Directives de sécurité d'Oracle® Solaris 11

Référence : E25813–03
Mars 2012

ORACLE®

120424@25097

Table des matières

Préface

Ce guide présente les recommandations relatives à la sécurité pour Système d'exploitation Oracle Solaris (SE Oracle Solaris). Dans un premier temps, ce guide décrit les problèmes de sécurité auxquels un SE d'entreprise se doit de répondre. Il énonce ensuite les valeurs par défaut des fonctionnalités de sécurité du SE Oracle Solaris. Enfin, le guide décrit des mesures spécifiques à prendre pour sécuriser le système et pour protéger les données et applications à l'aide des fonctions de sécurité d'Oracle Solaris. Vous pouvez adapter les recommandations de ce guide à la stratégie de sécurité de votre site.

Public visé

Directives de sécurité d'Oracle Solaris 11 est destiné aux administrateurs de sécurité et à d'autres administrateurs chargés d'effectuer les tâches suivantes :

- Analyse des exigences en matière de sécurité
- Mise en oeuvre de la stratégie de sécurité du site en ce qui concerne les logiciels
- Installation et configuration du SE Oracle Solaris
- Maintenance de la sécurité de systèmes et de réseaux

Pour utiliser ce guide, vous devez avoir une connaissance générale de l'administration UNIX, de bonnes bases en matière de logiciels de sécurité et une connaissance de la stratégie de sécurité de votre site.

Accès au support technique 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` adapté aux utilisateurs malentendants.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Description	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P–2 Invites de shell

Shell	Invite
Bash shell, korn shell et bourne shell	`$`
Bash shell, korn shell et bourne shell pour superutilisateur	`#`
C shell	`nom_machine%`

TABLEAU P–2 Invites de shell *(Suite)*

Shell	Invite
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

Présentation de la sécurité d'Oracle Solaris 11

Oracle Solaris 11 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 11 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.

Protections de sécurité Oracle Solaris 11

Oracle Solaris constitue un fondement solide pour les données d'entreprise et les applications en protégeant les données sur disque et lors des déplacements. Oracle Solaris Resource Manager, également appelé *gestionnaire de ressources*, et Oracle Solaris Zones offrent des fonctionnalités qui séparent et protègent les applications des mauvaises utilisations. Cette séparation, ainsi que le principe du moindre privilège mis en oeuvre par le biais des privilèges et de la fonctionnalité de contrôle d'accès basé sur les rôles (RBAC) d'Oracle Solaris, réduisent les risques de sécurité que peuvent présenter les actions d'éventuels intrus ou d'utilisateurs standard. Des protocoles authentifiés et chiffrés tels que le protocole IPsec (IP security) fournissent des réseaux privés virtuels (VPN) sur l'ensemble de l'Internet ainsi que des tunnels au sein d'un LAN ou d'un WAN pour assurer la remise sécurisée des données. En outre, la fonctionnalité d'audit d'Oracle Solaris permet de conserver une trace de toutes les activités importantes.

Les services de sécurité d'Oracle Solaris 11 assurent une protection renforcée en proposant plusieurs niveaux de protection pour le système et le réseau. Oracle Solaris protège le noyau en limitant, au sein des utilitaires du noyau, les actions privilégiées pouvant être effectuées par l'utilitaire. La configuration réseau par défaut assure la protection des données sur le système et dans l'ensemble du réseau. IPsec, la fonction de filtrage IP d'Oracle Solaris, de même que Kerberos, peuvent fournir une protection supplémentaire.

Les services de sécurité d'Oracle Solaris assurent :

- La protection du noyau : les démons et périphériques du noyau sont protégés par des permissions de fichiers et des privilèges.
- La protection des connexions : les connexions nécessitent des mots de passe. Le chiffrement des mots de passe est fortement sécurisé. Les connexions distantes sont initialement limitées à un canal chiffré et authentifié via la fonction Secure Shell d'Oracle Solaris. Le compte `root` ne peut pas se connecter directement.
- La protection des données : les données sur disque sont protégées par des autorisations de fichier. Des niveaux de protection supplémentaires peuvent être configurés. Vous pouvez par exemple avoir recours à des listes de contrôle d'accès (ACL), placer des données dans une zone, chiffrer un fichier, chiffrer une jeu de données ZFS Oracle Solaris, créer un jeu de données ZFS en lecture seule et monter des systèmes de fichiers de manière à empêcher l'exécution de programmes `setuid` et de fichiers exécutables.

Technologies de sécurité d'Oracle Solaris 11

Les fonctions de sécurité d'Oracle Solaris peuvent être configurées de manière à mettre en oeuvre la stratégie de sécurité de votre site.

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.

Service d'audit

L'audit consiste à collecter des données sur l'utilisation des ressources système. Les données d'audit fournissent un enregistrement des événements système ayant trait 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 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 une liste des pages de manuel portant sur le thème de l'audit, reportez-vous au Chapitre 29, "Audit (référence)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 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 36 et aux pages de manuel.
- Pour une présentation de l'audit, reportez-vous au Chapitre 26, "Audit (présentation)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour en savoir plus sur les tâches d'audit, reportez-vous au Chapitre 28, "Gestion de l'audit (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Utilitaire BART (Basic Audit Reporting Tool)

L'outil de génération de rapports d'audit de base (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. La création de manifestes BART est un moyen aisé de rassembler des informations fiables sur les composants de la pile de logiciels installée sur les systèmes déployés.

BART est utile pour gérer l'intégrité d'un système ou d'un réseau de systèmes.

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

- Pages de manuel connexes : `bart(1M)`, `bart_rules(4)` et `bart_manifest(4)`.
- Pour obtenir des instructions, reportez-vous à la section "Création d'un instantané BART du système" à la page 50, "Utilisation de l'utilitaire BART" à la page 53 et aux pages de manuel.
- Pour une présentation de BART, reportez-vous au Chapitre 6, "Utilisation de l'outil de génération de rapports d'audit de base (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour des exemples d'utilisation de BART, reportez-vous à la section "Utilisation de BART (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité* et aux pages de manuel.

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. Les différents mécanismes de stockage, utilitaires d'administration et

interfaces de programmation de diverses infrastructures à clé publique (PKI) ont la possibilité d'utiliser une interface unifiée lorsqu'elles adoptent des interfaces KMF.

La structure cryptographique fournit des services cryptographiques aux utilisateurs et aux applications par le biais de diverses commandes, d'une interface de programme de niveau utilisateur, d'une interface de programmation du noyau et de structures de niveau utilisateur et noyau. La structure cryptographique fournit ces services cryptographiques aux applications et aux modules du noyau d'une manière transparente pour l'utilisateur final. Elle fournit également des services cryptographiques directs, tels que le chiffrement et le déchiffrement de fichiers, à l'utilisateur final.

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 une vue d'ensemble des services cryptographiques, reportez-vous au Chapitre 11, “Structure cryptographique (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité* et au Chapitre 13, “Structure de gestion des clés” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour consulter des exemples d'utilisation de la structure cryptographique, reportez-vous au Chapitre 12, “Structure cryptographique (tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité* et aux pages de manuel.

Autorisations de fichiers 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. De plus, ZFS prend en charge les listes de contrôle d'accès (ACL), également appelées entrées de contrôle d'accès (ACE), lesquelles 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 des instructions concernant la définition d'ACL sur des fichiers ZFS, reportez-vous à la page de manuel `chmod(1)`.
- Pour obtenir une vue d'ensemble des autorisations de fichier, reportez-vous à la section "Utilisation des autorisations UNIX pour protéger les fichiers" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour obtenir une vue d'ensemble et des exemples de protection de fichiers ZFS, reportez-vous au Chapitre 8, "Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS" du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS* et aux pages de manuel.

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.

IP Filter

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 :

- Pages de manuel connexes : `ipfilter(5)`, `ipf(1M)`, `ipnat(1M)`, `svc.ipfd(1M)` et `ipf(4)`.
- Pour obtenir une vue d'ensemble d'IP Filter, reportez-vous au Chapitre 20, "IP Filter dans Oracle Solaris (présentation)" du manuel *Administration d'Oracle Solaris : Services IP*.
- Pour consulter des exemples d'utilisation de la fonction IP Filter, reportez-vous au Chapitre 21, "IP Filter (tâches)" du manuel *Administration d'Oracle Solaris : Services IP* et aux pages de manuel.
- 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)`.

Wrappers TCP

Les wrappers TCP permettent d'implémenter des contrôles d'accès en vérifiant à l'aide d'une liste de contrôle d'accès (ACL) l'adresse d'un hôte demandant un service réseau particulier. Les demandes sont accordées ou refusées en conséquence. Les wrappers TCP consignent également

les demandes de services réseau émises par les hôtes, et assurent ainsi une fonction de surveillance utile. Les fonctions Secure Shell et `sendmail` d'Oracle Solaris sont configurées pour utiliser des wrappers TCP. Peuvent notamment être placés sous contrôle d'accès les services réseau `ftpd` et `rpcbind`.

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, reportez-vous aux références suivantes :

- Pour plus d'informations sur les wrappers TCP, reportez-vous à la section "Contrôle d'accès aux services TCP à l'aide des wrappers TCP" du manuel *Administration d'Oracle Solaris : Services IP*.
- 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).

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 fournit un certain nombre de fonctions pouvant être utilisées pour accroître la force des mots de passe utilisateurs. Il est possible de définir la longueur, le contenu, la fréquence de modification des mots de passe ainsi que de conserver un historique des mots de passe. Un dictionnaire des mots de passe à éviter est fourni. Plusieurs algorithmes de mots de passe possibles sont disponibles.

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

- "Gestion du contrôle de connexion" du manuel *Administration d'Oracle Solaris : services de sécurité*
- "Sécurisation des connexions et des mots de passe (liste des tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `passwd`(1) et `crypt.conf`(4).

Module d'authentification PAM

La structure PAM (Pluggable Authentication Module) permet de coordonner et de configurer les exigences d'authentification utilisateur pour les comptes, les informations d'identification, les sessions et les mots de passe.

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 `ftp` utilisent la structure PAM pour s'assurer que tous les points d'entrée du système sont sécurisés. 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 faiblesses sont détectées, et ce sans nécessiter de modification dans les services système utilisant la structure PAM.

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

- Chapitre 15, “Utilisation de PAM” du manuel *Administration d'Oracle Solaris : services de sécurité*
- Page de manuel `pam.conf(4)`

Privilèges dans Oracle Solaris

Les privilèges sont des droits détaillés et discrets sur 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`. Les privilèges peuvent être accordés à une commande, un utilisateur, un rôle ou un système. De nombreuses commandes et démons Oracle Solaris fonctionnent uniquement avec les privilèges strictement nécessaires pour leur permettre d'accomplir leur tâche. L'utilisation de privilèges est également appelée *gestion des droits de processus*.

Des programmes prenant en charge les étiquettes peuvent empêcher les intrus d'obtenir plus de privilèges que le programme lui-même n'en utilise. En outre, les privilèges permettent aux entreprises de limiter les privilèges accordés aux services et aux processus qui s'exécutent sur leurs systèmes.

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

- “Privilèges (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité*
- “Utilisation des privilèges (tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité*
- Chapitre 2, “Developing Privileged Applications” du manuel *Developer's Guide to Oracle Solaris 11 Security*
- Pages de manuel connexes : `ppriv(1)` et `privileges(5)`.

Accès distant

Les attaques distantes peuvent endommager un système et un réseau. La sécurisation de l'accès au réseau est indispensable dans l'environnement Internet actuel et est utile même dans des environnements WAN et LAN.

IPsec et IKE

Le protocole IPsec (IP security) protège les paquets IP en authentifiant les paquets, en les chiffrant ou à l'aide des deux opérations. Oracle Solaris prend en charge IPsec pour les réseaux IPv4 et IPv6. 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 de clés softtoken pour les applications utilisant le metaslot. Lorsque 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 le keystore de clés softtoken.

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 14, “Architecture IPsec (présentation)” du manuel *Administration d'Oracle Solaris : Services IP*
- Chapitre 15, “Configuration d'IPsec (tâches)” du manuel *Administration d'Oracle Solaris : Services IP*
- Chapitre 17, “Protocole IKE (présentation)” du manuel *Administration d'Oracle Solaris : Services IP*
- Chapitre 18, “Configuration du protocole IKE (tâches)” du manuel *Administration d'Oracle Solaris : Services IP*
- Pages de manuel connexes : `ipsecconf`(1M) et `in.iked`(1M).

Secure Shell

La fonction Secure Shell d'Oracle Solaris permet à des utilisateurs ou des services d'accéder ou de transférer des fichiers d'un système distant à un autre via un canal de communication chiffré. Dans Secure Shell, tout le trafic réseau est chiffré. Secure Shell 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 entre un système local et des systèmes distants via un lien réseau authentifié et chiffré.

De cette manière, Secure Shell empêche les intrus potentiels de lire des communications interceptées et empêche un adversaire d'usurper le système. Par défaut, Secure Shell est le seul mécanisme d'accès distant actif sur un nouveau système installé.

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

- Chapitre 17, “Utilisation de Secure Shell (tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `ssh`(1), `sshd`(1M), `sshd_config`(4) et `ssh_config`(4).

Service Kerberos

La fonction Kerberos d'Oracle Solaris permet la connexion unique et des transactions sécurisées et ce, même dans des réseaux hétérogènes exécutant 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 Kerberos est une architecture client-serveur qui 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 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 :

- Partie VI, "Service Kerberos" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `kerberos(5)` et `kinit(1)`.

Contrôle d'accès basé sur les rôles (RBAC)

RBAC applique le principe de sécurité du moindre privilège en permettant aux entreprises d'octroyer de façon sélective des droits d'administration à des utilisateurs ou à des rôles en fonction des besoins spécifiques de ceux-ci.

La fonction RBAC d'Oracle Solaris contrôle l'accès des utilisateurs à des tâches qui seraient normalement réservées au rôle `root`. En appliquant des attributs de sécurité aux processus et aux utilisateurs, RBAC peut répartir les droits d'administration entre plusieurs administrateurs. La fonction RBAC est également appelée *gestion des droits des utilisateurs*.

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

- Partie III, "Rôles, profils de droits et privilèges" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `rbac(5)`, `roleadd(1M)`, `profiles(1)` et `user_attr(4)`.

Utilitaire de gestion des services (SMF)

L'utilitaire de gestion des services (SMF) d'Oracle Solaris permet d'ajouter, de supprimer, de configurer et de gérer les services. SMF utilise RBAC 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 :

- Chapitre 6, “Gestion des services (présentation) ” du manuel *Administration d'Oracle Solaris : Tâches courantes*
- Chapitre 7, “Gestion des services (tâches) ” du manuel *Administration d'Oracle Solaris : Tâches courantes*
- Pages de manuel connexes : `svcadm`(1M), `svcs`(1) et `smf`(5).

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 ACE protègent les fichiers et RBAC prend en charge l'administration déléguée de jeux de données ZFS.

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

- Chapitre 1, “Système de fichiers Oracle Solaris ZFS (introduction)” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
- Chapitre 3, “Différences entre les systèmes de fichiers Oracle Solaris ZFS et classiques” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
- Chapitre 6, “Gestion des systèmes de fichiers Oracle Solaris ZFS” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
- Pages de manuel connexes : `zfs`(1M) et `zfs`(7FS).

Zones Oracle Solaris

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 contrôlent 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.

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

- Partie II, “Oracle Solaris Zones” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*
- Pages de manuel connexes : `brands(5)`, `zoneadm(1M)` et `zonecfg(1M)`.

Trusted Extensions

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. Contrairement à la plupart des autres systèmes d'exploitation multiniveau, Trusted Extensions inclut un bureau multiniveau.

Trusted Extensions répond aux exigences des trois profils reconnus par les Critères communs : LSPP (Labeled Security Protection Profile), RBACPP (Role-Based Access Protection Profile) et CAPP (Controlled Access Protection Profile). Toutefois, Trusted Extensions se distingue par sa capacité à fournir un haut niveau de sécurité tout en maximisant la compatibilité et en minimisant les coûts.

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 d'Oracle Solaris Trusted Extensions*.
- Pour plus d'informations sur l'utilisation du bureau multiniveau, reportez-vous au *Guide de l'utilisateur Oracle Solaris Trusted Extensions*.
- Pages de manuel connexes : `trusted_extensions(5)` et `labeld(1M)`.

Valeurs par défaut de la sécurité Oracle Solaris 11

Après l'installation, Oracle Solaris protège le système contre les intrusions et surveille les tentatives de connexion, entre autres fonctions de sécurité.

Accès au système limité et contrôlé

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. Au départ, le mot de passe de ces deux comptes est identique.

- Une fois la connexion établie, l'utilisateur initial peut assumer le rôle `root` pour poursuivre la configuration du système. Au moment où il assume 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 assumer 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 nommage.

Exigences relatives au mot de passe : les mots de passe utilisateur doivent comporter six caractères au minimum et comprendre au moins un caractère alphabétique et un caractère numérique. 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 d'adresse IP.

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). Etant donné que le rôle `root` ne peut pas se connecter, le nom de l'utilisateur jouant le rôle `root` peut être retrouvé 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 et les applications de bureau sont protégés par le principe du moindre privilège, les autorisations et le 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`, de sorte que 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 sont `drwxr-xr-x` (`755`). Les autorisations du fichier sont `-rw-r--r--` (`644`).

Applets de bureau : les applets de bureau sont protégés par RBAC. Par exemple, seul l'utilisateur initial ou le rôle `root` peuvent utiliser l'applet Gestionnaire de packages pour installer de nouveaux packages. Le Gestionnaire de packages n'est pas visible pour les utilisateurs standard ne disposant pas des droits nécessaires pour l'utiliser.

Des fonctions de sécurité supplémentaires sont en place

Oracle Solaris 11 fournit des fonctions de sécurité permettant de configurer les systèmes et les utilisateurs afin de satisfaire les exigences de sécurité du site.

- **Contrôle d'accès basé sur les rôles (RBAC) :** Oracle Solaris fournit un certain nombre d'autorisations, de privilèges et de profils de droits. Le rôle `root` est le seul rôle défini. Les profils de droits fournissent une bonne base pour la création de rôles personnalisés. En outre, certaines commandes d'administration requièrent des autorisations RBAC afin de pouvoir aboutir. Les utilisateurs ne disposant pas des autorisations ne peuvent pas exécuter les commandes, même s'ils disposent des privilèges nécessaires.
- **Droits des utilisateurs :** les utilisateurs se voient attribuer un ensemble élémentaire 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 contrôlé ” à la page 22. Les tentatives de connexion par les utilisateurs ne sont pas limitées, mais toutes les connexions ayant échoué sont consignées par le service d'audit.

- **Protection des fichiers système :** les fichiers système sont protégés par des autorisations de fichier. Seul le rôle `root` peut modifier les fichiers de configuration du système.

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.

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

- Annexe A, “Stratégie de sécurité du site” du manuel *Configuration et administration d’Oracle Solaris Trusted Extensions*
- “Application des exigences de sécurité” du manuel *Configuration et administration d’Oracle Solaris 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 11

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

Lorsque vous installez le SE Oracle Solaris, sélectionnez le média qui installe 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 le groupe `group/system/solaris-large-server`, qui fournit un environnement Oracle Solaris pour serveur grande capacité.
- **Oracle Solaris Desktop** : l'installation Live Media installe le groupe `group/system/solaris-desktop`, qui fournit un environnement de bureau Oracle Solaris 11.

  Pour créer un système de bureau pour une utilisation centralisée, ajoutez le groupe `group/feature/multi-user-desktop` à un serveur Oracle Solaris. 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*.

Pour vous aider dans votre choix de média, consultez les guides d'installation suivants :

- *Installation des systèmes Oracle Solaris 11*
- *Création d’une image d’installation Oracle Solaris 11 personnalisée*
- *Ajout et mise à jour de packages logiciels Oracle Solaris 11*

Sécurisation du système

Il est recommandé d'effectuer les tâches suivantes dans l'ordre. A ce stade, le SE Oracle Solaris 11 est installé et seul l'utilisateur initial qui peut assumer le rôle `root` a accès au système.

Tâche	Description	Voir
1. Vérification des packages sur le système.	Vérifie que les packages du média d'installation sont identiques aux packages installés.	“Vérification des packages” à la page 27
2. Protection des paramètres du matériel sur le système.	Protège le matériel en exigeant un mot de passe pour toute modification de paramètres matériels.	“Contrôle de l’accès au matériel du système (tâches)” du manuel *Administration d’Oracle Solaris : services de sécurité*

Tâche	Description	Voir
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 27
4. Activation obligatoire de l'allocation de périphériques.	Empêche l'utilisation de médias amovibles sans autorisation explicite. Les périphériques incluent les microphones, les lecteurs USB et les CD.	"Procédure d'activation de l'allocation de périphériques" du manuel *Administration d'Oracle Solaris : services de sécurité*
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 28
6. Création d'un message d'avertissement de connexion reflétant la stratégie de sécurité de votre site.	Avertit les utilisateurs et les attaquants potentiels que le système est surveillé.	"Placement d'un message de sécurité dans les fichiers bannière" à la page 29 "Placement d'un message de sécurité dans l'écran de connexion au bureau" à la page 29

▼ Vérification des packages

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

Avant de commencer Vous devez être dans le rôle `root`.

1 Exécutez la commande `pkg verify`.

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

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

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

3 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`.

▼ Désactivation des services non utilisés

Cette procédure permet de désactiver les services qui, selon la finalité du système concerné, ne sont pas nécessaires.

Avant de commencer Vous devez être dans le rôle `root`.

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

```
# svcs | grep network
online         Sep_07   svc:/network/loopback: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 ou un serveur Web et les 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 6, "Gestion des services (présentation) " du manuel *Administration d'Oracle Solaris : Tâches courantes* et à la page de manuel `svcs(1)`.

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

Cette procédure permet d'empêcher les utilisateurs de ce système de le suspendre ou de le mettre hors tension.

Avant de commencer Vous devez être dans le rôle `root`.

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

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;help=RtConsUser.html
```

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

   Pour plus d'instructions, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" du manuel *Administration d'Oracle Solaris : services de sécurité*.

3. **Mettez en commentaire le profil de droits Console User 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.**

```
# usermod -P +new-profile username
```

Voir aussi Pour plus d'informations, reportez-vous à la section "Fichier policy.conf" du manuel *Administration d'Oracle Solaris : services de sécurité* et 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 d'avertissement reflétant la stratégie de sécurité de votre site. Le contenu de ces fichiers s'affiche lors de la connexion locale et à distance.

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.

Avant de commencer Vous devez être dans le rôle `root`. La meilleure pratique consiste à consulter le conseil juridique de votre entreprise à propos du contenu du message de sécurité.

1 Saisissez un message de sécurité dans le fichier `/etc/issue`.

```
# vi /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.
```

Pour plus d'informations, reportez-vous à la page de manuel `issue`(4).

Le programme `telnet` affiche le contenu du fichier `/etc/issue` en tant que message de connexion. Pour plus d'informations sur l'utilisation de ce fichier par d'autres applications, reportez-vous aux sections "Afficher des messages de sécurité aux utilisateurs `ssh` et `ftp`" à la page 40 et "Placement d'un message de sécurité dans l'écran de connexion au bureau" à la page 29.

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

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

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

Vous avez le choix entre plusieurs méthodes de création d'un message de sécurité que les utilisateurs pourront consulter lors de la connexion.

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.

Avant de commencer Vous devez être dans le rôle `root`. La meilleure pratique consiste à consulter le conseil juridique de votre entreprise à propos du contenu du message de sécurité.

- **Placez un message de sécurité dans l'écran de connexion au bureau**

  Vous disposez de plusieurs possibilités. Les possibilités qui créent une boîte de dialogue peuvent utiliser le fichier `/etc/issue` de l'Étape 1 de la section "Placement d'un message de sécurité dans les fichiers bannière" à la page 29.

  - **POSSIBILITE 1 : créez un fichier de bureau qui affiche le message de sécurité dans la boîte de dialogue lors de la connexion.**

    ```
    # vi /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/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

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

  - **POSSIBILITE 2 : 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, pendant et immédiatement après la connexion au bureau. Ces scripts sont également disponibles dans la version Oracle Solaris 10.

    - **Affichez le message de sécurité avant l'apparition de l'écran de connexion.**

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

- **Affichez le message de sécurité sur l'écran de connexion après l'authentification.**

  Ce script s'exécute avant l'affichage de l'espace de travail de l'utilisateur. Vous modifiez le script `Default.sample` pour créer ce script.

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

- **Affichez le message de sécurité dans l'espace de travail initial de l'utilisateur après l'authentification.**

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

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

- **POSSIBILITE 3 : 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) Après avoir modifié l'interface utilisateur de la fenêtre de connexion, enregistrez une copie.

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

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.

```
# vi /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 assumer 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.

Tâche	Description	Voir
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 33
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 35.
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 34

Tâche	Description	Voir
Présélection de classes d'audit supplémentaires.	Améliore le contrôle 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 36
Envoi de récapitulatifs textuels des événements d'audit vers l'utilitaire `syslog`.	Fournit des informations en temps réel sur les événements d'audit importants, tels que les connexions et les tentatives de connexion.	"Surveillance en temps réel des événements `lo`" à la page 37
Création de rôles.	Répartit des tâches d'administration distinctes parmi plusieurs utilisateurs de confiance afin qu'aucun utilisateur isolé ne puisse endommager le système.	"Configuration de comptes utilisateur" du manuel *Administration d'Oracle Solaris : Tâches courantes* "Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris : services de sécurité* "Procédure d'attribution de rôle" du manuel *Administration d'Oracle Solaris : services de sécurité*.
Affichage des applications autorisées seules sur le bureau d'un utilisateur.	Empêche les utilisateurs de voir ou d'utiliser des applications qu'ils ne sont pas autorisés à utiliser.	Reportez-vous à la section "Limitation d'un utilisateur à des applications de bureau" du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.
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 38

▼ 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 la liste des entrées du fichier `/etc/default/passwd`.

Avant de commencer

Avant de modifier les valeurs par défaut, assurez-vous que les modifications permettent à tous les utilisateurs de s'authentifier auprès de leurs applications et sur d'autres systèmes du réseau.

Vous devez être dans le rôle `root`.

- **Modifiez le fichier `/etc/default/passwd`.**

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

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

```
MAXWEEKS=4
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 la liste des variables qui restreignent la création des mots de passe, reportez-vous au fichier `/etc/default/passwd`. Les valeurs par défaut sont indiquées dans le fichier.
- Pour les contraintes de mot de passe en vigueur après l'installation, reportez-vous à la rubrique “Accès au système limité et contrôlé ” à la page 22.
- Page de manuel `passwd(1)`

▼ 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 – N'activez pas le verrouillage de compte pour les utilisateurs qui peuvent prendre des rôles car vous pouvez verrouiller le rôle.

Avant de commencer

Vous devez être dans le rôle `root`. Ne définissez pas cette protection à l'échelle du système sur un système que vous utilisez pour des activités d'administration.

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

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

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

   - **Effectuez l'activation pour un utilisateur.**

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

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

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

Voir aussi

- Pour une description des attributs de sécurité des utilisateurs et des rôles, reportez-vous au Chapitre 10, “Attributs de sécurité dans Oracle Solaris (référence)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pages de manuel connexes : `policy.conf`(4) et `user_attr`(4).

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

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 être dans le rôle `root`.

- **Modifiez la valeur umask dans les profils de connexion dans les répertoires squelette pour les différents shells.**

  Oracle Solaris fournit des répertoires dans lesquels les administrateurs peuvent personnaliser les valeurs par défaut des shells utilisateur. Les répertoires squelette incluent des fichiers tels que des fichiers `.profile` , `.bashrc` et `.kshrc`.

  Choisissez l'une des valeurs suivantes :

  - `umask 027` : offre une protection modérée des fichiers

    (`740`) : `w` pour le groupe, `rwx` pour les autres utilisateurs
  - `umask 026` : offre une protection légèrement renforcée des fichiers

    (`741`) : `w` pour le groupe, `rw` pour les autres utilisateurs

- `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 de comptes utilisateur" du manuel *Administration d'Oracle Solaris : Tâches courantes*
- "Valeur umask par défaut" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `usermod`(1M) et `umask`(1).

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

Cette procédure permet d'effectuer un audit des commandes d'administration, des tentatives de pénétration du système et d'autres événements importants spécifiés dans la stratégie de sécurité du 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 être dans le rôle `root`. Vous mettez en oeuvre la stratégie de sécurité de votre site en matière d'audit.

1 Réalisation d'un audit de toutes les utilisations de commandes privilégiées faites par des utilisateurs et des rôles.

Ajoutez l'événement d'audit `AUE_PFEXEC` au masque de présélection de tous les utilisateurs et rôles.

```
# usermod -K audit_flags=lo,ps:no username

# rolemod -K audit_flags=lo,ps:no rolename
```

2 Enregistrement des arguments saisis pour les commandes auditées.

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

3 Enregistrement de l'environnement dans lequel les commandes ayant fait l'objet d'un audit sont exécutées.

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

Voir aussi

- Pour plus d'informations sur la stratégie d'audit, reportez-vous à "Stratégie d'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*.

- Pour consulter des exemples de configuration des indicateurs d'audit, reportez-vous à la section "Configuration du service d'audit (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité* et à la section "Dépannage du service d'audit (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour configurer l'audit, reportez-vous à la page de manuel `auditconfig(1M)`.

▼ Surveillance en temps réel des événements lo

Cette procédure permet d'activer le plug-in `audit_syslog` pour les événements que vous souhaitez surveiller au moment même où ils se produisent.

Avant de commencer Vous devez être dans le rôle `root` pour modifier le fichier `syslog.conf`. D'autres étapes nécessitent le profil de droits Audit Configuration (Configuration d'audit).

1. **Envoyez la classe `lo` vers le plug-in `audit_syslog` et activez le plug-in.**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **Ajoutez une entrée `audit.notice` au fichier `syslog.conf`.**

   L'entrée par défaut inclut l'emplacement du fichier journal.

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. **Créez le fichier journal.**

   ```
   # touch /var/adm/auditlog
   ```

4. **Actualisez les informations de configuration du service `syslog`.**

   ```
   # svcadm refresh system/system-log
   ```

5. **Actualisez le service d'audit.**

   Le service d'audit lit les modifications apportées au plug-in d'audit lors de l'actualisation.

   ```
   # audit -s
   ```

Voir aussi

- Pour envoyer les récapitulatifs d'audit à un autre système, reportez-vous à l'exemple suivant "Procédure de configuration des journaux d'audit syslog" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Le service d'audit peut générer une sortie volumineuse. Pour gérer les journaux, reportez-vous à la page de manuel `logadm(1M)`.
- Pour surveiller la sortie, reportez-vous à "Contrôle des récapitulatifs d'audit `audit_syslog`" à la page 55.

▼ Suppression de privilèges de base non utilisés des utilisateurs

Dans certaines circonstances, il est possible de supprimer un ou plusieurs des trois privilèges suivants faisant partie de l'ensemble des privilèges de base des utilisateurs standard.

- `file_link_any` : permet à un processus de créer des liens physiques vers des fichiers appartenant à un ID utilisateur différent de l'ID utilisateur effectif du processus.
- `proc_info` : permet à un processus d'examiner l'état des processus autres que ceux auxquels il peut envoyer des signaux. Les processus qui ne peuvent pas être examinés ne sont pas visibles dans `/proc` et sont considérés comme inexistants.
- `proc_session` : permet à un processus d'envoyer des signaux ou de suivre des processus externes à sa propre session.

Avant de commencer Vous devez être dans le rôle `root`.

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

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

2. **Empêcher un utilisateur d'examiner des processus dont il n'est pas propriétaire.**

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

3. **Empêcher un utilisateur de démarrer une seconde session telle qu'une session `ssh` par exemple à partir de la session en cours.**

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

4. **Supprimer 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
   ```

Voir aussi Pour plus d'informations, reportez-vous au Chapitre 8, “Utilisation des rôles et des privilèges (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité* et à la page de manuel `privileges(5)`.

Sécurisation du noyau

A ce stade, vous avez peut-être créé des utilisateurs qui peuvent assumer des rôles et créé les rôles. Seul le rôle `root` peut modifier les fichiers système.

Tâche	Description	Voir
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 *Administration d'Oracle Solaris : services de sécurité*
Protection des fichiers noyau qui peuvent contenir des informations confidentielles.	Crée un répertoire d'accès restreint dédié aux fichiers noyau.	"Procédure d'activation d'un chemin d'accès au fichier noyau global" du manuel *Administration d'Oracle Solaris : Tâches courantes* "Gestion des fichiers noyau (liste des tâches)" du manuel *Administration d'Oracle Solaris : Tâches courantes*

Configuration du réseau

A ce stade, vous avez peut-être créé des utilisateurs qui peuvent assumer des rôles et créé les rôles. Seul le rôle `root` peut modifier les fichiers système.

Parmi les tâches réseau suivantes, effectuez celles qui fournissent une sécurité supplémentaire en fonction des exigences de votre site. Ces tâches réseau notifient les utilisateurs qui se connectent à distance que le système est protégé et renforcent les protocoles IP, ARP et TCP.

Tâche	Description	Voir
Affichage de messages d'avertissement reflétant la stratégie de sécurité de votre site.	Avertit les utilisateurs et les attaquants potentiels que le système est surveillé.	"Afficher des messages de sécurité aux utilisateurs `ssh` et `ftp`" à la page 40
Désactivation du démon de routage du réseau.	Limite l'accès aux systèmes par des renifleurs de réseau	"Désactivation du démon de routage réseau " à la page 41
Prévention de la diffusion d'informations sur la topologie du réseau.	Empêche la diffusion de paquets.	"Désactivation du transfert de paquets de diffusion" à la page 42
	Désactivation des réponses aux demandes d'écho de diffusion et aux demandes d'écho multidiffusion.	"Désactivation des réponses aux demandes d'écho" à la page 42
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 multiréseau 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 multiréseau strict" à la page 43

Tâche	Description	Voir
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” à la page 44
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 ” à la page 44
Génération de nombres aléatoires forts pour les connexions TCP initiales.	Respecte la valeur de génération de numéro de séquence spécifiée par RFC 1948.	“Spécification d'un numéro aléatoire fort pour la connexion TCP initiale” à la page 45
Restauration des valeurs sécurisées par défaut des paramètres réseau.	Renforce la sécurité lorsqu'elle a été réduite par des actions d'administration.	“Restauration des valeurs sécurisées de paramètres réseau” à la page 45
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. Par défaut, l'application `sendmail` 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 *Administration d'Oracle Solaris : Services réseau*.	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 d'Oracle Solaris : Services IP*. Pour consulter un exemple illustrant la protection du service réseau FTP par des wrappers TCP, reportez-vous à la section “Démarrage d'un serveur FTP à l'aide de SMF” du manuel *Administration d'Oracle Solaris : Services réseau*.

▼ Afficher des messages de sécurité aux utilisateurs ssh et ftp

Utilisez cette procédure pour afficher des messages de sécurité lors de la connexion à distance et du transfert de fichier.

Avant de commencer Vous devez être dans le rôle `root`. Vous avez créé le fichier `/etc/issue` au cours de l'Étape 1 de la section “Placement d'un message de sécurité dans les fichiers bannière” à la page 29.

1 Pour afficher un message de sécurité aux utilisateurs qui se connectent à l'aide de `ssh`, procédez comme suit :

a. Annulez la mise en commentaire de la directive de bannière dans le fichier `/etc/sshd_config`.

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. Actualisez le service `ssh`.

```
# svcadm refresh ssh
```

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

2 Pour afficher un message de sécurité aux utilisateurs qui se connectent via `ftp`, procédez comme suit :

a. Ajoutez la directive `DisplayConnect` au fichier `proftpd.conf`.

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. Redémarrez le service `ftp`.

```
# svcadm restart ftp
```

Pour plus d'informations, reportez-vous au site Web ProFTPD (`http://www.proftpd.org/`).

▼ Désactivation du démon de routage réseau

Cette procédure permet d'empêcher le routage réseau après l'installation en spécifiant un routeur par défaut. Cette procédure peut aussi être effectuée après une configuration manuelle du routage.

Remarque – De nombreuses procédures de configuration requièrent la désactivation du démon de routage. Vous avez donc peut-être désactivé ce démon dans le cadre d'une procédure de configuration générale.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 Assurez-vous que le démon de routage est en cours d'exécution.

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

Si le service n'est pas en cours d'exécution, vous pouvez vous arrêter ici.

2 Désactivez le démon de routage.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 **Vérifiez que le démon de routage est désactivé.**

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

Voir aussi Page de manuel routeadm(1M)

▼ Désactivation du transfert de paquets de diffusion

Par défaut, Oracle Solaris transmet les paquets de diffusion. Si la stratégie de sécurité de votre site exige une réduction du risque de saturation par diffusions, modifiez la valeur par défaut à l'aide de cette procédure.

Remarque – En désactivant la propriété `_forward_directed_broadcasts`, vous désactivez les commandes ping des diffusions.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 **Définissez sur 0 la propriété de transfert des paquets de diffusion pour les paquets IP.**

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 **Contrôlez la valeur en cours.**

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                   PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts  rw   0         --           0         0,1
```

Voir aussi Page de manuel ipadm(1M)

▼ Désactivation des réponses aux demandes d'écho

Cette procédure permet d'empêcher la diffusion d'informations sur la topologie du réseau.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 **Définissez sur 0 la propriété de réponse aux demandes d'écho de diffusion pour les paquets IP, puis contrôlez la valeur en cours.**

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
```

```
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2 Définissez sur 0 la propriété de réponse aux demandes d'écho multidiffusion pour les paquets IP, puis contrôlez la valeur en cours.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

Voir aussi Pour plus d'informations, reportez-vous à la section "_respond_to_echo_broadcast et _respond_to_echo_multicast (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris* et à la page de manuel `ipadm`(1M).

▼ Définition du multiréseau strict

Pour les systèmes constituant des passerelles vers d'autres domaines, tels qu'un pare-feu ou un noeud de réseau privé virtuel (VPN), cette procédure permet d'activer les systèmes multiréseau stricts.

La version Oracle Solaris 11 présente une nouvelle propriété appelée `hostmodel` pour IPv4 et IPv6. Cette propriété contrôle le comportement d'envoi et de réception de paquets IP sur un système multiréseau.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 Définissez la propriété `hostmodel` sur `strong` pour les paquets IP.

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2 Contrôlez la valeur en cours et notez les valeurs possibles.

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

Voir aussi Pour plus d'informations, reportez-vous à la section "hostmodel (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris* et à la page de manuel `ipadm`(1M).

Pour plus d'informations à propos du multiréseau, reportez-vous à la section "Procédure de protection d'un VPN avec IPsec en mode Tunnel" du manuel *Administration d'Oracle Solaris : Services IP*.

▼ Définition du nombre maximal de connexions TCP incomplètes

Cette procédure permet d'empêcher les attaques par déni de service en contrôlant le nombre de connexions en attente incomplètes.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 Définissez le nombre maximal de connexions entrantes.

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2 Contrôlez la valeur en cours.

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0  rw   4096      --           128       1-4294967295
```

Voir aussi Pour plus d'informations, reportez-vous à la section "_conn_req_max_q0" du manuel *Manuel de référence des paramètres réglables Oracle Solaris* et à la page de manuel `ipadm`(1M).

▼ Définition du nombre maximal de connexions TCP en attente

Cette procédure permet d'empêcher les attaques par déni de service en contrôlant le nombre de connexions entrantes autorisées.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué.

1 Définissez le nombre maximal de connexions entrantes.

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2 Contrôlez la valeur en cours.

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q   rw   1024      --           128       1-4294967295
```

Voir aussi Pour plus d'informations, reportez-vous à "_conn_req_max_q" du manuel *Manuel de référence des paramètres réglables Oracle Solaris* et à la page de manuel `ipadm`(1M).

Spécification d'un numéro aléatoire fort pour la connexion TCP initiale

Cette procédure définit le paramètre de génération du numéro de séquence initial TCP de manière à ce qu'il soit conforme à RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`).

Avant de commencer Vous devez être dans le rôle `root` pour modifier un fichier système.

- **Modifiez la valeur par défaut de la variable `TCP_STRONG_ISS`.**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

Restauration des valeurs sécurisées de paramètres réseau

De nombreux paramètres réseau sécurisés par défaut sont réglables et peuvent donc être modifiés. Si les conditions du site le permettent, restaurez les valeurs par défaut des paramètres réglables suivants.

Avant de commencer Le profil de droits Network Management (Gestion du réseau) doit vous avoir été attribué. La valeur actuelle du paramètre est moins sûre que la valeur par défaut.

1. **Définissez sur 0 la propriété de transfert des packages source pour les paquets IP, puis contrôlez la valeur en cours.**

   La valeur par défaut empêche les attaques par déni de service provenant de paquets falsifiés.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

   Pour plus d'informations, reportez-vous à la section "forwarding (ipv4 ou ipv6)" du manuel *Manuel de référence des paramètres réglables Oracle Solaris*.

2. **Définissez sur 0 la propriété de réponse netmask pour les paquets IP, puis contrôlez la valeur en cours.**

   La valeur par défaut empêche la diffusion d'informations sur la topologie du réseau.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 Définissez sur 0 la propriété de réponse de l'horodatage pour les paquets IP, puis contrôlez la valeur en cours.

La valeur par défaut supprime les demandes supplémentaires des unités centrales par rapport aux systèmes et empêche la diffusion d'informations sur le réseau.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp          rw   0         --           0         0,1
```

4 Définissez sur 0 la propriété de réponse de diffusion de l'horodatage pour les paquets IP, puis contrôlez la valeur en cours.

La valeur par défaut supprime les demandes supplémentaires des unités centrales par rapport aux systèmes et empêche la diffusion d'informations sur le réseau.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast rw   0         --           0         0,1
```

5 Définissez sur 0 la propriété ignorer les réacheminements, puis contrôlez la valeur en cours.

La valeur par défaut empêche les demandes supplémentaires des unités centrales par rapport aux systèmes.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6 Empêchez le routage de source IP.

Si vous avez besoin du routage de source IP à des fins de diagnostic, ne désactivez pas ce paramètre réseau.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

Pour plus d'informations, reportez-vous à la section "_rev_src_routes" du manuel *Manuel de référence des paramètres réglables Oracle Solaris*.

7 Définissez sur 0 la propriété ignorer les réacheminements, puis contrôlez la valeur en cours.

La valeur par défaut empêche les demandes supplémentaires des unités centrales par rapport aux systèmes. Normalement, les réacheminements ne sont pas nécessaires sur un réseau bien conçu.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
```

```
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

Voir aussi Page de manuel `ipadm(1M)`

Protection des systèmes de fichiers et des fichiers

Les systèmes de fichiers ZFS sont légers et peuvent être chiffrés, compressés et configurés de manière à respecter des espaces réservés et des limites d'espace disque.

Les tâches ci-après donnent un aperçu des protections disponibles dans ZFS, le système de fichiers par défaut d'Oracle Solaris. Pour plus d'informations, reportez-vous à "Définition des quotas et réservations ZFS" du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS* et à la page de manuel `zfs(1M)`.

Tâche	Description	Voir
Prévention des attaques par déni 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 *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
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 *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
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 *Administration d'Oracle Solaris : Systèmes de fichiers ZFS* "Exemples de chiffrement de systèmes de fichiers ZFS" du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*
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 (`http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf`).	ZFS End-to-End Data Integrity (`http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data`)

Protection et modification de fichiers

Seul le rôle `root` peut modifier les fichiers système.

Tâche	Description	Voir
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 35
Prévention du remplacement de systèmes de fichiers par des fichiers non fiables.	Détecte les fichiers non fiables à l'aide d'un script ou de l'utilitaire BART.	"Procédure de recherche de fichiers avec des autorisations de fichier spéciales" du manuel *Administration d'Oracle Solaris : services de sécurité*

Sécurisation des applications et des services

Vous pouvez configurer les fonctions de sécurité d'Oracle Solaris de manière à protéger vos applications.

Création de zones contenant les applications essentielles

Les zones sont des conteneurs qui isolent les processus. Elles sont particulièrement utiles en tant que conteneurs d'applications et de 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.

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

- Chapitre 15, "Introduction à Oracle Solaris Zones" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*
- "Présentation des zones par fonction" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*
- "Caractéristiques des zones non globales" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*
- "Paramétrage des zones sur le système (liste des tâches)" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.
- Chapitre 16, "Configuration des zones non globales (présentation)" du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

- *Hardening Oracle Database with Oracle Solaris Security Technologies* (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

Gestion des ressources dans les zones

Les zones fournissent un certain nombre d'outils permettant de gérer les ressources des zones.

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

- Chapitre 14, “Exemple de configuration de la gestion des ressources” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*
- Partie I, “Gestion des ressources Oracle Solaris” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*

Configuration d'IPsec et d'IKE

IPsec et IKE protègent les transmissions réseau entre des noeuds et des réseaux conjointement configurés à l'aide d'IPsec et d'IKE.

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

- Chapitre 14, “Architecture IPsec (présentation)” du manuel *Administration d’Oracle Solaris : Services IP*
- Chapitre 17, “Protocole IKE (présentation)” du manuel *Administration d’Oracle Solaris : Services IP*
- Chapitre 15, “Configuration d’IPsec (tâches)” du manuel *Administration d’Oracle Solaris : Services IP*
- Chapitre 18, “Configuration du protocole IKE (tâches)” du manuel *Administration d’Oracle Solaris : Services IP*

Configuration d'IP Filter

La fonction de filtrage IP fournit un pare-feu.

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

- Chapitre 20, “IP Filter dans Oracle Solaris (présentation)” du manuel *Administration d’Oracle Solaris : Services IP*
- Chapitre 21, “IP Filter (tâches)” du manuel *Administration d’Oracle Solaris : Services IP*

Configuration de 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 20, "Planification du service Kerberos" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Chapitre 21, "Configuration du service Kerberos (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Pages de manuel connexes : `kadmin`(1M), `pam_krb5`(5) et `kclient`(1M).

Ajout de SMF à un service hérité

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.

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

- "Procédure d'ajout de propriétés RBAC aux anciennes applications" du manuel *Administration d'Oracle Solaris : services de sécurité*
- 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) et `svccfg`(1M).

Création d'un instantané BART du système

Après avoir configuré le système, vous pouvez créer un ou plusieurs manifestes BART. Ces manifestes constituent des instantanés du système. Vous pouvez ensuite programmer des instantanés à intervalles réguliers et des comparaisons. Pour plus d'informations, reportez-vous à la section "Utilisation de l'utilitaire BART" à la page 53.

Ajout d'une sécurité (étiquetée) multiniveau

Trusted Extensions accroît la sécurité d'Oracle Solaris en imposant une stratégie de contrôle d'accès obligatoire (MAC). 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 `group/feature/trusted-desktop` fournissent 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 des packages, 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 Trusted Extensions” du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*
- Partie II, “Administration de Trusted Extensions ” du manuel *Configuration et administration d'Oracle Solaris 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 14, “Architecture IPsec (présentation)” du manuel *Administration d'Oracle Solaris : Services IP*
- “Administration d'IPsec avec étiquettes” du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*
- “Configuration d'IPsec avec étiquettes (liste des tâches)” du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*

◆ ◆ ◆ CHAPITRE 3

Surveillance et maintenance de la sécurité d'Oracle Solaris 11

Oracle Solaris fournit deux outils système permettant de surveiller l'état de la sécurité, l'utilitaire BART (Basic Audit Reporting Tool) et le service d'audit. Différents programmes et applications peuvent également générer des journaux d'accès et d'utilisation.

Utilisation de l'utilitaire BART

Les manifestes BART constituent un enregistrement des éléments installés sur votre système à un moment donné. Il est possible de comparer les manifestes BART créés au fil du temps et sur différents systèmes afin d'assurer un suivi des modifications apportées aux systèmes installés et des différences entre les systèmes.

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

- "Outil de génération de rapports d'audit de base (présentation)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- "Utilisation de BART (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- "Manifestes BART, fichiers de règles et rapports (référence)" du manuel *Administration d'Oracle Solaris : services de sécurité*

Pour des instructions plus détaillées sur le suivi des modifications apportées aux systèmes installés, reportez-vous à la section "Procédure de comparaison des manifestes pour le même système dans le temps" du manuel *Administration d'Oracle Solaris : services de sécurité*.

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 Partie VII, "Audit dans Oracle Solaris" du manuel *Administration d'Oracle Solaris : services de sécurité*.

- Chapitre 26, "Audit (présentation)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Chapitre 27, "Planification de l'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Chapitre 28, "Gestion de l'audit (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*
- Chapitre 29, "Audit (référence)" du manuel *Administration d'Oracle Solaris : services de sécurité*

  Pour obtenir la liste des pages de manuel et des liens correspondants, reportez-vous à la section "Pages de manuel du service d'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*.

Pour satisfaire aux conditions requises par votre site, les procédures de service d'audit suivantes peuvent être utiles :

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

  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 un rôle, reportez-vous à "Procédure de création d'un rôle" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Contrôlez les récapitulatifs textuels des événements ayant fait l'objet d'un audit dans l'utilitaire `syslog`

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

  Voir "Procédure de configuration des journaux d'audit syslog" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 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 "Procédure d'affectation de l'espace d'audit pour la piste d'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 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 récapitulatifs d'audit audit_syslog

Le plug-in `audit_syslog` vous permet d'enregistrer des récapitulatifs d'événements d'audit présélectionnés.

Vous pouvez afficher les récapitulatifs d'audit dans une fenêtre de terminal lors de leur génération en exécutant une commande semblable à celle-ci :

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

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 *Administration d'Oracle Solaris : services de sécurité*
- "Procédure de contrôle du dépassement de la piste d'audit" du manuel *Administration d'Oracle Solaris : services de sécurité*
- "Gestion des enregistrements d'audit sur les systèmes locaux (tâches)" du manuel *Administration d'Oracle Solaris : services de sécurité*

Repérage de fichiers non fiables

Vous pouvez repérer l'utilisation éventuellement non autorisée des autorisations `setuid` et `setgid` sur les programmes. Un fichier exécutable suspect a pour propriétaire un utilisateur, et non un compte système tel que `root` ou `bin`.

Pour plus d'informations sur la procédure et pour obtenir un exemple, reportez-vous à "Procédure de recherche de fichiers avec des autorisations de fichier spéciales" du manuel *Administration d'Oracle Solaris : services de sécurité*.

◆ ◆ ◆ 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 Oracle Solaris 11

Le livre et les articles ci-dessous contiennent des descriptions de la sécurité sur les systèmes Oracle Solaris 11.

- *Administration d'Oracle Solaris : services de sécurité*

  Ce guide de sécurité est publié par Oracle et est destiné aux administrateurs d'Oracle Solaris 11. Il décrit les fonctions de sécurité d'Oracle Solaris et leur usage lors de la configuration de votre système. La préface contient des liens vers d'autres guides d'administration système Oracle Solaris contenant des informations de sécurité.

- *Oracle Solaris Security: Oracle Solaris Express (*`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`*)*.

  Cet article fournit un aperçu des fonctions de sécurité de la version actuelle d'Oracle Solaris, édition de novembre 2010.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  Cet article fournit un aperçu des fonctions de la version actuelle d'Oracle Solaris, édition de novembre 2010.

Pour consulter des références utiles relatives à Oracle Solaris 10, reportez-vous à *Oracle Solaris 10 Security Guidelines*.