vous pouvez refuser d'accorder des droits basiques et d'étendre les droits d'un utilisateur.

Oracle Solaris protège les utilisateurs à l'aide d'exigences à complexité variable en matière de mot de passe, d'une authentification configurable selon les différentes exigences du site et d'une gestion des droits des utilisateurs à l'aide de profils de droits, d'autorisations et de privilèges

limitant et répartissant les droits d'administration à des utilisateurs de confiance. En outre, les comptes spéciaux partagés, ou *rôles*, accordent ces droits d'administration à l'utilisateur lorsqu'il prend le rôle. Le package Authorization Rules Managed On RBAC (ARMOR) fournit des rôles prédéfinis.

Mots de passe et contraintes de mot de passe

Des mots de passe utilisateur forts protègent contre les attaques en force cherchant à deviner les mots de passe.

Oracle Solaris propose diverses fonctions permettant de configurer les mots de passe conformément aux exigences de votre site. Vous pouvez en spécifier la longueur, le contenu, la fréquence de modification et les exigences de modification, et conserver un historique des mots de passe. Un dictionnaire des mots de passe à éviter vous est fourni. Plusieurs algorithmes de hachage de mots de passe sont disponibles. La valeur par défaut est SHA256.

Pour plus d'informations, reportez-vous aux références suivantes :

- “ Gestion du contrôle de connexion ” du manuel “ Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 ”
- “ Sécurisation des connexions et des mots de passe ” du manuel “ Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 ”
- Pages de manuel connexes : `passwd`(1) et `crypt.conf`(4).

Modules d'authentification enfichables

La structure PAM (module d'authentification enfichable) permet aux administrateurs de coordonner et de configurer les exigences d'authentification des utilisateurs en termes de comptes, d'informations d'identification, de sessions et de mots de passe, sans modifier les services nécessitant une authentification.

La structure PAM permet aux entreprises de personnaliser les paramètres d'authentification des utilisateurs ainsi que la fonction de gestion des comptes, des sessions et des mots de passe. Les services d'entrée système tels que `login` et `ssh` utilisent la structure PAM pour sécuriser tous les points d'entrée des systèmes récemment installés. Cette architecture autorise le remplacement ou la modification de modules d'authentification sur le terrain afin de permettre la sécurisation du système lorsque de nouvelles vulnérabilités sont détectées, et ce sans nécessiter de modification dans les services système utilisant la structure PAM.

Oracle Solaris fournit un vaste ensemble de modules et configurations PAM pour répondre à la plupart des stratégies du site. Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 1, “ Utilisation de modules d’authentification enfichables ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”

- " Writing Applications That Use PAM Services " du manuel " Developer's Guide to Oracle Solaris 11 Security "
- Page de manuel `pam.conf`(4)

Gestion des droits des utilisateurs

Dans Oracle Solaris, les droits des utilisateurs sont régis par le principe de sécurité du moindre privilège. En fonction de leurs besoins et exigences spécifiques, les entreprises peuvent accorder des droits d'administration aux utilisateurs ou rôles de façon sélective. En cas de besoin, elles peuvent également refuser d'accorder certains droits aux utilisateurs. Les droits sont implémentés en tant que privilèges liés à des processus et autorisations par rapport à des utilisateurs ou des méthodes SMF. Les profils de droits représentent un moyen pratique de collecter des privilèges et autorisations dans un bundle de droits liés.

Pour plus d'informations, reportez-vous aux références suivantes :

- " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- Pages de manuel connexes : `auths`(1), `privileges`(5). `profiles`(1), `rbac`(5), `roleadd`(1M), `roles`(1) et `user_attr`(4).

Sécurisation des communications réseau

Les communications réseau peuvent être protégées par des fonctionnalités, telles que des pare-feux, des wrappers TCP liés à des applications en réseau, ou des connexions à distance chiffrés et authentifiées.

Filtrage des paquets

Le filtrage de paquets assure une protection de base contre les attaques potentielles via le réseau. Oracle Solaris inclut la fonction IP Filter et des wrappers TCP.

Pare-feu

La fonction IP Filter d'Oracle Solaris crée un pare-feu destiné à repousser les attaques basées sur le réseau.

Plus précisément, IP Filter permet le filtrage de paquets avec état et est capable de filtrer les paquets en fonction de leur adresse IP ou du réseau, du port, du protocole, de l'interface réseau et de la direction du trafic. Elle permet également le filtrage de paquets sans état, ainsi que la

création et la gestion de pools d'adresses. En outre, IP Filter est capable d'effectuer la translation d'adresse de réseau (NAT) et la translation d'adresse de port (PAT).

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour obtenir un aperçu d'IP Filter, reportez-vous au Chapitre 4, “ A propos d’IP Filter dans Oracle Solaris ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”.
- Pour obtenir des exemples d'utilisation d'IP Filter, reportez-vous au Chapitre 5, “ Configuration d’IP Filter ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”, ainsi qu'aux pages de manuel correspondantes.
- Pour plus d'informations et pour consulter des exemples illustrant la syntaxe du langage de règles IP Filter, reportez-vous à la page de manuel `ipnat`(4).
- Pages de manuel connexes : `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) et `ipf`(4).

Wrappers TCP

Les wrappers TCP permettent de contrôler l'accès aux services Internet. Lorsque divers services internet (`inetd`) sont activés, le démon `tcpd` recherche l'adresse d'un hôte demandant un service réseau particulier par rapport à un ACL. Les demandes sont accordées ou refusées en conséquence. Les wrappers TCP consignent également les demandes de services réseau émises par les hôtes dans l'utilitaire `syslog`, assurant ainsi une fonction de surveillance utile.

Les fonctions Shell sécurisé (`ssh`) et `sendmail` d'Oracle Solaris sont configurées pour utiliser des wrappers TCP. Les services réseau disposant d'un mappage bi-univoque pour les fichiers exécutables, tels que `proftpd` et `rpcbind`, sont des candidats aux wrappers TCP.

Les wrappers TCP prennent en charge un langage de règles de configuration riche qui permet aux entreprises de définir des stratégies de sécurité non seulement à l'échelle globale, mais aussi à l'échelle des différents services. L'accès aux services peut être autorisé ou restreint sur la base du nom de l'hôte, de l'adresse IPv4 ou IPv6, du nom du groupe réseau, du réseau, voire même du domaine DNS.

Pour plus d'informations sur les wrappers TCP, reportez-vous aux rubriques suivantes :

- “Utilisation des wrappers TCP” à la page 49
- Pour plus d'informations et pour consulter des exemples illustrant la syntaxe du langage de contrôle d'accès des wrappers TCP, reportez-vous à la page de manuel `hosts_access`(4).
- Pages de manuel connexes : `tcpd`(1M) et `inetd`(1M).

Accès à distance

Les attaques distantes peuvent endommager un système et un réseau. Oracle Solaris assure une protection renforcée des transmissions réseau. Les fonctions de défense comprennent des

contrôles du chiffrement et de l'authentification dans le cadre de la transmission de données, de l'authentification de connexion et de la désactivation de services distants inutiles.

IPsec et IKE

La sécurité IP (IPsec) protège les transmissions réseau en authentifiant les paquets IP, en les chiffrant ou en effectuant ces deux opérations. IPsec étant mis en oeuvre à un niveau bien inférieur au niveau de l'application, les applications Internet peuvent l'utiliser sans que des modifications de leur code ne soient nécessaires.

IPsec et son protocole d'échange de clés IKE utilisent des algorithmes de la structure cryptographique. En outre, la structure cryptographique fournit un keystore central. Lorsqu'IKE est configuré pour utiliser le metaslot, les entreprises ont la possibilité de stocker les clés sur un disque, sur un keystore matériel connecté ou dans un keystore logiciel appelé *softtoken*.

IPsec et IKE sont installés mais désactivés par défaut, il est donc nécessaire de les configurer. Lorsqu'il est administré correctement, IPsec est un outil efficace de sécurisation du trafic réseau.

Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 6, “ A propos de l’architecture de sécurité IP ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- Chapitre 7, “ Configuration d’IPsec ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- “ IPsec et FIPS 140 ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- Chapitre 8, “ A propos d’Internet Key Exchange ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- Chapitre 9, “ Configuration d’IKEv2 ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- Pages de manuel connexes : `ipsecconf`(1M) et `in.iked`(1M).

Shell sécurisé

Par défaut, la fonction Shell sécurisé d'Oracle Solaris est le seul mécanisme d'accès distant actif sur un nouveau système installé. Tous les autres services réseau sont désactivés ou en écoute seule.

Shell sécurisé crée un canal de communication chiffré entre les systèmes. Shell sécurisé peut également être utilisé comme un réseau privé virtuel (VPN) à la demande capable d'acheminer le trafic système X Window ou de connecter des numéros de port individuel entre un système local et des systèmes distants via un lien réseau authentifié et chiffré.

De cette manière, Shell sécurisé empêche les intrus potentiels de lire des communications interceptées et empêche un adversaire d'usurper le système.

Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 1, “ Utilisation du shell sécurisé (Tâches) ” du manuel “ Gestion de l’accès au shell sécurisé dans Oracle Solaris 11.2 ”
- “ Secure Shell et FIPS 140 ” du manuel “ Gestion de l’accès au shell sécurisé dans Oracle Solaris 11.2 ”
- Pages de manuel connexes : `ssh`(1), `sshd`(1M), `sshd_config`(4) et `ssh_config`(4).

Service Kerberos

La fonction Kerberos d'Oracle Solaris permet une connexion unique et des transactions sécurisées, même sur des réseaux hétérogènes au sein desquels les systèmes exécutent différents systèmes d'exploitation et le service Kerberos.

Le service Kerberos d'Oracle Solaris est basé sur le protocole d'authentification réseau Kerberos V5 développé au Massachusetts Institute of Technology (MIT). Le service assure l'authentification fiable des utilisateurs, et préserve l'intégrité et la confidentialité. A l'aide du service Kerberos, vous pouvez vous connecter une fois et accéder à d'autres systèmes, exécuter des commandes, échanger des données et transférer des fichiers en toute sécurité. En outre, le service permet aux administrateurs de limiter l'accès aux services et systèmes.

Pour plus d'informations, reportez-vous aux références suivantes :

- “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”
- “ Algorithmes FIPS 140 et types de chiffrement Kerberos ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”
- Pages de manuel connexes : `kadmin`(1M), `kdcmgr`(1M), `kerberos`(5), `kinit`(1) et `krb5.conf`(4).

Mise à jour de la sécurité du système

Oracle Solaris propose les fonctions suivantes pour mettre à jour la sécurité d'un système :

- Verified Boot – Sécurise le processus d'initialisation. La fonction Verified Boot est désactivée par défaut.
- Vérification des packages – Vérifie que les packages installés sont identiques aux packages du référentiel source.
- Service d'audit - Audite l'accès au système et son utilisation. L'audit est activé par défaut.
- Vérification de l'intégrité des fichiers – Les manifestes BART peuvent répertorier chaque fichier du système. Des comparaisons des manifestes permettent de vérifier si l'intégrité des fichiers est à jour.

- Fichiers journaux – SMF fournit des fichiers journaux pour chaque service. L'utilitaire `syslog` fournit un fichier central d''attribution de nom et de configuration des journaux pour les services système, et peut également informer les administrateurs des événements critiques. D'autres fonctions, tels que l'audit, créent également leurs propres journaux.
- Rapports de conformité – Oracle Solaris fournit plusieurs tests d'évaluation de la sécurité permettant d'évaluer votre système. Ces évaluations créent des rapports qui vous aident à évaluer la sécurisation du système.

Verified Boot

Verified Boot est une fonction Oracle Solaris permettant de sécuriser le processus d'initialisation d'un système. Elle protège le système contre toutes sortes de menaces telles que l'installation de modules de noyau non autorisés et de chevaux de Troie. Verified Boot est désactivée par défaut.

Pour plus d'informations, reportez-vous au Chapitre 2, “ Protection de l’intégrité des systèmes Oracle Solaris ” du manuel “ Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 ”.

Vérification de l'intégrité des packages

Après l'installation ou la mise à jour de packages, vous pouvez exécuter la commande `pkg verify` pour vérifier que les packages installés sur votre système sont identiques aux packages du référentiel source.

Pour plus d'informations, reportez-vous à la page de manuel `pkg`(1) et à la section “Vérification des packages” à la page 33.

Service d'audit

Oracle Solaris fournit un service d'audit qui collecte des données sur l'accès au système et son utilisation. Les données d'audit fournissent un journal horodaté fiable des événements système associés à la sécurité. Ces données peuvent ensuite être utilisées pour déterminer la responsabilité quant aux actions effectuées sur un système.

La réalisation d'audits est une exigence fondamentale pour l'évaluation de la sécurité, la validation, la conformité et les organismes de certification. L'audit peut également constituer un moyen de dissuasion vis-à-vis d'intrus potentiels.

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour obtenir la liste des pages de manuel portant sur l'audit, reportez-vous au Chapitre 7, “ Référence d’audit ” du manuel “ Gestion de l’audit dans Oracle Solaris 11.2 ”.

- Pour obtenir des instructions, reportez-vous à la section “Réalisation d'un audit des événements importants en plus de la connexion/déconnexion” à la page 45 et aux pages de manuel.
- Pour obtenir un aperçu de la procédure d'audit, reportez-vous au Chapitre 1, “ A propos de l’audit dans OracleÂ Solaris ” du manuel “ Gestion de l’audit dans Oracle Solaris 11.2 ”.
- Pour plus d'informations sur les tâches d'audit, reportez-vous au Chapitre 3, “ Gestion du service d’audit ” du manuel “ Gestion de l’audit dans Oracle Solaris 11.2 ”.

Vérification de l'intégrité des fichiers

La fonction BART d'Oracle Solaris permet de valider de manière exhaustive des systèmes en effectuant des vérifications des systèmes se situant au niveau des fichiers et réparties dans le temps. Après l'installation, la commande `pkg verify` permet de confirmer que le contenu du package source et de destination est identique. Une fois les packages vérifiés, les manifestes BART peuvent facilement (et de manière fiable) rassembler des informations sur les fichiers d'un système.

BART est utile pour gérer l'intégrité d'un système ou d'un réseau de systèmes. Les fichiers d'un système peuvent être comparés aux fichiers d'origine ainsi qu'à d'autres fichiers de ce système. Les rapports peuvent indiquer qu'un système n'a pas été corrigé à l'aide d'un patch, qu'un intrus a installé des fichiers non autorisés ou a modifié les autorisations ou le contenu de fichiers sensibles, tels que les fichiers possédés par un utilisateur `root`.

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour obtenir des instructions, reportez-vous aux sections “Vérification de l'intégrité des fichiers à l'aide de l'utilitaire BART” à la page 58, “Vérification de l'intégrité des fichiers à l'aide de l'utilitaire BART” à la page 58, ainsi qu'aux pages de manuel correspondantes.
- Pour obtenir un aperçu de BART, reportez-vous au Chapitre 2, “ Vérification de l’intégrité des fichiers à l’aide de l’utilitaire BART ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”.
- Pour obtenir des exemples d'utilisation de BART, reportez-vous à la section “ A propos de l’utilisation de BART ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”, ainsi qu'aux pages de manuel correspondantes.
- Pages de manuel connexes : `bart`(1M), `bart_rules`(4) et `bart_manifest`(4).

Fichiers journaux

La fonction SMF (utilitaire de gestion des services) d'Oracle Solaris consigne dans un journal le statut de ses services un par un. De nombreux services, tels que l'audit et Shell sécurisé, élaborent leurs propres journaux. Le démon `syslog` ou `rsyslog` rédige un journal centralisé

qui informe et alerte les administrateurs en cas d'erreur critique survenue dans de nombreux services. Par exemple, l'audit peut être configuré pour écrire des enregistrements d'audit dans l'utilitaire `syslog`. Pour plus d'informations, reportez-vous aux pages de manuel `syslogd`(1M) et `syslog.conf`(4).

Conformité aux normes de sécurité

La commande `compliance assess` fournit un instantané de la sécurisation de votre système. Les rapports issus des évaluations suggèrent des modifications propres à votre système afin de se conformer aux tests d'évaluation de la sécurité. Pour plus d'informations, reportez-vous au manuel “ Guide de conformité à la sécurité d’Oracle Solaris 11.2 ” et à la page de manuel `compliance`(1M).

Sécurité étiquetée

La sécurité étiquetée de Oracle Solaris est fournie par la fonction Trusted Extensions.

Fonction Trusted Extensions dans Oracle Solaris

La fonction Trusted Extensions d'Oracle Solaris est une couche de technologie d'étiquetage sécurisée optionnelle permettant de distinguer les stratégies de sécurité des données de la propriété des données. Trusted Extensions prend en charge aussi bien les stratégies de contrôle d'accès discrétionnaire (DAC) traditionnelles basées sur la propriété que les stratégies de contrôle d'accès obligatoire (MAC) basées sur les étiquettes. Lorsque la couche Trusted Extensions n'est pas activée, toutes les étiquettes sont égales, de sorte que le noyau n'est pas configuré pour appliquer les politiques MAC. Lorsque les stratégies MAC basées sur les étiquettes sont activées, tous les flux de données sont restreints et soumis à une comparaison entre les étiquettes associées aux processus sollicitant l'accès (les sujets) et celles associées aux objets contenant les données.

L'implémentation de Trusted Extensions se distingue par sa capacité à fournir un haut niveau de sécurité tout en maximisant la compatibilité et en minimisant les coûts. Trusted Extensions fait partie de la “Certification EAL4+ d'Oracle Solaris 11 selon les Critères communs” à la page 30.

Trusted Extensions répond aux exigences des Critères communs en termes de package de sécurité étiquetée (LSP). Voir “Certification EAL4+ d'Oracle Solaris 11 selon les Critères communs” à la page 30.

Pour plus d'informations, reportez-vous aux références suivantes :

- Pour plus d'informations sur la configuration et la maintenance de Trusted Extensions, reportez-vous au manuel “ Configuration et administration de Trusted Extensions ”.
- Pages de manuel connexes :`trusted_extensions`(5), `labeladm`(1M) et `labeld`(1M).

Système de fichiers étiqueté

Par défaut, une étiquette unique est attribuée aux systèmes de fichiers dans une zone. Vous pouvez créer un jeu de données ZFS multiniveau, le monter sur un système Trusted Extensions et, si vous disposez des autorisations nécessaires, passer les fichiers de ce jeu de données à un niveau supérieur ou inférieur. Pour plus d'informations, reportez-vous à la section “ Jeux de données multiniveau pour la modification d’étiquette de fichiers ” du manuel “ Configuration et administration de Trusted Extensions ”.

Communications réseau étiquetées

Trusted Extensions étiquette les communications réseau. Les flux de données sont restreints en fonction d'une comparaison entre les étiquettes associées aux extrémités du réseau d'origine et du réseau de destination. Les passerelles et pas intermédiaires doivent également être étiquetés pour permettre le passage des informations sous l'étiquette de la communication. Les jeux de données NFS et ZFS multiniveau fournissent des fonctionnalités supplémentaires sur un réseau.

Pour plus d'informations, reportez-vous aux références suivantes :

- “ Configuration des interfaces réseau dans TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”
- Chapitre 15, “ Gestion d’un réseau de confiance ” du manuel “ Configuration et administration de Trusted Extensions ”
- Chapitre 16, “ Gestion des réseaux dans TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”

Bureau multiniveau Trusted Extensions

Contrairement à la plupart des autres systèmes d'exploitation multiniveau, Trusted Extensions inclut un bureau multiniveau. Les utilisateurs peuvent être configurés afin de voir uniquement leur étiquettes autorisées. Chaque étiquette peut être configurée de façon à exiger un mot de passe distinct.

Pour plus d'informations, reportez-vous au manuel “ Guide de l’utilisateur de Trusted Extensions ”. Pour configurer les utilisateurs, reportez-vous au Chapitre 11, “ Gestion des utilisateurs, des droits et des rôles dans TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”.

Certification EAL4+ d'Oracle Solaris 11 selon les Critères communs

D'après le schéma canadien d'évaluation et de certification selon les Critères communs, Oracle Solaris 11 a obtenu la certification EAL4 (niveau 4 d'assurance de l'évaluation) augmenté (EAL4+). Il s'agit également du plus haut niveau d'évaluation reconnu par 26 pays dans le cadre du CCRA (Common Criteria Recognition Arrangement).

La certification concerne le profil de protection du système d'exploitations (OSPP) et inclut les packages étendus suivants :

- Advanced Management
- Extended Identification and Authentication (EIA)
- Sécurité étiquetée
- Virtualization

Pour plus d'informations sur la certification, consultez les références suivantes :

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

Stratégie de sécurité du site et pratiques

Pour garantir la sécurité du système ou du réseau de systèmes, un site doit mettre en place une stratégie de sécurité s'appuyant sur des pratiques de sécurité. Si vous développez des programmes ou installez des programmes tiers, vous devez développer et installer ces programmes de manière sécurisée.

Pour plus d'informations, reportez-vous aux références suivantes :

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- Annexe A, “ Secure Coding Guidelines for Developers ” du manuel “ Developer’s Guide to Oracle Solaris 11 Security ”
- Annexe A, “ Stratégie de sécurité du site ” du manuel “ Configuration et administration de Trusted Extensions ”
- “ Application des exigences de sécurité ” du manuel “ Configuration et administration de Trusted Extensions ”
- Sécurisation de votre code (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ CHAPITRE 2

Configuration de la sécurité d'Oracle Solaris

Ce chapitre décrit les opérations à effectuer pour configurer la sécurité sur votre système. Ce chapitre traite de l'installation des packages, de la configuration du système lui-même ainsi que de la configuration de différents sous-systèmes et applications supplémentaires dont vous êtes susceptible d'avoir besoin, comme par exemple IPsec.

Installation du SE Oracle Solaris

Le SE Oracle Solaris est installé en sélectionnant à partir d'un référentiel de packages un jeu de packages appelé *groupe*. Des groupes différents fournissent des packages à usages multiples, tels que des serveurs multi-usage, des systèmes installés de manière minimale et des systèmes de bureau. Les packages sont signés et leur transfert sécurisé peut être vérifié.

Lorsque vous installez le SE Oracle Solaris, sélectionnez comme suit le média devant installer le package de *groupe* approprié :

- **Oracle Solaris Large Server** : le manifeste par défaut en cas d'installation à l'aide du programme d'installation automatisée (AI) et le programme d'installation en mode texte installent tous deux le groupe `group/system/solaris-large-server`, qui fournit un environnement Oracle Solaris pour serveur grande capacité.
- **Oracle Solaris Small Server :** le programme d'installation automatisée (AI) et le programme d'installation en mode texte peuvent éventuellement installer le groupe `group/system/solaris-small-server`, qui fournit un environnement de ligne de commande utile auquel vous pouvez ajouter des packages.

- **Oracle Solaris Minimal Server :** le programme d'installation automatisée (AI) et le programme d'installation en mode texte peuvent éventuellement installer le groupe `group/system/solaris-minimal-server`, qui fournit un environnement de ligne de commande minimal auquel vous pouvez ajouter les packages que vous souhaitez.
- **Oracle Solaris Desktop :** le média Live Media installe le groupe `group/system/solaris-desktop`, qui fournit un environnement de bureau Oracle Solaris 11.

  Pour créer un système de bureau en vue d'une utilisation centralisée, ajoutez le groupe `group/feature/multi-user-desktop` au serveur du bureau. Pour plus d'informations, reportez-vous à l'article " Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment ".

Pour plus d'informations sur l'installation automatisée à l'aide du programme d'installation automatisée (AI), reportez-vous à la Partie III, " Installation à l'aide d'un serveur d'installation " du manuel " Installation des systèmes Oracle Solaris 11.2 ".

Pour vous aider dans votre choix de média, reportez-vous aux guides relatifs à l'installation et au contenu des packages suivants :

- " Installation des systèmes Oracle Solaris 11.2 "
- " Création d'une image d'installation personnalisée d'Oracle Solaris 11.2 "
- " Ajout et mise à jour de logiciels dans Oracle Solaris 11.2 "
- " Oracle Solaris 11.2 Package Group Lists "

Sécurisation initiale du système

Il est recommandé d'effectuer les tâches suivantes dans l'ordre. A ce stade, le SE Oracle Solaris est installé et seul l'utilisateur initial pouvant prendre le rôle `root` a accès au système.

TABLEAU 2-1 Sécurisation de la liste des tâches système

Tâche	Description	Pour obtenir des instructions
1. Vérification des packages sur le système.	Vérifie que les packages de la source de l'installation sont identiques aux packages installés.	"Vérification des packages" à la page 33
2. Vérification de la protection des exécutables.	Vérifie que la fonction ASLR est activée.	"Vérification de l'activation de la fonction ASLR" à la page 33
3. Protection des paramètres du matériel sur le système.	Protège le matériel en exigeant un mot de passe pour toute modification de paramètres matériels. Sur un serveur x86, l'accès au menu GRUB est contrôlé. Sur un serveur SPARC, la commande `eeprom` protège le matériel.	" Contrôle de l'accès au matériel du système " du manuel " Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 "
3. Désactivation des services non utilisés.	Empêche l'exécution des processus qui ne font pas partie des fonctions indispensables pour le système.	"Désactivation des services non utilisés" à la page 34

Tâche	Description	Pour obtenir des instructions
5. Interdiction de la mise hors tension du système par le propriétaire du poste de travail.	Empêche l'utilisateur de la console d'arrêter ou de suspendre le système.	“Désactivation de la possibilité pour les utilisateurs de gérer l'alimentation” à la page 35
6. Création d'un message d'avertissement de connexion reflétant la stratégie de sécurité de votre site.	Avertit les utilisateurs que le système est surveillé avant et après l'authentification.	“Placement d'un message de sécurité dans les fichiers bannière” à la page 36 “Placement d'un message de sécurité dans l'écran de connexion au bureau” à la page 37

▼ Vérification des packages

Immédiatement après l'installation, validez l'installation en contrôlant les packages.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Consultez le journal d'installation.**

2. **Exécutez la commande `pkg verify`.**

   Pour conserver un enregistrement, envoyez le résultat de la commande dans un fichier.

   ```
   # pkg verify > /var/pkgverifylog
   ```

3. **Consultez le journal pour vérifier s'il y a des erreurs.**

4. **Si vous trouvez des erreurs, réinstallez à partir du média ou corrigez les erreurs.**

Voir aussi Pour plus d'informations, reportez-vous aux pages de manuel `pkg`(1) et `pkg`(5). Les pages de manuel présentent des exemples d'utilisation de la commande `pkg verify`.

▼ Vérification de l'activation de la fonction ASLR

Des instructions exécutables marquées sont écrites par défaut dans des espaces d'adressage déconnectés afin de réduire la possibilité que des intrus injectent des instructions sur la pile exécutable.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Vérifiez que la fonction ASLR est activée.**

```
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (all)           enabled (all)
```

La valeur `all` est plus forte que la valeur par défaut. Elle peut créer des erreurs dans des applications qui s'appuient sur une pile consécutive située en mémoire. Par exemple, les bases de données peuvent dépendre d'une pile consécutive située en mémoire.

2. **Si la fonction ASLR est désactivée, activez la valeur par défaut et vérifiez qu'elle est prise en compte.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (tagged-files)  system default (default)
```

Voir aussi Vous pouvez désactiver la fonction ASLR à des fins de débogage en appelant la commande `sxadm` sur un fichier binaire particulier. Pour consulter des exemples, reportez-vous à la page de manuel `sxadm`(1M).

▼ Désactivation des services non utilisés

Appliquez cette procédure pour désactiver les services qui ne sont pas indispensables sur ce système.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Répertoriez les services réseau en ligne.**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **Désactivez les services qui ne sont pas requis par ce système.**

Par exemple, si le système n'est pas un serveur NFS ni un serveur Web et que leurs services sont en ligne, désactivez-les.

```
# svcadm disable svc:/network/nfs/server:default
# svcadm disable svc:/network/http:apache22
```

Voir aussi Pour plus d'informations, reportez-vous au Chapitre 1, “ Introduction à l’utilitaire de gestion des services ” du manuel “ Gestion des services système dans Oracle Solaris 11.2 ”, ainsi qu'à la page de manuel `svcs`(1).

▼ Désactivation de la possibilité pour les utilisateurs de gérer l'alimentation

Appliquez cette procédure pour empêcher les utilisateurs de la console du système de le suspendre ou de le mettre hors tension. Cette solution logicielle est inefficace si l'utilisateur de la console peut débrancher le matériel du système.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Passez en revue le contenu du profil de droits Console User (Utilisateur de la console).**

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 help=RtConsUser.html
```

2. **Créez un profil de droits comprenant tous les droits du profil Console User que les utilisateurs doivent conserver.**

   Pour obtenir des instructions, reportez-vous à la section “ Création d’un profil de droits ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

3. **Commentez le profil de droits de l'utilisateur de la console dans le fichier `/etc/security/policy.conf`.**

```
#CONSOLE_USER=Console User
```

4. **Attribuez aux utilisateurs le profil de droits que vous avez créé au cours de l'Étape 2.**

   - En guise de solution évolutive, vous pouvez définir cette valeur dans un profil de droits si un grand nombre d'utilisateurs partagent un même profil.

     ```
     # usermod -P shared-profile username
     ```

   - Vous pouvez également assigner le profil par système dans le fichier `policy.conf`.

```
# pfedit /etc/security/policy.conf...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

Voir aussi Pour plus d'informations, reportez-vous à la section " Fichier policy.conf " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ", ainsi qu'aux pages de manuel `policy.conf`(4) et `usermod`(1M).

▼ Placement d'un message de sécurité dans les fichiers bannière

Cette procédure permet de créer des messages de sécurité compris dans deux fichiers bannière et reflétant la stratégie de sécurité de votre site. Le fichier `/etc/issue` s'affiche avant l'authentification, tandis que le fichier `/etc/motd` s'affiche après.

Remarque - Les exemples de messages dans cette procédure ne répondent pas aux exigences du gouvernement des Etats-Unis et ne satisfont probablement pas les exigences de votre stratégie de sécurité. Consultez le conseil juridique de votre entreprise à propos du contenu du message de sécurité.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Administrator Message Edit (édition des messages administrateur). Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Créez le fichier `/etc/issue` et ajoutez un message de sécurité.**

```
# pfedit /etc/issue
ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

La commande `login` affiche le contenu du fichier `/etc/issue` avant l'authentification, à l'instar des commandes `ssh`, `telnet` et des services FTP. Pour afficher le contenu du fichier `/etc/issue` lors de la connexion au bureau, reportez-vous à la section "Placement d'un message de sécurité dans l'écran de connexion au bureau" à la page 37.

Pour plus d'informations, reportez-vous aux pages de manuel `issue`(4) et `pfedit`(1M).

2. **Ajoutez un message de sécurité au fichier `/etc/motd`.**

```
# pfedit /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

Dans Oracle Solaris, le shell initial de l'utilisateur affiche le contenu du fichier `/etc/motd`.

▼ Placement d'un message de sécurité dans l'écran de connexion au bureau

Choisissez parmi plusieurs méthodes de création d'un message de sécurité d'authentification, que les utilisateurs pourront consulter avant l'authentification, après ou les deux. Le fichier `/etc/issue` s'affiche avant l'authentification, tandis que le fichier `/etc/motd` s'affiche après.

Pour plus d'informations, cliquez sur le menu System (Système) -> Help (Aide) du bureau pour faire apparaître le navigateur d'aide GNOME. Vous pouvez également utiliser la commande `yelp`. Les scripts de connexion au bureau sont traités dans la section `GDM Login Scripts and Session Files` de la page de manuel `gdm`(1M).

Remarque - L'exemple de message dans cette procédure ne répond pas aux exigences du gouvernement des Etats-Unis et ne satisfait probablement pas les exigences de votre stratégie de sécurité. Consultez le conseil juridique de votre entreprise à propos du contenu du message de sécurité.

Avant de commencer Pour créer un fichier, vous devez prendre le rôle `root`. Pour modifier un fichier existant, vous devez utiliser un compte administrateur disposant de l'autorisation `solaris.admin.edit/`*path-to-existing-file*.

1. **Placez un message de sécurité sur l'écran de connexion au bureau avant l'authentification à l'aide de l'une des trois options suivantes :**

   Les options permettant de créer une boîte de dialogue utilisent le message de sécurité contenu dans le fichier `/etc/issue` mentionné à l'Étape 1 de la section “Placement d'un message de sécurité dans les fichiers bannière” à la page 36.

   - **POSSIBILITE 1 : modifiez un script d'initialisation GDM pour afficher le message de sécurité dans une boîte de dialogue.**

     Le répertoire `/etc/gdm` contient trois scripts d'initialisation qui affichent le message de sécurité avant et après l'authentification.

     ```
     # pfedit /etc/gdm/Init/Default
     /usr/bin/zenity --text-info --width=800 --height=300 \
     --title="Security Message"  --filename=/etc/issue
     ```

Pour plus d'informations sur la modification des systèmes de fichiers en tant qu'utilisateur sans rôle `root`, reportez-vous à la page de manuel `pfedit`(1M).

- **POSSIBILITE 2 : modifiez la fenêtre de connexion pour afficher le message de sécurité au -dessus du champ de saisie.**

  La fenêtre de connexion s'agrandit pour s'adapter à votre message. Cette méthode ne pointe pas vers le fichier `/etc/issue`. Vous devez saisir le texte dans l'interface graphique.

Remarque - La fenêtre de connexion, `gdm-greeter-login-window.ui`, est écrasée par les commandes `pkg fix` et `pkg update`. Pour conserver vos modifications, copiez le fichier vers un répertoire de fichiers de configuration et fusionnez-en les modifications avec le nouveau fichier après la mise à niveau du système. Pour plus d'informations, reportez-vous à la page de manuel`pkg`(5).

---

a. **Accédez au répertoire de l'interface utilisateur de la fenêtre de connexion.**

```
# cd /usr/share/gdm
```

b. **(Facultatif) Enregistrez une copie de l'interface utilisateur d'origine de la fenêtre de connexion.**

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
```

c. **Ajoutez une étiquette à la fenêtre de connexion à l'aide du concepteur d'interface graphique de GNOME Toolkit.**

Le programme `glade-3` ouvre le concepteur d'interface graphique de GTK+. Vous saisissez le message de sécurité dans une étiquette qui s'affiche au-dessus du champ de saisie de l'utilisateur.

```
# /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
```

Pour consulter le guide du concepteur d'interface graphique, cliquez sur Development (Développement) dans le navigateur d'aide GNOME. La page de manuel `glade-3`(1) est répertoriée sous Applications dans les pages de manuel.

d. **(Facultatif) Enregistrez une copie de l'interface utilisateur modifiée de la fenêtre de connexion.**

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
```

2. **Placez un message de sécurité sur l'écran de connexion au bureau après l'authentification à l'aide de l'une des trois options suivantes :**

Le fichier créant une boîte de dialogue après l'authentification utilise le message de sécurité contenu dans le fichier `/etc/motd` mentionné à l'Étape 2 de la section “Placement d'un message de sécurité dans les fichiers bannière” à la page 36.

- **POSSIBILITE 1 : Placez un message de sécurité sur le bureau après l'authentification.**

```
# pfedit /etc/gdm/PreSession/Default
/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message"  --filename=/etc/motd
```

Remarque - La boîte de dialogue peut être masquée par des fenêtres de l'espace de travail de l'utilisateur.

- **POSSIBILITE 2 : Créez un fichier de bureau affichant le message de sécurité dans une autre fenêtre après l'authentification.**

```
# pfedit /usr/share/gdm/autostart/LoginWindow/banner.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message" \
--filename=/etc/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Après s'être authentifié dans la fenêtre de connexion, l'utilisateur doit fermer la fenêtre contenant le message de sécurité pour atteindre l'espace de travail. Pour connaître les options de la commande `zenity`, reportez-vous à la page de manuel `zenity`(1).

Exemple 2-1 Création d'un court message d'avertissement qui s'affiche lors de la connexion au bureau

Dans cet exemple, l'administrateur saisit un court message en tant qu'argument de la commande `zenity` dans le fichier de bureau. L'administrateur utilise également l'option `--warning`, qui affiche une icône d'avertissement avec le message.

```
# pfedit /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Sécurisation des utilisateurs

A ce stade, seul l'utilisateur initial qui peut prendre le rôle `root` a accès au système. Il est conseillé d'effectuer les tâches suivantes dans l'ordre avant que les utilisateurs standard ne puissent se connecter.

TABLEAU 2-2 Sécurisation de la liste de tâches des utilisateurs

Tâche	Description	Pour obtenir des instructions
Exigence de mots de passe forts et de la modification fréquente des mots de passe.	Renforce les contraintes de mot de passe par défaut sur chaque système.	“Définition de contraintes de mot de passe renforcées” à la page 40
Configuration d'autorisations de fichier restrictives pour les utilisateurs standard.	Définit une valeur plus restrictive que `022` pour les autorisations de fichier concernant les utilisateurs standard.	“Définition d'une valeur `umask` plus restrictive pour les utilisateurs standard” à la page 44
Activation du verrouillage de compte pour les utilisateurs standard.	Sur les systèmes qui ne sont pas utilisés pour l'administration, active le verrouillage de compte à l'échelle du système et réduit le nombre de connexions activant le verrouillage.	“Activation du verrouillage de compte pour les utilisateurs standard” à la page 42
Présélection de la classe d'audit `cusa` pour tous les utilisateurs.	Améliore la surveillance et l'enregistrement des menaces potentielles à l'égard du système.	“Réalisation d'un audit des événements importants en plus de la connexion/déconnexion” à la page 45
Création de rôles.	Répartit des tâches d'administration distinctes parmi plusieurs utilisateurs de confiance afin qu'aucun utilisateur isolé ne puisse endommager le système. Vous pouvez utiliser des rôles ARMOR prédéfinis, créer vos propres rôles ou étendre ARMOR à l'aide de vos propres rôles.	“ Configuration des comptes utilisateur dans l’interface de ligne de commande ” du manuel “ Gestion des comptes utilisateur et des environnements utilisateur dans Oracle Solaris 11.2 ” “ Attribution de droits aux utilisateurs ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”
Réduction du nombre d'applications de bureau GNOME visibles.	Empêche les utilisateurs d'utiliser les applications de bureau qui peuvent compromettre la sécurité.	Reportez-vous au Chapitre 11, “ Désactivation de fonctionnalités dans le système de bureau Oracle Solaris ” du manuel “ Guide de l’administrateur du bureau Oracle Solaris 11.2 ”.
Limitation des privilèges des utilisateurs.	Supprime des privilèges de base dont les utilisateurs n'ont pas besoin.	“Suppression de privilèges de base non utilisés des utilisateurs” à la page 46

▼ Définition de contraintes de mot de passe renforcées

Cette procédure permet de modifier les valeurs par défaut si elles ne satisfont pas aux exigences de sécurité du site. Les étapes suivent l'ordre des entrées de variable du fichier `/etc/default/passwd`.

Avant de commencer Vous devez vous connecter en tant qu'administrateur bénéficiant de l'autorisation `solaris.admin.edit/etc/default/passwd`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

- **Utilisez la commande `pfedit` pour modifier comme suit le fichier `/etc/default/passwd` :**

  a. **Exigez que les utilisateurs changent de mot de passe tous les quatre mois, mais pas plus que toutes les trois semaines.**

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  MINWEEKS=3
  ```

  b. **Exigez un mot de passe d'au moins huit caractères.**

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. **Conservez un historique des mots de passe.**

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. **Exigez une différence minimale par rapport au dernier mot de passe.**

  ```
  #MINDIFF=3
  MINDIFF=4
  ```

  e. **Exigez une majuscule au minimum.**

  ```
  #MINUPPER=0
  MINUPPER=1
  ```

  f. **Exigez un chiffre au minimum.**

  ```
  #MINDIGIT=0
  MINDIGIT=1
  ```

Voir aussi

- Pour obtenir la liste des variables restreignant la création de mots de passe, reportez-vous à la page de manuel `passwd`(1).
- Pour les contraintes de mot de passe en vigueur après l'installation, reportez-vous à la rubrique "Accès au système limité et surveillé" à la page 14.

Activation du verrouillage de compte pour les utilisateurs standard

Cette procédure permet de verrouiller des comptes d'utilisateurs standard après un certain nombre d'échecs de tentatives de connexion.

Remarque - Les rôles sont des comptes partagés. N'activez pas le verrouillage de compte pour les utilisateurs pouvant prendre en charge des rôles, car un utilisateur verrouillé peut verrouiller un rôle.

Avant de commencer

Ne définissez pas cette protection à l'échelle du système sur un système que vous utilisez pour des activités d'administration. Optez plutôt pour une surveillance du système d'administration afin de détecter toute utilisation inhabituelle et maintenez-le accessible aux administrateurs.

Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Définissez l'attribut `LOCK_AFTER_RETRIES` sur `OUI`.**

   Choisissez la portée de la valeur de l'attribut.

   - **Effectuez l'activation à l'échelle du système.**

     Cette protection s'applique à tous les utilisateurs tentant d'utiliser le système.

     ```
     # pfedit /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - **Effectuez l'activation par utilisateur.**

     Cette protection s'applique uniquement à l'utilisateur pour lequel vous exécutez cette commande. Il ne s'agit pas d'une solution évolutive si vous disposez de plusieurs utilisateurs.

     ```
     # usermod -K lock_after_retries=yes username
     ```

   - **Créez et assignez un profil de droits.**

     Cette protection s'applique à n'importe quel utilisateur ou système auquel vous assignez ce profil de droits.

     a. **Créez le profil de droits.**

        ```
        # profiles -p shared-profile -S ldap
        ```

```
shared-profile: set lock_after_retries=yes
...
```

Pour plus d'informations sur la création de profils de droits, reportez-vous à la section " La création des profils de droits et autorisations " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

b. Assignez le profil de droits à des utilisateurs ou à l'échelle du système.

En guise de solution évolutive, vous pouvez définir cette valeur dans un profil de droits si un grand nombre d'utilisateurs partagent un même profil.

```
# usermod -P shared-profile username
```

Vous pouvez également assigner le profil par système dans le fichier `policy.conf`.

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. Définissez l'attribut de sécurité `RETRIES` sur `3`.

Choisissez la portée de la valeur de l'attribut.

- **Effectuez l'activation à l'échelle du système.**

```
# pfedit /etc/default/login
...
#RETRIES=5
RETRIES=3
...
```

- **Effectuez l'activation par utilisateur.**

```
# usermod -K lock_after_retries=3 username
```

- **Créez et assignez un profil de droits.**

  Suivez les étapes présentées à l'Étape 1.3 pour créer un profil de droits incluant `lock_after_retries =3`.

Voir aussi

- Pour en savoir plus sur les attributs de sécurité d'utilisateur et de rôle, reportez-vous au Chapitre 8, " Droits OracleÂ Solaris (référence) " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".
- Pages de manuel connexes : `policy.conf`(4), `profiles`(1), `user_attr`(4) et `usermod`(1M).

Définition d'une valeur umask plus restrictive pour les utilisateurs standard

L'utilitaire umask définit les bits d'autorisation de fichier créés par les utilisateurs. Si la valeur umask par défaut, 022, n'est pas assez restrictive, la procédure décrite ici permet de définir un masque plus restrictif à l'aide de la procédure décrite ici.

Avant de commencer Vous devez vous connecter en tant qu'administrateur autorisé à modifier les fichiers squelette. Le rôle root est assigné à ces autorisations. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Consultez les fichiers d'exemple fournis par Oracle Solaris par rapport aux valeurs par défaut du shell utilisateur.**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **Définissez la valeur umask dans les fichiers /etc/skel que vous comptez assigner aux utilisateurs.**

   Choisissez l'une des valeurs suivantes :

   - umask 026 : offre une protection modérée des fichiers (751) : r pour le groupe, x pour les autres
   - umask 027 : offre une protection avancée des fichiers (750) : r pour le groupe, pas d'accès pour les autres
   - umask 077 : offre une protection complète des fichiers (700) : pas d'accès pour le groupe ni d'autres personnes

Voir aussi Pour plus d'informations, reportez-vous aux références suivantes :

- " Configuration des comptes utilisateur dans l'interface de ligne de commande " du manuel " Gestion des comptes utilisateur et des environnements utilisateur dans Oracle Solaris 11.2 "
- " Valeur umask par défaut " du manuel " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 "
- Pages de manuel connexes : useradd(1M) et umask(1).

▼ Réalisation d'un audit des événements importants en plus de la connexion/déconnexion

Appliquez cette procédure pour effectuer un audit des commandes d'administration, des accès au système et d'autres événements importants spécifiés dans la stratégie de sécurité de votre site.

Remarque - Les exemples présentés dans cette procédure peuvent ne pas être suffisants pour satisfaire la stratégie de sécurité de votre entreprise.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Auditez toutes les applications de commandes privilégiées réalisées par des utilisateurs disposant de profils de droits et de rôles d'administration.**

   Ajoutez la classe d'audit `cusa` à leur masque de présélection.

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   Les classes d'audit incluses dans les métaclasses `cusa` sont répertoriées dans le fichier. `/etc/security/audit_class`.

2. **Enregistrez les arguments saisis pour les commandes auditées.**

   ```
   # auditconfig -setpolicy +argv
   ```

3. **(Facultatif) Enregistrez l'environnement dans lequel les commandes ayant fait l'objet d'un audit sont exécutées.**

   ```
   # auditconfig -setpolicy +arge
   ```

Remarque - Cette option de stratégie peut s'avérer utile en cas de dépannage.

Voir aussi

- Pour plus d'informations sur la stratégie d'audit, reportez-vous à la section " Stratégie d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".
- Pour obtenir des exemples d'indicateurs d'audit, reportez-vous aux sections " Configuration du service d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 " et " Dépannage du service d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".
- Page de manuel `auditconfig`(1M)

Suppression de privilèges de base non utilisés des utilisateurs

Dans certaines circonstances, certains privilèges de base peuvent être retirés du jeu de base d'un utilisateur standard ou invité. Par exemple, les utilisateurs de Sun Ray peuvent ne pas être autorisés à consulter l'état de processus qui ne sont pas en leur possession.

Avant de commencer Vous devez prendre le rôle `root`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Rédigez une définition complète du jeu de privilèges de base.**

   Les trois privilèges de base suivants sont susceptibles d'être supprimés.

```
% ppriv -lv basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
...
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. **Sélectionnez la portée de la suppression des privilèges.**

   - **Effectuez l'activation à l'échelle du système.**

     Tout utilisateur tentant d'utiliser le système ne peut obtenir ces privilèges. L'application de cette méthode de suppression des privilèges peut s'avérer appropriée sur un ordinateur mis à la disposition du public.

```
# pfedit /etc/security/policy.conf
...
#PRIV_DEFAULT=basic
PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
```

   - **Retirez des privilèges à des utilisateurs individuels.**

     - **Empêchez un utilisateur de créer un lien vers un fichier dont l'utilisateur n'est pas propriétaire.**

```
# usermod -K 'defaultpriv=basic,!file_link_any' user
```

- **Empêchez un utilisateur d'examiner des processus dont il n'est pas propriétaire.**

  ```
  # usermod -K 'defaultpriv=basic,!proc_info' user
  ```

- **Empêchez un utilisateur de démarrer une seconde session, telle qu'une session `ssh`, à partir de la session en cours.**

  ```
  # usermod -K 'defaultpriv=basic,!proc_session' user
  ```

- **Supprimez les trois privilèges de l'ensemble de privilèges de base d'un utilisateur.**

  ```
  # usermod -K 'defaultpriv=basic,!file_link_any,!proc_info,!proc_session' user
  ```

- **Créez et assignez un profil de droits.**

  Cette protection s'applique à n'importe quel utilisateur ou système auquel vous assignez ce profil de droits.

  a. **Créez le profil de droits.**

  ```
  # profiles -p shared-profile -S ldap
  shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
  ...
  ```

  Pour plus d'informations sur la création de profils de droits, reportez-vous à la section " La création des profils de droits et autorisations " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

  b. **Assignez le profil de droits à des utilisateurs ou à l'échelle du système.**

  En guise de solution évolutive, vous pouvez définir cette valeur dans un profil de droits si un grand nombre d'utilisateurs (tels que des utilisateurs de Sun Ray ou distants) partagent un même profil.

  ```
  # usermod -P shared-profile username
  ```

  Vous pouvez également assigner le profil par système dans le fichier `policy.conf`.

  ```
  # pfedit /etc/security/policy.conf
  ...
  #PROFS_GRANTED=Basic Solaris User
  PROFS_GRANTED=shared-profile,Basic Solaris User
  ```

Voir aussi Pour plus d'informations, reportez-vous au Chapitre 1, " A propos de l'utilisation de droits pour contrôle Users and Processes " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ", ainsi qu'à la page de manuel `privileges`(5).

Protection du réseau

A ce stade, vous avez peut-être créé des utilisateurs qui peuvent prendre des rôles et créé les rôles.

Parmi les tâches réseau suivantes, effectuez celles qui fournissent une sécurité supplémentaire en fonction des exigences de votre site. Ces tâches réseau renforcent les protocoles IP, ARP et TCP.

TABLEAU 2-3 Configuration de la liste de tâches du réseau

Tâche	Description	Pour obtenir des instructions
Désactivation du démon de routage du réseau.	Limite l'accès aux systèmes par des renifleurs de réseau	“ Désactivation du démon de routage réseau ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Prévention de la diffusion d'informations sur la topologie du réseau.	Empêche la diffusion de paquets.	“ Désactivation du transfert de paquets de diffusion ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
	Désactive les réponses aux demandes d'écho de diffusion et aux demandes d'écho multidiffusion.	“ Désactivation des réponses aux demandes d’écho ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Pour les systèmes constituant des passerelles vers d'autres domaines, tels qu'un pare-feu ou un noeud de réseau privé virtuel (VPN), activation du multihébergement strict de la source et de la destination.	Empêche les paquets qui ne possèdent pas dans leur en-tête l'adresse de la passerelle de se déplacer au-delà de la passerelle.	“ Définition du multihébergement strict ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Prévention des attaques DOS en contrôlant le nombre de connexions incomplètes au système.	Limite le nombre maximal de connexions TCP incomplètes pour un processus d'écoute TCP.	“ Définition du nombre maximal de connexions TCP incomplètes ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Prévention des attaques DoS en contrôlant le nombre de connexions entrantes autorisées.	Spécifie le nombre maximal par défaut de connexions TCP en attente pour un processus d'écoute TCP.	“ Définition du nombre maximal de connexions TCP en attente ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Restauration des valeurs sécurisées par défaut des paramètres réseau.	Renforce la sécurité lorsqu'elle a été réduite par des actions d'administration.	“ Réinitialisation des paramètres réseau sur des valeurs sécurisées ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Ajout de wrappers TCP aux services réseau pour limiter l'accès des applications aux utilisateurs légitimes.	Indique les systèmes autorisés à accéder aux services réseau, tels que FTP.	Utilisation des wrappers TCP
Configuration d'un pare-feu.	Utilise la fonction IP Filter pour fournir un pare-feu.	Chapitre 4, “ A propos d’IP Filter dans Oracle Solaris ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ” Chapitre 5, “ Configuration d’IP Filter ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Configuration de connexions réseau chiffrées et authentifiées.	Utilise IPsec et IKE pour protéger les transmissions réseau entre des noeuds et des réseaux conjointement configurés à l'aide d'IPsec et IKE.	Chapitre 7, “ Configuration d’IPsec ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”

Tâche	Description	Pour obtenir des instructions
		Chapitre 9, “ Configuration d’IKEv2 ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”

▼ Utilisation des wrappers TCP

Les étapes suivantes décrivent les trois manières dont les wrappers TCP sont utilisés ou peuvent être utilisés dans Oracle Solaris.

Avant de commencer Vous devez prendre le rôle `root` pour modifier un programme afin d'utiliser des wrappers TCP.

1. **Vous n'avez pas besoin de protéger l'application `sendmail` à l'aide de wrappers TCP.**

   Par défaut, elle est protégée à l'aide de wrappers TCP, comme décrit à la section “ Prise en charge des wrappers TCP à partir de la version 8.12 de sendmail ” du manuel “ Gestion des services sendmail dans Oracle Solaris 11.2 ”.

2. **Pour activer des wrappers TCP pour tous les services `inetd`, reportez-vous à la section “ Contrôle d’accès aux services TCP à l’aide des wrappers TCP ” du manuel “ Administration des réseaux TCP/IP, d’IPMP et des tunnels IP dans Oracle Solaris 11.2 ”.**

3. **Protégez le service de réseau FTP à l'aide de wrappers TCP.**

   a. **Suivez les instructions du module `/usr/share/doc/proftpd/modules/mod_wrap.html`.**

      Ce module étant dynamique, vous devez le charger pour utiliser des wrappers TCP avec FTP.

   b. **Chargez le module en ajoutant les instructions suivantes au fichier `proftpd.conf` :**

      ```
      # pfedit /etc/proftpd.conf
      <IfModule mod_dso.c>
          LoadModule mod_wrap.c
      </IfModule>
      ```

   c. **Redémarrez le service FTP.**

      ```
      # svcadm restart svc:/network/ftp
      ```

Protection des systèmes de fichiers

Les systèmes de fichiers ZFS sont légers et peuvent être chiffrés, compressés et configurés par rapport à des quotas d'espace réservé et d'espace disque.

Le système de fichiers `tmpfs` peut croître sans limite. Pour empêcher un déni de service, appliquez la procédure de “Limitation de la taille du système de fichiers `tmpfs`” à la page 50.

Les tâches suivantes permettent de définir une limite de taille pour le système de fichiers `tmpfs` et donnent un aperçu des protections disponibles dans ZFS, le système de fichiers par défaut d'Oracle Solaris. Pour plus d'informations, reportez-vous à la section “ Définition des quotas et réservations ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”, ainsi qu'à la page de manuel`zfs`(1M).

TABLEAU 2-4 Protection de la liste de tâches des systèmes de fichiers

Tâche	Description	Pour obtenir des instructions
Prévention des dénis de service grâce à la gestion et à la réservation d'espace disque.	Spécifie l'utilisation de l'espace disque par système de fichiers, par utilisateur ou groupe, ou encore par projet.	“ Définition des quotas et réservations ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”
Garantie d'une quantité d'espace disque minimum pour un jeu de données et ses descendants.	Garantit de l'espace disque par système de fichiers, par utilisateur ou groupe, ou par projet.	“ Définition de réservations sur les systèmes de fichiers ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”
Chiffrement des données sur un système de fichiers.	Protège un jeu de données par chiffrement et par la définition au moment de la création du jeu de données d'une phrase de passe permettant d'y accéder.	“ Chiffrement des systèmes de fichiers ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ” “ Exemples de chiffrement de systèmes de fichiers ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”
Limitation de la taille du système de fichiers `tmpfs`.	Empêche un utilisateur malveillant de créer des fichiers volumineux dans le répertoire `/tmp` en vue de ralentir le système.	“Limitation de la taille du système de fichiers `tmpfs`” à la page 50

▼ Limitation de la taille du système de fichiers `tmpfs`

Par défaut, la taille du système de fichiers `tmpfs` n'est pas limitée. La taille du système de fichiers `tmpfs` peut donc croître au point de saturer la mémoire système et la mémoire swap disponibles. Dans la mesure où le répertoire `/tmp` est utilisé par toutes les applications et tous les utilisateurs, une seule application peut remplir la mémoire système disponible. De même, un utilisateur mal intentionné qui ne dispose d'aucun privilège peut provoquer un ralentissement du système en créant des fichiers volumineux dans le répertoire `/tmp`. Pour assurer des performances optimales, vous pouvez limiter la taille de chaque montage du système de fichiers `tmpfs`.

Vous pouvez essayer de définir différentes valeurs pour identifier celle qui garantit des performances système optimales.

Avant de commencer

Pour modifier le fichier `vfstab`, vous devez vous connecter en tant qu'administrateur disposant de l'autorisation `solaris.admin.edit/etc/vfstab`. Vous ne pouvez réinitialiser le système que si le profil de droits Maintenance and Repair (Maintenance et réparations) vous est affecté. Le rôle `root` dispose de tous ces droits. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. Identifiez la quantité de mémoire disponible sur votre système.

Remarque - Le système de la série SPARC T3 utilisé dans l'exemple suivant est équipé d'un disque SSD (Solid State Disk), pour un E/S plus rapide, et dispose de huit disques de 279,40 Mo. Le système possède environ 500 Go de mémoire.

```
% prtconf | head
System Configuration:  Oracle Corporation  sun4v
Memory size: 523776 Megabytes
System Peripherals (Software Nodes):

ORCL,SPARC-T3-4
scsi_vhci, instance #0
disk, instance #4
disk, instance #5
disk, instance #6
disk, instance #8
```

2. Calculez une limite pour la mémoire de `tmpfs`.

En fonction de la taille de la mémoire système, vous pouvez évaluer la limite à environ 20 % pour les grands systèmes et à environ 30 % pour les systèmes plus restreints.

Ainsi, dans le cas d'un système plus petit, utilisez le multiplicateur `.30`.

```
10240M x .30 ≈ 340M
```

Pour un système plus grand, utilisez le multiplicateur `.20`.

```
523776M x .20 ≈ 10475M
```

3. Modifiez l'entrée `swap` dans le fichier `/etc/vfstab` en respectant la taille limite.

```
# pfedit /etc/vfstab
#device     device       mount       FS      fsck    mount mount
#to mount   to fsck      point       type    pass    at boot options
#
...
#swap       -            /tmp        tmpfs   -       yes     -
swap        -            /tmp        tmpfs   -       yes     size=10400m
```

```
/dev/zvol/dsk/rpool/swap   -      -  swap    -       no      -
```

4. **Réinitialisez le système.**

```
# reboot
```

5. **Assurez-vous que la limite a bien été appliquée.**

```
% mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. **Surveillez l'utilisation de la mémoire pour l'ajuster aux besoins de votre site.**

   La commande `df` présente un intérêt certain. Cependant, les statistiques les plus utiles sont fournies par la commande `swap`.

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

   Pour plus d'informations, reportez-vous aux pages de manuel `tmpfs`(7FS), `mount_tmpfs`(1M), `df`(1M) et `swap`(1M) man pages.

Protection et modification de fichiers

Par défaut, seul le rôle `root` peut modifier les autorisations de fichier système. Les rôles et utilisateurs disposant de l'autorisation `solaris.admin.edit/`*path-to-system-file* peuvent modifier ce *system-file*. Seul le rôle `root` peut rechercher tous les fichiers.

TABLEAU 2-5 Liste de tâches de protection et modification de fichiers

Tâche	Description	Pour obtenir des instructions
Configuration d'autorisations de fichier restrictives pour les utilisateurs standard.	Définit une valeur plus restrictive que `022` pour les autorisations de fichier concernant les utilisateurs standard.	"Définition d'une valeur `umask` plus restrictive pour les utilisateurs standard" à la page 44
Spécification de listes de contrôle d'accès (ACL) afin de protéger les fichiers à une granularité plus fine que les autorisations de fichier UNIX standard.	Les attributs de sécurité étendus peuvent être utiles pour protéger les fichiers. Pour une mise en garde à propos de l'utilisation de listes de contrôle d'accès, reportez-vous à Hiding Within the Trees	Intégrité complète des données ZFS (http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data)

Tâche	Description	Pour obtenir des instructions
	(http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf).	
Mise à jour de l'intégrité des fichiers système.	Détecte les fichiers non fiables à l'aide d'un script ou de l'utilitaire BART.	“ Recherche de fichiers avec des autorisations de fichier spéciales ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”

Sécurisation de l'accès au système et de son utilisation

Vous pouvez configurer les fonctions de sécurité d'Oracle Solaris afin de protéger votre utilisation du système, y compris les applications et services situés sur le système et le réseau.

TABLEAU 2-6 Liste de tâches de sécurisation de l'accès au système et de son utilisation

Tâche	Description	Pour obtenir des instructions
Prévention de l'exploitation d'une pile exécutable par les programmes.	Définit une variable système qui empêche l'exploitation des débordements de tampon qui exploitent la pile exécutable.	“ Protection contre les problèmes de sécurité causés par les fichiers exécutables ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”
Vérification que les fichiers binaires libellés pour la fonctionnalité de randomisation du format d'espace d'adressage (ASLR) peuvent utiliser la fonction ASLR.	Active la fonction ASLR pour les fichiers binaires marqués.	“Vérification de l'activation de la fonction ASLR” à la page 33
Configuration de l'audit.	Personnalise la configuration de l'audit pour la protection et l'intégrité des fichiers.	“Utilisation du service d'audit” à la page 58
Protection des dumps noyau qui peuvent contenir des informations confidentielles.	Crée un répertoire d'accès restreint dédié aux dumps noyau.	“ Activation des chemins d’accès aux fichiers ” du manuel “ Dépannage des problèmes d’administration système dans Oracle Solaris 11.2 ” “ Administration des spécifications de vos dumps noyau ” du manuel “ Dépannage des problèmes d’administration système dans Oracle Solaris 11.2 ”
Protection d'un serveur Web avec le proxy SSL au niveau du noyau.	Le protocole SSL (Secure Sockets Layer) peut être utilisé pour chiffrer et accélérer les communications des serveurs Web.	Chapitre 3, “ Serveurs Web et protocole SSL (Secure Sockets Layer) ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Création de zones contenant des applications.	Les zones sont des conteneurs qui isolent les processus. Elles peuvent isoler les applications et des composants d'applications. Par exemple, les zones peuvent être utilisées pour séparer la base de données d'un site Web et le serveur Web du site.	“ Présentation d’Oracle Solaris Zones ”
Gestion des ressources dans des zones.	Les zones fournissent un certain nombre d'outils permettant de gérer les ressources des zones.	“ Administration de la gestion des ressources dans Oracle Solaris 11.2 ”

Protection d'un service hérité avec SMF

Vous pouvez limiter la configuration d'une application aux utilisateurs ou rôles de confiance en ajoutant l'application à la fonction SMF (utilitaire de gestion des services) d'Oracle Solaris, puis en exigeant de disposer des droits de démarrer, d'actualiser et d'arrêter le service.

Pour plus d'informations et de procédures, consultez les références suivantes :

- " Verrouiller les ressources à l'aide de privilèges étendus " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- Securing MySQL using SMF - the Ultimate Manifest (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the).
- Pages de manuel connexes : `smf`(5), `smf_security`(5), `svcadm`(1M), `svcbundle`(1M) et `svccfg`(1M).

Configuration d'un réseau Kerberos

Vous pouvez protéger votre réseau à l'aide du service Kerberos. Cette architecture client-serveur garantit la sécurité des transactions sur les réseaux. Le service assure l'authentification fiable des utilisateurs, ainsi que l'intégrité et la confidentialité. A l'aide du service Kerberos, vous pouvez vous connecter à d'autres systèmes, exécuter des commandes, échanger des données et transférer des fichiers en toute sécurité. En outre, le service permet aux administrateurs de limiter l'accès aux services et systèmes. En tant qu'utilisateur Kerberos, vous pouvez réguler l'accès d'autres personnes à votre compte.

Pour plus d'informations et de procédures, consultez les références suivantes :

- Chapitre 3, " Planification du service Kerberos " du manuel " Gestion de Kerberos et d'autres services d'authentification dans Oracle Solaris 11.2 "
- Chapitre 4, " Configuration du service Kerberos " du manuel " Gestion de Kerberos et d'autres services d'authentification dans Oracle Solaris 11.2 "
- Pages de manuel connexes : `kadmin`(1M), `pam_krb5`(5) et `kclient`(1M).

Ajout d'une sécurité multiniveau étiquetée

Trusted Extensions accroît la sécurité d'Oracle Solaris en imposant une stratégie de contrôle d'accès obligatoire (MAC) basée sur des étiquettes. Des étiquettes de sensibilité sont automatiquement appliquées à toutes les sources de données (réseaux, systèmes de fichiers et fenêtres) ainsi qu'aux consommateurs de données (utilisateurs et processus). L'accès à toutes les données est limité en fonction de la relation entre l'étiquette des données (objet) et le consommateur (sujet). La fonctionnalité en couches est constituée d'un ensemble de services prenant en charge les étiquettes.

Les services de Trusted Extensions comprennent notamment les éléments suivants :

- Mise en réseau étiquetée
- Montage et partage de systèmes de fichiers prenant en charge les étiquettes
- Bureau étiqueté
- Configuration et traduction d'étiquettes
- Outils de gestion système sensibles aux étiquettes
- Allocation de périphériques sensible aux étiquettes

Les packages `system/trusted` et `system/trusted/trusted-global-zone` suffisent pour un écouteur ou un serveur qui ne nécessite pas de bureau multiniveau. Le package `group/feature/trusted-desktop` fournit l'environnement de bureau sécurisé multiniveau d'Oracle Solaris.

Configuration de Trusted Extensions

Vous devez installer les packages Trusted Extensions puis configurer le système. Après l'installation du package `trusted-extensions`, le système peut exécuter un bureau avec un affichage bitmap directement connecté, tel qu'un ordinateur portable ou une station de travail. La configuration du réseau est nécessaire pour communiquer avec d'autres systèmes.

Pour plus d'informations et de procédures, consultez les références suivantes :

- Partie I, “ Configuration initiale de TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”
- Partie II, “ Administration de TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”

Configuration d'IPsec avec étiquettes

Vous pouvez protéger vos paquets étiquetés à l'aide d'IPsec.

Pour plus d'informations et de procédures, consultez les références suivantes :

- Chapitre 6, “ A propos de l’architecture de sécurité IP ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
- “ Administration d’IPsec avec étiquettes ” du manuel “ Configuration et administration de Trusted Extensions ”
- “ Configuration d’IPsec avec étiquettes ” du manuel “ Configuration et administration de Trusted Extensions ”

♦ ♦ ♦ CHAPITRE 3

Mise à jour et surveillance de la sécurité d'Oracle Solaris

Une fois l'installation et la configuration initiales effectuées, vous pouvez mettre à jour et surveiller la sécurisation de votre système comme suit :

- En consultant régulièrement les enregistrements d'audit
- En procédant à des contrôles de l'intégrité des packages et des fichiers
- En surveillant l'activité du réseau
- En procédant à des contrôles de la conformité.

Mise à jour et surveillance de la sécurité du système

Les tâches suivantes permettent de mettre à jour et contrôler l'accès au système et aux données ainsi que leur utilisation, et de vérifier la conformité à vos exigences de sécurité.

TABLEAU 3-1 Liste de tâches de mise à jour et de surveillance du système

Tâche	Description	Pour obtenir des instructions
Vérification des packages sur le système.	Vérifie que les packages sont identiques à ceux de la source suite à une mise à jour.	“Vérification des packages” à la page 33
Vérification de l'intégrité des fichiers.	Une fois la configuration terminée, comparez les manifestes BART à intervalles réguliers afin de vérifier que seuls les fichiers à modifier sont modifiés.	“Vérification de l'intégrité des fichiers à l'aide de l'utilitaire BART” à la page 58
Repérage de fichiers non fiables.	Repère dans les programmes l'utilisation éventuellement non autorisée des permissions `setuid` et `setgid`.	“ Recherche de fichiers avec des autorisations de fichier spéciales ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”
Passage en revue régulier des journaux d'audit.	Localise les accès et l'utilisation inhabituels du système.	“Utilisation du service d'audit” à la page 58
Passage en revue des journaux d'audit relatifs aux événements de connexion et de déconnexion en temps réel.	Identifie les tentatives de violation quasiment en simultané.	“Contrôle des enregistrements d'audit en temps réel” à la page 59

Tâche	Description	Pour obtenir des instructions
Exécution de tests de compatibilité.	Evalue la conformité du système aux tests d'évaluation de la sécurité.	“ Guide de conformité à la sécurité d’Oracle Solaris 11.2 ” et la page de manuel `compliance`(1M)

Vérification de l'intégrité des fichiers à l'aide de l'utilitaire BART

BART est un outil qui génère des rapports et analyse l'intégrité des fichiers en fonction de règles. Il s'appuie sur des repères cryptographiques et les métadonnées de systèmes de fichiers pour répertorier les modifications dans des rapports.

Pour plus d'informations et de procédures, reportez-vous aux références suivantes :

- “ A propos de BART ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”
- “ A propos de l’utilisation de BART ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”
- “ Manifestes BART, fichiers de règles et rapports ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”

Pour des instructions plus détaillées sur le suivi des modifications apportées aux systèmes installés, reportez-vous à la section “ Comparaison des manifestes pour le même système dans le temps ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”.

Utilisation du service d'audit

L'audit permet de conserver une trace de la façon dont le système est utilisé. Le service d'audit inclut des outils pour vous aider à analyser des données d'audit.

Le service d'audit est décrit dans la section “ Gestion de l’audit dans Oracle Solaris 11.2 ”. Pour obtenir la liste des pages de manuel et liens correspondants, reportez-vous à la section “ Pages de manuel du service d’audit ” du manuel “ Gestion de l’audit dans Oracle Solaris 11.2 ”.

Les procédures de service d'audit suivantes sont utiles dans la plupart des environnements sécurisés :

- Créez des rôles distincts chargés de configurer les audits, de vérifier les audits ainsi que de démarrer et d'arrêter le service d'audit. Assignez ces rôles à des utilisateurs de confiance.

  Utilisez les profils de droits Audit Configuration (Configuration d'audit), Audit Review (Vérification d'audit) et Audit Control (Contrôle d'audit) comme bases pour ces rôles.

Pour créer des rôles ou utiliser les rôles ARMOR prédéfinis, reportez-vous à la section " Attribution de droits aux utilisateurs " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

- Auditez tous les administrateurs à l'aide de la classe d'audit `cusa`.

  Les évènements relatifs à la classe d'audit `cusa` comprennent les actions d'administration affectant la sécurisation du système. Pour obtenir une description, reportez-vous au fichier `/etc/security/audit_class`. Pour plus d'informations sur cette procédure, reportez -vous à la section"Réalisation d'un audit des événements importants en plus de la connexion/déconnexion" à la page 45.
- Envoyez des enregistrements d'audit à un serveur central.
  - Configurez l'audit de manière à ce qu'il fonctionne avec le serveur d'audit à distance (ARS).

    Voir la section " Envoi des fichiers d'audit à un référentiel distant " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".
  - Programmez le transfert sécurisé des fichiers d'audit complets vers un système de fichiers de vérification d'audit sur un pool ZFS distinct.
- Contrôlez les récapitulatifs textuels des événements audités dans l'utilitaire `syslog`.

  Activez le plug-in `audit_syslog`, puis contrôlez les événements pris en compte.

  Voir la section " Configuration des journaux d'audit syslog " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".
- Limitez la taille des fichiers d'audit.

  Spécifiez une taille pertinente pour l'attribut `p_fsize` du plug-in `audit_binfile`. Prenez en compte votre planning de vérifications, l'espace disque et la fréquence des travaux `cron`, entre autres facteurs.

  Pour consulter des exemples, reportez-vous à la section " Affectation de l'espace d'audit pour la piste d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".
- Programmez le transfert sécurisé des fichiers d'audit complets vers un système de fichiers de vérification d'audit sur un pool ZFS distinct.
- Vérifiez les fichiers d'audit complets sur le système de fichiers de vérification d'audit.

Contrôle des enregistrements d'audit en temps réel

Le plug-in `audit_syslog` vous permet d'enregistrer des récapitulatifs d'événements d'audit présélectionnés. Lors de la génération des récapitulatifs d'audit, vous pouvez les afficher dans une fenêtre de terminal en exécutant une commande du type :

```
# tail -0f  /var/adm/auditlog
```

Pour configurer le journal d'audit, reportez-vous à la section " Configuration des journaux d'audit syslog " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".

Vérification et archivage des journaux d'audit

Les enregistrements d'audit peuvent être consultés au format texte ou dans un navigateur au format XML.

Pour plus d'informations et de procédures, consultez les références suivantes :

- " Journaux d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 "
- " Contrôle du dépassement de la piste d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 "
- " Affichage des données de la piste d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 "

♦ ♦ ♦ ANNEXE A

Bibliographie relative à la sécurité d'Oracle Solaris

Les références suivantes contiennent des informations de sécurité utiles pour les systèmes Oracle Solaris. Les informations relatives à la sécurité datant des versions antérieures du SE Oracle Solaris contiennent des informations utiles, mais aussi quelques informations obsolètes.

Références de sécurité sur le réseau Oracle Technology Network

La documentation et les articles suivants sont disponibles sur le site Web du réseau Oracle Technology Network et contiennent des descriptions de la sécurité sur les systèmes Oracle Solaris 11 :

- " Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.2 "
- " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 "
- " Sécurisation du réseau dans Oracle Solaris 11.2 "
- " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "
- " Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 "
- " Gestion de l'audit dans Oracle Solaris 11.2 "
- " Gestion de Kerberos et d'autres services d'authentification dans Oracle Solaris 11.2 "
- " Gestion de l'accès au shell sécurisé dans Oracle Solaris 11.2 "
- " Guide de conformité à la sécurité d'Oracle Solaris 11.2 "
- " Using a FIPS 140 Enabled System in Oracle Solaris 11.2 "

Références à la sécurité d'Oracle Solaris dans des publications tierces

La documentation et les articles suivants contiennent des descriptions de la sécurité sur les systèmes Oracle Solaris 11 :

- *Security Configuration Benchmark For Solaris 11 11/11 Version 1.0.0 11 juin 2012*

  Ces tests d'évaluation de la sécurité sont publiés par le Center for Internet Security (CIS), http://cisecurity.org/ à l'attention des acteurs de la sécurité informatique. Ce document indique les paramètres de sécurité recommandés pour le système d'exploitation Oracle Solaris. Le public ciblé comprend les administrateurs de systèmes et d'applications, les spécialistes de la sécurité, les chargés d'audit, les ingénieurs de support, ainsi que les installateurs et les développeurs qui créent, installent, évaluent ou fournissent des solutions de sécurité pour Oracle Solaris. Pour obtenir un exemplaire, rendez-vous sur la page CIS Security Benchmarks (http://benchmarks.cisecurity.org/).
- *Oracle Solaris 11 System Administration: The Complete Reference*. Michael Jang, Harry Foxwell, Christine Tran, and Alan Formy-Duval. 2012. McGraw-Hill. ISBN 978007179042.

  Cet ouvrage traite de l'étendue de la sécurité d'Oracle Solaris.
- *Oracle Solaris 11: First Look*. Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

  Cet ouvrage présente Oracle Solaris ainsi que sa sécurité aux administrateurs.
- *Oracle Solaris 11 System Administration*, Bill Calkins. 2013. Prentice Hall. ISBN 9780133007114.

  Cet ouvrage décrit les nouvelles fonctions d'Oracle Solaris, notamment en termes de sécurité.