Sécurisation des systèmes et des périphériques connectés dans Oracle® Solaris 11.2

Référence: E53942-02
Septembre 2014

Table des matières

Utilisation de la présente documentation

Securing Systems and Attached Devices in Oracle® Solaris 11.2 explique comment protéger et contrôler votre système Oracle Solaris contre tout accès non autorisé.

- **Présentation** : description de différentes méthodes permettant de sécuriser les systèmes et les périphériques contre tout accès non autorisé.
- **public visé** : les administrateurs chargés de mettre en oeuvre la sécurité sur le réseau de l'entreprise.
- **Connaissances requises** : être familiarisé avec les concepts et fonctions de sécurité pris en charge dans Oracle Solaris.

Bibliothèque de la documentation des produits

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

Accès aux services de support Oracle

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

Commentaires en retour

Vous pouvez faire part de vos commentaires sur cette documentation à l'adresse http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

Gestion de la sécurité des machines

La préservation de la sécurité des informations d'un ordinateur constitue une responsabilité d'administration du système importante. Ce chapitre fournit des informations générales sur la gestion de la sécurité de la machine.

Nouveautés dans le manuel Sécurisation des systèmes et des périphériques dans Oracle Solaris 11.2

Cette section met en évidence sur des informations importantes pour les utilisateurs existants les nouvelles fonctions de cette version qui sécurisent les systèmes et les périphériques contre tout accès non autorisé.

- La vérification d'initialisation de la prise en charge les noyaux protège le système d'exploitation. Pour plus d'informations, reportez-vous à la section “Utilisation de Verified Boot” à la page 31.
- Prise en charge des modules TPM (Trusted Platform Modules) Pour plus d'informations, reportez-vous à la section “Initialisation de TPM sur les systèmes Oracle Solaris” à la page 39.

Contrôle de l'accès à un système informatique

Dans une entreprise, tous les ordinateurs connectés à un serveur peuvent être considérés comme un grand système multiforme. Vous êtes responsable de la sécurité de ce vaste système. Vous

devez défendre le réseau contre les tentatives d'accès par des intrus. Vous devez également garantir l'intégrité des données sur les ordinateurs à l'intérieur du réseau.

Au niveau des fichiers, Oracle Solaris fournit des fonctionnalités de sécurité standard que vous pouvez utiliser pour protéger les fichiers, répertoires et périphériques. Au niveau du système et du réseau, les problèmes de sécurité sont pratiquement identiques. La première ligne de défense de la sécurité est le contrôle de l'accès à votre système, comme décrit dans les sections suivantes.

Maintenance de la sécurité physique

Pour contrôler l'accès à votre système, vous devez maintenir la sécurité physique de votre environnement informatique. Par exemple, un système qui est connecté et laissé sans surveillance est vulnérable aux accès non autorisés. Un intrus peut accéder au système d'exploitation et au réseau. La zone alentour de l'ordinateur et le matériel de l'ordinateur doivent être physiquement protégés contre tout accès non autorisé.

Vous pouvez protéger un système SPARC contre tout accès non autorisé aux paramètres du matériel. Utilisez la commande `eeprom` pour exiger un mot de passe pour accéder à la PROM. Pour plus d'informations, reportez-vous à la section “Spécification d'un mot de passe obligatoire pour l'accès au matériel SPARC” à la page 57. Pour protéger le matériel x86, consultez la documentation du fournisseur.

Gestion du contrôle de connexion

Vous pouvez empêcher toute connexion non autorisée à un système ou au réseau, par le biais de l'affectation d'un mot de passe et du contrôle de connexion. Un mot de passe est un mécanisme d'authentification simple. Tous les comptes sur un système doivent disposer d'un mot de passe. Un compte sans mot de passe rend l'ensemble du réseau accessible à un intrus ayant deviné un nom d'utilisateur. Un algorithme de mot de passe fort protège contre les attaques en force.

Lorsqu'un utilisateur se connecte à un système, la commande `login` vérifie le service de noms adéquat ou la base de données de service d'annuaire adéquate en fonction des informations présentes dans le service de commutation de noms, `svc:/system/name-service/switch` . Pour changer les valeurs dans un service de noms SMF, vous utilisez la base de données des commandes. Les services de noms indiquent l'emplacement des bases de données qui peuvent avoir une incidence sur la connexion :

- `files` : désigne les fichiers `/etc` sur le système local
- `ldap` : désigne le service d'annuaire LDAP sur le serveur LDAP
- `nis` : désigne la base de données NIS sur le serveur maître NIS
- `dns` : désigne le service de noms de domaine sur le réseau

Pour une description du service de noms, reportez-vous à la page de manuel `nscd`(1M). Pour plus d'informations sur les services de noms et les services d'annuaire, reportez- vous aux sections “ Utilisation des services de noms et d’annuaire Oracle Solaris 11.2 : DNS et NIS ” et “ Utilisation des services de noms et d’annuaire Oracle Solaris 11.2 : LDAP ”.

La commande `login` vérifie l'identifiant et le mot de passe indiqués par l'utilisateur. Si le nom d'utilisateur ne figure pas dans la base de données des mots de passe, la commande `login` refuse l'accès au système. Si le mot de passe ne correspond pas au nom d'utilisateur spécifié, la commande `login` refuse l'accès au système. Lorsque l'utilisateur fournit un nom d'utilisateur valide et son mot de passe correspondant, le système accorde à l'utilisateur l'accès au système.

Des modules PAM peuvent simplifier la connexion aux applications après une connexion réussie au système. Pour plus d'informations, voir Chapitre 1, “ Utilisation de modules d’authentification enfichables ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”.

Des mécanismes d'authentification et d'autorisation sophistiqués sont disponibles sur les systèmes Oracle Solaris. Pour une description des mécanismes d'authentification et d'autorisation au niveau du réseau, reportez-vous à la section “Authentification et autorisation pour l'accès à distance” à la page 27.

Gestion des informations de mot de passe

Lorsque des utilisateurs se connectent à un système, ils doivent fournir un nom d'utilisateur et un mot de passe. Bien que les informations de connexion soient publiquement connues, les mots de passe doivent être tenus secrets. Les mots de passe ne doivent être connus que des utilisateurs. Les utilisateurs doivent choisir leurs mots de passe avec soin et les modifier souvent.

Les mots de passe sont initialement créés lorsque vous configurez un compte utilisateur. Pour assurer la sécurité des comptes utilisateur, vous pouvez configurer le vieillissement du mot de passe afin d'obliger les utilisateurs à en changer régulièrement. Vous pouvez également désactiver un compte utilisateur en verrouillant le mot de passe. Pour plus d'informations sur l'administration des mots de passe, reportez-vous au Chapitre 1, “ Gestion des comptes et des environnements utilisateur ” du manuel “ Gestion des comptes utilisateur et des environnements utilisateur dans Oracle Solaris 11.2 ” et à la page de manuel `passwd`(1).

Mots de passe locaux

Si votre réseau utilise des fichiers locaux pour authentifier les utilisateurs, les informations du mot de passe sont conservées dans les fichiers `/etc/passwd` et `/etc/shadow` du système. Le nom de l'utilisateur et les autres informations apparentées sont conservés dans le fichier `/etc/passwd`. Les mots de passe chiffrés eux-mêmes sont conservés dans un fichier *shadow* séparé, `/etc/shadow` Cette mesure de sécurité empêche les utilisateurs d'accéder aux mots de passe

chiffrés. Alors que le fichier `/etc/passwd` est accessible à tous ceux qui peuvent se connecter à un système, seul le compte `root` peut lire le fichier `/etc/shadow`. Vous pouvez utiliser la commande `passwd` pour modifier un mot de passe utilisateur sur un système local.

Mots de passe NIS

Si votre réseau utilise NIS pour authentifier des utilisateurs, les informations de mots de passe sont conservées dans la carte des mots de passe NIS. NIS ne prend pas en charge le vieillissement des mots de passe. Vous pouvez utiliser la commande `passwd -r nis` pour modifier le mot de passe d'un utilisateur qui est stocké dans une carte de mots de passe NIS.

Mots de passe LDAP

Le service de noms LDAP d'Oracle Solaris stocke les informations de mot de passe et les informations en double dans le conteneur `ou=people` de la structure de répertoire LDAP. Sur le client du service de noms LDAP d'Oracle Solaris, vous pouvez utiliser la commande `passwd -r ldap` pour changer le mot de passe d'un utilisateur. Le service de noms LDAP stocke le mot de passe dans le référentiel LDAP.

La stratégie de mot de passe est appliquée sur le Oracle Directory Server Enterprise Edition. Plus précisément, le module `pam_ldap` du client suit les contrôles de stratégie de mot de passe mis en oeuvre sur Oracle Directory Server Enterprise Edition. Pour plus d'informations, reportez-vous à la section " Modèle de sécurité des services de noms LDAP " du manuel " Utilisation des services de noms et d'annuaire Oracle Solaris 11.2 : LDAP ".

Chiffrement du mot de passe

Le chiffrement du mot de passe fort constitue une première barrière contre les attaques. Le logiciel Oracle Solaris fournit six algorithmes de chiffrement de mot de passe. Les algorithmes Blowfish et SHA permettent le chiffrement fiable des mots de passe.

Remarque - Pour être certifié FIPS 140, utilisez les algorithmes SHA. Pour plus d'informations, reportez-vous à la section " passwd Command as a FIPS 140 Consumer " du manuel " Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ".

Identificateurs d'algorithmes de mot de passe

La configuration des algorithmes de mot de passe de votre site est effectuée dans le fichier `/etc/security/policy.conf`. Dans le fichier `policy.conf` , les algorithmes sont nommés par leur identificateur, comme indiqué dans le tableau ci-après. Pour la mise en correspondance des identificateurs et des algorithmes, reportez-vous au fichier `/etc/security/crypt.conf`.

Remarque - Utilisez des algorithmes certifiés FIPS lorsque cela est possible. Pour obtenir des listes d'algorithmes certifiés FIPS, reportez-vous à la section " FIPS 140 Algorithm Lists and Certificate References for Oracle Solaris Systems " du manuel " Using a FIPS 140 Enabled System in Oracle Solaris 11.2 " .

TABLEAU 1-1 Algorithmes de chiffrement de mot de passe

Identifiant	Description	Page de manuel de l'algorithme
`1`	Algorithme MD5 compatible avec des algorithmes MD5 sur des systèmes BSD et Linux.	`crypt_bsdmd5`(5)
`2a`	Algorithme Blowfish compatible avec l'algorithme Blowfish existant sur les systèmes BSD. **Remarque -** Pour promouvoir la sécurité FIPS 140, supprimez l'algorithme Blowfish (2a) de l'entrée `CRYPT_ALGORITHMS_ALLOW=2a,5,6` dans le fichier `/etc/security/policy.conf`.	`crypt_bsdbf`(5)
`md5`	L'algorithme Sun MD5 est considéré comme plus puissant que la version BSD et Linux de MD5.	`crypt_sunmd5`(5)
`5`	Algorithme SHA256. SHA est l'acronyme de Secure Hash Algorithm (algorithme de hachage sécurisé). Cet algorithme est un membre de la famille SHA-2. SHA256 prend en charge des mots de passe à 255 caractères. Il s'agit de l'algorithme par défaut, `(CRYPT_DEFAULT)`.	`crypt_sha256`(5)
`6`	Algorithme SHA512.	`crypt_sha512`(5)
`__unix__`	Désapprouvé. Algorithme de chiffrement UNIX standard. Cet algorithme peut être utile lors de la connexion aux anciens systèmes.	`crypt_unix`(5)

Remarque - L'algorithme qui est utilisé pour un mot de passe initial de l'utilisateur continue à être utilisée pour la génération de nouveau mot de passe même si un autre utilisateur a peut - être été sélectionné algorithme par défaut avant de générer un nouveau mot de passe pour cet utilisateur. Ce mécanisme s'applique dans les conditions suivantes :

- L'algorithme est inclus dans la liste des algorithmes autorisés à utiliser pour le chiffrement des mots de passe.
- Identificateur non `_unix_`.

Pour connaître les procédures de changement d'algorithme pour le chiffrement des mots de passe, reportez-vous à la section "Modification de l'algorithme par défaut pour le chiffrement de mot de passe" à la page 51.

Configuration des algorithmes dans le fichier `policy.conf`

La configuration des algorithmes par défaut dans le fichier `policy.conf` est la suivante :

```
#
…
# crypt(3c) Algorithms Configuration
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed
to
# be used for new passwords.  This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6

# To deprecate use of the traditional unix algorithm, uncomment below
# and change CRYPT_DEFAULT= to another algorithm.  For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__

# The Oracle Solaris default is a SHA256 based algorithm.  To revert to
# the policy present in Solaris releases set CRYPT_DEFAULT=__unix__,
# which is not listed in crypt.conf(4) since it is internal to libc.
#
CRYPT_DEFAULT=5
…
```

Si vous modifiez la valeur de `CRYPT_DEFAULT`, les mots de passe des nouveaux utilisateurs sont chiffrés avec l'algorithme associé à la nouvelle valeur.

Lorsque des utilisateurs existants modifient leur mot de passe, le chiffrement de leur ancien mot de passe a une incidence sur l'algorithme utilisé pour chiffrer le nouveau mot de passe. Par exemple, supposons que `CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6`, et `CRYPT_DEFAULT=6`. Le tableau ci-dessous montre quel algorithme sera utilisé pour générer le mot de passe chiffré. L'identificateur le mot de passe se compose d'algorithme.

Mot de passe initial	Mot de passe modifié	Explication
`1` = `crypt_bsdmd5`	Utilise le même algorithme	L'identificateur `1` est dans la liste `CRYPT_ALGORITHMS_ALLOW`. Le mot de passe de l'utilisateur continue d'être chiffré avec l'algorithme `crypt_bsdmd5`.
`2a` = `crypt_bsdbf`	Utilise le même algorithme	L'identificateur `2a` est dans la liste `CRYPT_ALGORITHMS_ALLOW`. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme `crypt_bsbdf`.
`md5` = `crypt_md5`	Utilise le même algorithme	L'identificateur `md5` est dans la liste `CRYPT_ALGORITHMS_ALLOW`. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme `crypt_md5`.
`5` = `crypt_sha256`	Utilise le même algorithme	L'identificateur `5` est dans la liste `CRYPT_ALGORITHMS_ALLOW`. Par conséquent, le nouveau mot de passe continue à être chiffré avec l'algorithme `crypt_sha256` algorithm.

Mot de passe initial	Mot de passe modifié	Explication
6 = crypt_sha512	Utilise le même algorithme	L'identificateur6 est la valeur de CRYPT_DEFAULT. Par conséquent, le nouveau mot de passe continue à être chiffré avec l'algorithme crypt_sha512 algorithm.
__unix__ = crypt_unix	utilise l'algorithme crypt_sha512	L'identificateur __unix__ n'est pas dans la liste CRYPT_ALGORITHMS_ALLOW. Par conséquent, l'algorithme crypt_unix ne peut pas être utilisé. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme CRYPT_DEFAULT.

Pour plus d'informations sur la configuration des sélections d'algorithme, reportez-vous à la page de manuel policy.conf(4) Pour spécifier les algorithmes de chiffrement des mots de passe, consultez “Modification de l'algorithme par défaut pour le chiffrement de mot de passe” à la page 51.

Comptes système spéciaux

Le compte root fait partie de plusieurs comptes *système* spéciaux. Parmi ces comptes, seul le compte root est associé à un mot de passe et peut se connecter. Le compte nuucp peut se connecter pour les transferts de fichiers. Les autres comptes système protègent les fichiers ou exécutent des processus administratifs sans recourir aux pleins pouvoirs de root.

Attention - Ne modifiez jamais la définition du mot de passe d'un compte système. Les comptes système dans Oracle Solaris sont fournis dans un état sûr et sécurisé. Il est interdit de modifier ou créer des fichiers système ayant une UID égale ou inférieure à 101.

Le tableau suivant décrit certains comptes système et leur utilisation. Les comptes système exécutent des fonctions spéciales. Chaque compte de cette liste possède un ID utilisateur inférieur à 100. Pour obtenir la liste complète des systèmes de fichiers, utilisez la commande logins -s.

TABLEAU 1-2 Comptes système sélectionnés et leurs utilisations

Compte système	UID	Utilisation
root	0	N'a pratiquement pas de restrictions. Peut remplacer d'autres protections et autorisations. Le compte root a accès à l'ensemble du système. Le mot de passe pour le compte root doit être très soigneusement protégé. Le compte root est propriétaire de la plupart des commandes Oracle Solaris.
daemon	1	Contrôle le traitement en arrière-plan.
bin	2	Est propriétaire de certaines commandes Oracle Solaris.
sys	3	Est propriétaire de nombreux fichiers système.
adm	4	Est propriétaire de certains fichiers administratifs.

Compte système	UID	Utilisation
`lp`	`71`	Est propriétaire des fichiers de données d'objet et des fichiers de données mis en spool pour l'imprimante.
`uucp`	`5`	Est propriétaire des fichiers de données d'objet et des fichiers de données mis en spool pour UUCP, le programme de copie UNIX-to-UNIX.
`nuucp`	`9`	Utilisé par les systèmes distants pour se connecter au système et démarrer des transferts de fichiers.

Connexions à distance

Les connexions à distance constituent une cible tentante pour les intrus. Oracle Solaris fournit plusieurs commandes pour surveiller, limiter et désactiver les connexions à distance. Pour plus d'informations sur les procédures, reportez-vous au tableau Tableau 3-1, “Sécurisation des connexions et des mots de passe (Liste des tâches)”.

Par défaut, les connexions à distance ne peuvent ni contrôler ni lire certains périphériques système tels que la souris, le clavier, la mémoire graphique ou le périphérique audio. Pour plus d'informations, reportez-vous à la page de manuel `logindevperm`(4).

Contrôle de l'accès aux périphériques

Les périphériques reliés à un système informatique représentent un risque pour la sécurité. Les microphones peuvent capter des conversations, puis les transmettre à des systèmes distants. Les CD-ROM peuvent laisser des informations pouvant être lues par l'utilisateur suivant de l'unité de CD-ROM. Les imprimantes sont accessibles à distance. Les périphériques qui font partie intégrante du système, par exemple, des interfaces réseau telles que `bge0`, peuvent également présenter des problèmes de sécurité.

Le logiciel Oracle Solaris offre plusieurs méthodes de contrôle d'accès aux périphériques.

- **Définition de la stratégie de périphériques** : vous pouvez exiger que le processus accédant à un périphérique particulier s'exécute avec un ensemble de privilèges. Les processus ne disposant pas de ces privilèges ne peuvent pas utiliser le périphérique. Au moment de l'initialisation, le logiciel Oracle Solaris configure la stratégie de périphériques. Les pilotes tiers peuvent être configurés avec la stratégie de périphériques au cours de l'installation. Après l'installation, vous pouvez, en tant qu'administrateur, ajouter une stratégie de périphériques à un périphérique.
- **Rendre des périphériques allouables** : vous pouvez exiger que l'utilisateur alloue un périphérique avant de pouvoir l'utiliser. L'allocation limite l'utilisation d'un périphérique à un utilisateur à la fois. Vous pouvez en outre exiger que l'utilisateur soit autorisé à utiliser le périphérique.

- **Empêcher l'utilisation de périphériques** : vous pouvez empêcher l'utilisation d'un périphérique, tel qu'un microphone, quel que soit l'utilisateur sur un système informatique. Par exemple, un ordinateur kiosque peut être un poste approprié pour rendre certains périphériques indisponibles.
- **Confiner un périphérique dans une zone particulière** : vous pouvez affecter l'utilisation d'un périphérique à une zone non globale. Pour plus d'informations, reportez-vous à la section " Utilisation de périphériques dans les zones non globales " du manuel " Création et utilisation des zones Oracle Solaris ". Pour une analyse plus générale des périphériques et des zones, reportez-vous à la section " Système de fichiers /dev dans les zones non globales " du manuel " Présentation d'Oracle Solaris Zones ".

Stratégie de périphériques

Le mécanisme de la stratégie de périphériques vous permet d'indiquer que des processus permettant d'ouvrir un périphérique nécessitent certains privilèges. Les périphériques protégés par une stratégie de périphériques ne sont accessibles que par les processus s'exécutant avec les privilèges spécifiés par la stratégie correspondante. Oracle Solaris fournit une stratégie de périphériques par défaut. Par exemple, des interfaces réseau telles que `bge0` exigent que les processus accédant à l'interface s'exécutent avec le privilège `net_rawaccess`. L'exigence est appliquée dans le noyau. Pour plus d'informations sur les privilèges, reportez-vous à la rubrique " Processus Rights Management " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Dans Oracle Solaris, les périphériques sont protégés par des autorisations de fichier *et* par une stratégie de périphériques. Par exemple, le fichier `/dev/ip` a `666` autorisations. Cependant, le périphérique peut uniquement être ouvert par un processus disposant des privilèges appropriés.

La configuration de la stratégie de périphériques peut être auditée. L'événement d'audit `AUE_MODDEVPLCY` enregistre les modifications apportées à la stratégie de périphériques.

Pour plus d'informations sur la stratégie de périphériques, reportez-vous aux sections suivantes :

- Tableau 4-1, "Configuration de la stratégie de périphériques (Liste des tâches)"
- "Commandes de la stratégie de périphériques" à la page 71
- " Privilèges et périphériques " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 "

Allocation de périphériques

Le mécanisme d'allocation des périphériques vous permet de limiter l'accès à un périphérique, tel qu'un CD-ROM. Si l'allocation des périphériques n'est pas activée, les périphériques ne sont protégés que par les autorisations de fichier. Par exemple, par défaut, les périphériques sont disponibles pour les utilisations suivantes :

- Tous les utilisateurs peuvent lire et écrire sur CD-ROM ou sur disque.
- Tous les utilisateurs peuvent connecter un microphone.
- Tous les utilisateurs peuvent accéder à une imprimante connectée.

L'allocation des périphériques peut limiter l'utilisation d'un périphérique aux utilisateurs autorisés. L'allocation des périphériques peut également empêcher tout accès à un périphérique. Un utilisateur qui alloue un périphérique bénéficie d'un usage exclusif jusqu'à ce que l'utilisateur libère le périphérique. Lorsqu'un périphérique est libéré, des scripts de nettoyage de périphériques effacent toutes les données résiduelles. Vous pouvez écrire un script de nettoyage de périphériques pour supprimer des informations sur des périphériques ne disposant pas de script. Pour un exemple, reportez-vous à la section “Ecriture de nouveaux scripts de nettoyage de périphériques” à la page 79.

Les tentatives visant à allouer ou libérer un périphérique et à répertorier les périphériques allouables peuvent être auditées. Les événements d'audit font partie de l'`autre` classe d'audit.

Pour plus d'informations sur l'allocation de périphériques, reportez-vous aux sections suivantes :

- Tableau 4-2, “Gestion de l'allocation des périphériques (liste des tâches)”
- “Allocation de périphériques” à la page 72
- “Commandes d'allocation de périphériques” à la page 73

Contrôle de l'accès aux ressources de la machine

Certaines ressources système sont protégées par défaut. En outre, en tant qu'administrateur système, vous pouvez contrôler et surveiller l'activité du système. Vous pouvez définir des limites quant aux utilisateurs pouvant utiliser les ressources. Vous pouvez consigner l'utilisation des ressources et surveiller qui utilise les ressources. Vous pouvez également configurer vos systèmes pour réduire l'utilisation inappropriée des ressources.

Randomisation du format d'espace d'adressage

Oracle Solaris étiquette un grand nombre de ses fichiers binaires utilisateur afin de permettre la randomisation du format d'espace d'adressage (ASLR). ASLR randomise l'adresse de début des éléments clés de l'espace d'adressage. Ce mécanisme de défense de sécurité peut entraîner l'échec des attaques ROP (Return Oriented Programming) lorsqu'elles tentent d'exploiter les vulnérabilités logicielles.

Les zones héritent de ce format aléatoire pour leurs processus. Dans la mesure où l'utilisation de la fonction ASLR risque de ne pas être optimale pour tous les fichiers binaires, elle peut être configurée au niveau des zones et au niveau des fichiers binaires.

Les trois configurations ASLR sont les suivantes :

- **Désactivée** : la fonction ASLR est désactivée pour tous les fichiers binaires.
- **Fichiers binaires étiquetés** : la fonction ASLR est contrôlée par l'étiquette codée dans les fichiers binaires.

  La valeur Oracle Solaris par défaut pour ASLR est `tagged-binaries`. Dans Oracle Solaris, de nombreux fichiers binaires sont étiquetés pour utiliser la fonction ASLR.
- **Activée** : la fonction ASLR est activée pour tous les fichiers binaires, à l'exception de ceux qui sont étiquetés explicitement pour la désactiver.

La commande `sxadm` permet de configurer la fonction ASLR. Vous devez prendre le rôle `root` pour exécuter cette commande. Pour obtenir des exemples et des informations, reportez-vous à la page de manuel `sxadm`(1M). Pour plus d'informations, reportez-vous au " Developer's Guide to Oracle Solaris 11 Security ".

Limitation et contrôle de l'accès superutilisateur

Votre système nécessite un mot de passe `root` pour l'accès superutilisateur. Dans la configuration par défaut, l'utilisateur ne peut pas se connecter à distance à un système en tant que `root`. Lors d'une connexion à distance, un utilisateur doit se connecter avec son nom d'utilisateur, puis utiliser la commande `su` pour se connecter en tant que `root`. Vous pouvez surveiller les personnes utilisant la commande `su`, en particulier les utilisateurs qui essaient d'obtenir un accès superutilisateur. Pour plus d'informations sur les procédures permettant de surveiller le superutilisateur et de limiter l'accès au superutilisateur, reportez-vous à la section "Contrôle et restriction de l'accès `root`" à la page 54.

Configuration du contrôle d'accès basé sur les rôles pour remplacer le superutilisateur

Fonction d'Oracle Solaris, le contrôle d'accès basé sur les rôles (RBAC) est conçu pour distribuer les capacités du superutilisateur à des rôles d'administration. Le superutilisateur, utilisateur `root`, a accès à toutes les ressources du système. Avec RBAC, vous pouvez remplacer de nombreuses responsabilités du rôle `root` par un ensemble de rôles disposant de pouvoirs discrets. Par exemple, vous pouvez configurer un rôle pour gérer la création des comptes utilisateur, et un autre rôle pour gérer les modifications d'un fichier du système. Même si vous ne pouvez pas modifier le compte `root`, vous pouvez le laisser en tant que rôle, puis ne pas attribuer ce rôle. Cette stratégie supprime l'accès `root` au système.

Chaque rôle exige qu'un utilisateur connu se connecte avec son nom d'utilisateur et son mot de passe. Une fois connecté, l'utilisateur prend le rôle avec un mot de passe spécifique. Pour plus d'informations sur RBAC, reportez-vous à la section " Utilisateur Rights Management " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Prévention des mauvaises utilisations involontaires des ressources système

Vous pouvez empêcher vos utilisateurs et vous-même de commettre des erreurs involontaires de l'une des façons suivantes :

- Vous pouvez empêcher l'exécution d'un cheval de Troie en définissant correctement la variable `PATH`.
- Vous pouvez affecter un shell restreint aux utilisateurs. Un shell restreint empêche les erreurs d'utilisateurs en orientant ceux-ci vers les parties du système dont ils ont besoin pour effectuer leurs tâches. Une configuration réalisée avec soin permet de vous assurer que les utilisateurs accèdent uniquement aux parties du système requises pour travailler efficacement.
- Vous pouvez définir des autorisations restrictives sur les fichiers auxquels les utilisateurs n'ont pas besoin d'accéder.

Définition de la variable `PATH`

Veillez à définir correctement la variable `PATH`. Dans le cas contraire, vous risquez d'exécuter par mégarde un programme introduit par un tiers qui crée un risque de sécurité. Le programme intrusif peut altérer vos données ou endommager votre système. Ce type de programme est appelé un *cheval de Troie*. Par exemple, un programme `su` de substitution peut être placé dans un répertoire public où, en tant qu'administrateur système, vous pouvez exécuter le programme de substitution. Un tel script ressemble exactement à la commande `su` standard. Etant donné que le script se supprime lui-même après l'exécution, vous disposez de peu de moyens de prouver que vous avez réellement exécuté un cheval de Troie.

La variable `PATH` est automatiquement définie au moment de la connexion. Le chemin d'accès est défini par l'intermédiaire de vos fichiers d'initialisation, comme `.bashrc` et `/etc/profile`. Lorsque vous configurez le chemin de recherche d'utilisateur pour que le répertoire courant (`.`) apparaisse en dernier, vous êtes protégé contre l'exécution de ce type de cheval de Troie. La variable `PATH` du compte `root` ne doit absolument pas inclure le répertoire actuel.

Affectation d'un shell restreint à des utilisateurs

Le shell standard permet d'ouvrir des fichiers, d'exécuter des commandes, etc. Le shell restreint limite la capacité d'un utilisateur à changer de répertoires et exécuter des commandes. Le shell restreint est appelé avec la commande `/usr/lib/rsh`. Notez que le shell restreint n'est pas le shell distant, lequel est `/usr/sbin/rsh`.

Le shell restreint diffère d'un shell standard de l'une des manières suivantes :

- L'utilisateur est limité en accès à son répertoire d'accueil, de sorte qu'il ne peut pas utiliser la commande `cd` pour changer de répertoire. Par conséquent, l'utilisateur ne peut pas parcourir des fichiers système.
- L'utilisateur ne peut pas modifier la variable `PATH`. Il peut donc utiliser uniquement des commandes dans le chemin d'accès défini par l'administrateur système. L'utilisateur ne peut pas non plus exécuter de commandes ou de scripts à l'aide d'un nom de chemin d'accès complet.
- L'utilisateur ne peut pas rediriger la sortie avec > ou >>.

Le shell restreint vous permet de limiter la capacité d'un utilisateur à parcourir des fichiers système. Le shell crée un environnement restreint pour un utilisateur ayant besoin d'effectuer des tâches spécifiques. Cependant, le shell restreint n'est pas complètement sécurisé et il est uniquement destiné à empêcher des utilisateurs non qualifiés de causer des dommages par inadvertance.

Pour plus d'informations sur le shell restreint, utilisez la commande `man -s1m rsh` pour voir la page de manuel `rsh`(1M).

Restriction de l'accès aux données dans les fichiers

Etant donné qu'Oracle Solaris est un environnement multiutilisateur, la sécurité du système de fichiers constitue le risque de sécurité le plus élémentaire sur un ordinateur. Vous pouvez utiliser des protections de fichier UNIX conventionnelles pour protéger vos fichiers. Vous pouvez également utiliser des listes de contrôle d'accès (ACL) qui assurent une plus grande sécurité.

En règle générale, il est conseillé de ne permettre à certains utilisateurs que de lire des fichiers, tout en autorisant d'autres utilisateurs à modifier ou supprimer des fichiers. Il se peut que vous disposiez de données dont vous souhaitez qu'elles ne soient vues par personne d'autre. Chapitre 1, “ Contrôle de l’accès aux fichiers ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ” explique comment définir les autorisations sur les fichiers.

Restriction des fichiers exécutables `setuid`

Les fichiers exécutables peuvent présenter un risque pour la sécurité. Quelques programmes exécutables doivent être exécutés en tant que `root` pour fonctionner correctement. Ces programmes `setuid` s'exécutent lorsque l'ID utilisateur est défini sur `0`. Toute personne exécutant ces programmes les exécute avec l'ID `root`. Un programme s'exécutant avec l'ID `root` pose un problème de sécurité potentiel si le programme n'a pas été écrit en tenant compte des questions de sécurité.

A l'exception des exécutables fournis par Oracle Solaris avec le bit `setuid` défini sur `root`, vous devez désactiver l'utilisation des programmes `setuid`. Si vous ne pouvez pas interdire

l'utilisation des programmes `setuid`, vous devez restreindre leur utilisation. Une administration sécurisée requiert quelques programmes `setuid`.

Pour plus d'informations, reportez-vous à la section " Protection contre les problèmes de sécurité causés par les fichiers exécutables " du manuel " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 ". Les procédures sont décrites dans la section " Protection contre les programmes présentant des risques de sécurité " du manuel " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 ".

Utilisation de la configuration Secure by Default

Par défaut, lorsque Oracle Solaris est installé, un grand nombre de services réseau sont désactivés. Cette configuration est dite SDB, "sécurisée par défaut". Avec la configuration SBD, le seul service réseau acceptant les demandes réseau est le démon `sshd`. Tous les autres services réseau sont désactivés ou traitent uniquement des demandes locales. Pour activer des services réseau spécifiques, comme `ftp`, utilisez l'utilitaire SMF (gestion des services) d'Oracle Solaris. Pour plus d'informations, consultez les pages de manuel `netservices`(1M) et `smf`(5).

Utilisation des fonctions de gestion des ressources

Oracle Solaris dispose de fonctions évoluées de gestion des ressources. Ces fonctions vous permettent d'allouer, de planifier, de surveiller et de limiter l'utilisation des ressources par les applications dans un environnement de consolidation du serveur. La structure de contrôle des ressources vous permet de définir des contraintes sur les ressources du système utilisées par les processus. Ces contraintes aident à prévenir les attaques par déni de service effectuées par un script tentant d'envahir les ressources du système.

Avec les fonctions de gestion des ressources, vous pouvez désigner des ressources pour des projets particuliers. Vous pouvez également régler de façon dynamique les ressources disponibles. Pour plus d'informations, reportez-vous à la section " Administration de la gestion des ressources dans Oracle Solaris 11.2 "

Utilisation des zones Oracle Solaris

Les zones Oracle Solaris offrent un environnement d'exécution d'applications dans lequel les processus sont isolés du reste du système au sein d'une seule instance du Oracle Solaris (SE). Cela empêche les processus exécutés dans une zone de surveiller ou d'affecter les processus exécutés dans d'autres zones. Ainsi, même un processus exécuté avec des capacités de superutilisateur ne peut affecter l'activité des autres zones.

Les zones Oracle Solaris sont idéales pour les environnements qui regroupent plusieurs applications sur un serveur unique. Pour plus d'informations, reportez-vous à la section " Présentation d'Oracle Solaris Zones ".

Surveillance de l'utilisation des ressources de la machine

En tant qu'administrateur système, vous devez surveiller les activités du système. Vous devez connaître tous les aspects de vos machines, y compris les éléments suivants :

- Quelle est la charge normale ?
- Qui a accès au système ?
- Quand les individus accèdent-ils au système ?
- Quels programmes s'exécutent habituellement sur le système ?

Grâce à ce type d'informations, vous pouvez utiliser les outils disponibles pour auditer l'utilisation du système et surveiller les activités des utilisateurs individuels. La surveillance est très utile lorsqu'une violation de sécurité est suspectée. Pour plus d'informations sur le service d'audit, consultez le Chapitre 1, " A propos de l'audit dans OracleÂ Solaris " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".

Surveillance de l'intégrité des fichiers

En tant qu'administrateur système, vous devez vous assurer que les fichiers installés sur les systèmes que vous administrez n'ont pas subi de modifications inattendues. Dans les installations de grande taille, un outil de comparaison et de génération de rapports sur la pile de logiciels sur chacun de vos systèmes vous permet d'effectuer le suivi de vos systèmes. L'outil de génération de rapports d'audit de base (BART) permet de valider de manière exhaustive les systèmes en effectuant des vérifications d'un ou plusieurs systèmes dans le temps au niveau des fichiers. Les modifications apportées à un manifeste BART sur l'ensemble des systèmes ou pour un système au fil du temps peuvent valider l'intégrité de vos systèmes. BART assure la création et la comparaison de manifestes et fournit des règles pour les rapports d'écriture de script. Pour plus d'informations, reportez-vous au Chapitre 2, " Vérification de l'intégrité des fichiers à l'aide de l'utilitaire BART " du manuel " Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 11.2 ".

Contrôle de l'accès aux fichiers

Oracle Solaris est un environnement multiutilisateur dans lequel tous les utilisateurs connectés à un système peuvent lire des fichiers appartenant à d'autres utilisateurs. Les utilisateurs

disposant des autorisations de fichiers appropriées peuvent également utiliser des fichiers appartenant à d'autres utilisateurs. Pour plus d'informations, reportez-vous au Chapitre 1, “ Contrôle de l’accès aux fichiers ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ” Pour obtenir des instructions détaillées sur la définition des autorisations de fichiers appropriées, reportez-vous à la section “ Protection des fichiers ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”.

Chiffrement des fichiers sur le disque

Vous pouvez assurer la sécurité d'un fichier en le rendant inaccessible aux autres utilisateurs. Par exemple, un fichier avec des autorisations de `600` ne peut être lu que par son propriétaire et le compte `root`. Un répertoire disposant d'autorisations de `700` est également inaccessible. Cependant, quiconque devine votre mot de passe ou découvre le mot de passe `root` peut accéder à ce fichier. De même, un fichier inaccessible autrement est conservé sur une bande de sauvegarde chaque fois que les fichiers système sont sauvegardés sur un média hors ligne. Pour ajouter un niveau de protection supplémentaire, vous pouvez utiliser le chiffrement sur disque ou utilisez Commande de la structure cryptographique.

Pour plus d'informations sur les systèmes de fichiers ZFS File Systems, reportez-vous à la section “ Chiffrement des systèmes de fichiers ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.

La structure cryptographique permet de disposer des commandes `digest`, `mac` et `encrypt`. Les utilisateurs standard peuvent utiliser ces commandes pour protéger les fichiers et les répertoires. Pour plus d'informations, reportez-vous au Chapitre 1, “ Structure cryptographique ” du manuel “ Gestion du chiffrement et des certificats dans Oracle Solaris 11.2 ”.

Utilisation des listes de contrôle d'accès

Les listes de contrôle d'accès (ACL), qui se prononce "ackkls" en anglais, peuvent offrir un plus grand contrôle sur les autorisations de fichier. Vous ajoutez des ACL lorsque les protections de fichier UNIX conventionnelles ne sont pas suffisantes. Les protections de fichier UNIX conventionnelles fournissent des autorisations de lecture, d'écriture et d'exécution pour les trois classes d'utilisateur : propriétaire, groupe et autre. Une ACL permet d'affiner la sécurité des fichiers.

Les ACL vous permettent de définir des autorisations de fichier précises, notamment :

- Autorisations de fichier de propriétaire
- Autorisations de fichier pour le groupe du propriétaire
- Autorisations de fichier pour d'autres utilisateurs n'appartenant pas au groupe du propriétaire

- Autorisations de fichier pour des utilisateurs spécifiques
- Autorisations de fichier pour des groupes spécifiques
- Autorisations par défaut pour chacune des catégories précédentes

Pour protéger les fichiers ZFS avec des listes de contrôle d'accès (ACL), reportez-vous auChapitre 7, “ Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”. Pour plus d'informations sur l'utilisation des listes ACL sur les systèmes de fichiers hérités, reportez-vous à la section “ Utilisation des ACL pour protéger les fichiers UFS ” du manuel “ Sécurisation des fichiers et vérification de l’intégrité des fichiers dans Oracle Solaris 11.2 ”.

Partage de fichiers entre des machines

Sur un serveur de fichiers réseau, il est possible de contrôler les fichiers disponibles en partage. Un serveur de fichiers réseau peut également déterminer quels clients ont accès aux fichiers et quel type d'accès est autorisé pour ces clients. En général, le serveur de fichiers peut accorder un accès en lecture-écriture ou un accès en lecture seule à tous les clients ou à des clients spécifiques. Le contrôle d'accès est spécifié lorsque des ressources sont mises à disposition à l'aide de la commande `share`.

Lorsque vous créez un partage NFS d'un système de fichiers ZFS, le système de fichiers est partagé définitivement jusqu'à ce que vous supprimiez le partage. SMF gère automatiquement le partage lorsque le système est redémarré. Pour plus d'informations, reportez-vous à la section “ Différences entre les systèmes de fichiers Oracle Solaris ZFS et classiques ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.

Restriction de l'accès `root` aux fichiers partagés

En général, le superutilisateur ne dispose pas d'un accès `root` aux systèmes de fichiers partagés sur le réseau. Le système NFS empêche l'accès `root` aux systèmes de fichiers montés en modifiant le type d'utilisateur du demandeur en utilisateur `nobody` avec l'ID utilisateur `60001`. Les droits d'accès de l'utilisateur `nobody` sont identiques à ceux donnés à public. L'utilisateur `nobody` dispose des droits d'accès d'un utilisateur sans informations d'identification. Par exemple, si public ne dispose que d'une autorisation d'exécution pour un fichier, l'utilisateur `nobody` peut uniquement exécuter ce fichier.

Un serveur NFS peut accorder l'accès `root` à un système de fichiers partagé en fonction de l'hôte. Pour accorder ces privilèges, utilisez l'option `root=`*hostname* avec la commande `share`. Vous devez utiliser cette option avec précaution. Pour une description des options de sécurité avec NFS, reportez-vous au Chapitre 5, “ Commandes de gestion des systèmes de fichiers NFS ” du manuel “ Gestion des systèmes de fichiers réseau dans Oracle Solaris 11.2 ”.

Contrôle de l'accès réseau

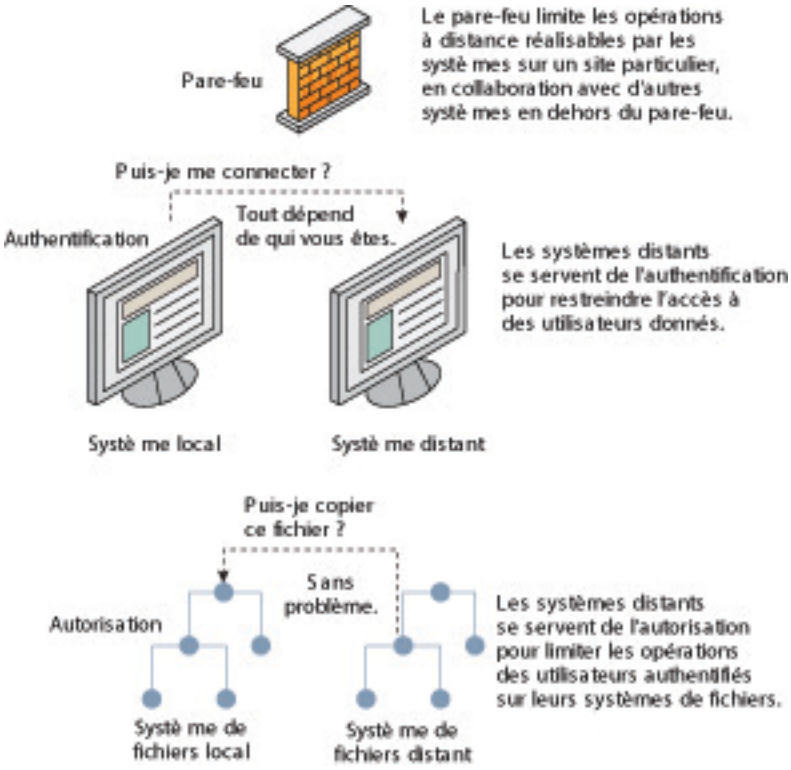
Les ordinateurs font souvent partie d'un réseau d'ordinateurs qui permet aux ordinateurs connectés d'échanger des informations. Les ordinateurs en réseau peuvent accéder aux données et à des ressources sur d'autres ordinateurs du réseau. Bien que les réseaux d'ordinateurs créent un environnement informatique puissant et sophistiqué compliquez, les réseaux également la sécurité informatique.

Par exemple, au sein d'un réseau d'ordinateurs, des systèmes individuels permettent de partager des informations. Les accès non autorisés représentent un risque pour la sécurité. Dans la mesure où un grand nombre de personnes ont accès à un réseau, la probabilité d'accès non autorisé est accrue, en particulier suite à une erreur d'utilisateur. Une utilisation inappropriée des mots de passe peut également conduire à des accès non autorisés.

Mécanismes de sécurité réseau

La sécurité réseau repose généralement sur la restriction ou le blocage d'opérations à partir de systèmes distants. La figure ci-après décrit les restrictions de sécurité que vous pouvez imposer sur les opérations à distance.

FIGURE 1-1 Restrictions de sécurité sur les opérations à distance



Authentification et autorisation pour l'accès à distance

L'*authentification* est un moyen de contrôler l'accès lorsque l'utilisateur tente d'accéder à un système distant. L'authentification peut être configurée à la fois au niveau du système et au niveau du réseau. Une fois qu'un utilisateur a obtenu l'accès à un système distant, l'*autorisation* constitue un moyen de restreindre les opérations pouvant être réalisées par l'utilisateur. Le tableau ci-dessous répertorie les services assurant l'authentification et l'autorisation.

TABLEAU 1-3 Services d'authentification pour l'accès à distance

service	Description	Pour en savoir plus
IPsec	IPsec propose une authentification par certificat basée sur les hôtes et le chiffrement du trafic réseau.	Chapitre 6, “ A propos de l’architecture de sécurité IP ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”
Kerberos	Kerberos utilise le chiffrement pour authentifier et autoriser un utilisateur se connectant au système.	Pour obtenir un exemple, reportez-vous à la section “ Fonctionnement du service Kerberos ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”.
LDAP	Le service d'annuaire LDAP peut fournir à la fois l'authentification et l'autorisation au niveau du réseau.	“ Utilisation des services de noms et d’annuaire Oracle Solaris 11.2 : DNS et NIS ”
Commandes de connexion à distance	Les commandes de connexion à distance permettent aux utilisateurs de se connecter à un système distant via le réseau et d'utiliser ses ressources. `rlogin`, `rcp` et `ftp` sont des exemples de commandes de connexion à distance. Si vous êtes un "hôte de confiance", l'authentification est automatique. Sinon, vous êtes invité à vous authentifier.	Chapitre 3, “ Accès aux systèmes distants ” du manuel “ Gestion des systèmes distants dans Oracle Solaris 11.2 ”
SASL	La couche SASL (Simple Authentication and Security Layer) est une structure fournissant des services d'authentification et de sécurité facultatifs aux protocoles réseau. Des plug-ins vous permettent de choisir un protocole d'authentification approprié.	“ A propos de SASL ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”
RPC sécurisé	Le RPC sécurisé améliore la sécurité des environnements réseau en authentifiant des utilisateurs adressant des demandes sur des machines distantes. Vous pouvez utiliser un mécanisme d'authentification UNIX, DES ou Kerberos pour le RPC sécurisé.	“ A propos de RPC sécurisé ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”
	Le RPC sécurisé peut également être utilisé pour assurer une sécurité supplémentaire dans un environnement NFS. Un environnement NFS avec RPC sécurisé est appelé NFS sécurisé.	“ Services NFS et RPC sécurisé ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”
Secure Shell, shell sécurisé	Secure Shell, shell sécurisé chiffre le trafic réseau sur un réseau non sécurisé. Secure Shell, shell sécurisé assure l'authentification par le biais de mots de passe, de clés publiques, ou les deux.	“ Shell sécurisé (Présentation) ” du manuel “ Gestion de l’accès au shell sécurisé dans Oracle Solaris 11.2 ”

Le mécanisme de *ports privilégiés* de Oracle Solaris représente une alternative possible à Secure RPC. Un port privilégié reçoit un numéro de port inférieur à `1024`. Une fois qu'un système client a authentifié les informations d'identification du client, le client établit une connexion au serveur à l'aide du port privilégié. Le serveur vérifie ensuite les informations d'identification du client en examinant le numéro de port de la connexion.

Les clients n'exécutant pas le logiciel Oracle Solaris risquent de ne pas pouvoir communiquer en utilisant le port privilégié. Si les clients ne peuvent pas communiquer via le port, un message d'erreur similaire au suivant s'affiche :

```
“Weak Authentication
NFS request from unprivileged port”
```

Systèmes pare-feu

Vous pouvez configurer un pare-feu système pour protéger les ressources de votre réseau contre les accès externes. Un *système pare-feu* est un hôte sécurisé agissant comme une barrière entre votre réseau interne et les réseaux extérieurs. Le réseau interne traite tous les autres réseaux comme non fiables. Vous devez considérer cette configuration comme obligatoire entre votre réseau interne et les réseaux externes, tels que l'Internet, avec lesquels vous communiquez.

Un pare-feu se comporte comme une passerelle et comme une barrière. En tant que passerelle, il transmet des données entre les réseaux. En tant que barrière, il bloque le passage des données vers le réseau et en provenance de celui-ci. Un utilisateur sur le réseau interne doit se connecter au système de pare-feu pour accéder à des hôtes sur des réseaux distants. De même, un utilisateur sur un réseau extérieur doit d'abord se connecter au système pare-feu avant de se voir accorder l'accès à un hôte sur le réseau interne.

Il peut également être utile de configurer un pare-feu entre plusieurs réseaux internes. Par exemple, vous pouvez configurer un pare-feu ou un ordinateur passerelle sécurisé pour restreindre le transfert de paquets par adresse ou par protocole. Par exemple, vous pouvez autoriser des paquets pour le transfert de messages, mais pas pour la commande `ftp`.

En outre, tous les messages électroniques envoyés depuis le réseau interne sont d'abord envoyés au système pare-feu. Le pare-feu transfère ensuite le courrier à un hôte sur un réseau externe. Le système pare-feu reçoit également tout le courrier électronique entrant et distribue le courrier aux hôtes sur le réseau interne.

Attention - Même si vous strictes et rigides sécurité appliquées sur le pare-feu , si vous alors alléger la protection sur d'autres hôtes du réseau, un intrus capable de pénétrer dans votre système pare-feu peut ensuite accéder à tous les hôtes sur le réseau interne.

Un système de pare-feu ne doit pas comporter d'hôtes de confiance. Un *hôte de confiance* est un hôte à partir duquel un utilisateur peut se connecter sans devoir fournir de mot de passe. Un système pare-feu ne doit partager aucun de ses systèmes de fichiers, ni monter des systèmes de fichiers à partir d'autres serveurs.

IPsec et la fonction IP Filter d'Oracle Solaris peuvent fournir une protection par pare-feu. Pour plus d'informations sur la protection du trafic réseau, reportez-vous à “ Sécurisation du réseau dans Oracle Solaris 11.2 ”.

Chiffrement et systèmes pare-feu

Les utilisateurs non autorisés à partir de l'extérieur d'une réseau peuvent altérer ou détruire les données à capturer les paquets dans les paquets en fonction de leur n'atteignent leur destination et avant d'être des données arbitraires dans le contenu de l'injection avant d'envoyer les paquets à leur course initiale. Cette procédure est appelée *éclatement de paquets*.

Sur un réseau local, l'éclatement de paquets est impossible car ceux-ci atteignent tous les systèmes, y compris le serveur, en même temps. En revanche, la procédure est possible sur une passerelle. Vous devez donc vous assurer que toutes les passerelles du réseau sont protégées.

Les attaques les plus dangereuses affectent l'intégrité des données. De telles attaques impliquent la modification du contenu des paquets ou l'emprunt d'identité d'un utilisateur.

Mais d'autres attaques par déni de service peut s'agir d'effectuer l'écoute électronique ne compromettent pas l'intégrité des données ou usurper l'identité d'un utilisateur. Un système d'écoute électronique enregistre des conversations pour une rediffusion ultérieure. Bien que les attaques de ce type n'affectent pas l'intégrité des données, elles portent atteinte à leur confidentialité. Vous avez la possibilité de protéger la confidentialité des informations sensibles en chiffrant les données qui transitent sur le réseau.

- Pour chiffrer des opérations à distance via un réseau non sécurisé, reportez-vous au Chapitre 1, “ Utilisation du shell sécurisé (Tâches) ” du manuel “ Gestion de l’accès au shell sécurisé dans Oracle Solaris 11.2 ”.
- Pour chiffrer et authentifier des données sur un réseau reportez-vous au Chapitre 2, “ A propos du service Kerberos ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”.
- Pour chiffrer des datagrammes IP, reportez-vous au Chapitre 6, “ A propos de l’architecture de sécurité IP ” du manuel “ Sécurisation du réseau dans Oracle Solaris 11.2 ”.

Génération de rapports sur les problèmes de sécurité

Si vous suspectez une violation de sécurité majeure, vous pouvez contacter le Computer Emergency Response Team/Coordination Center (CERT/CC). CERT/CC est un projet financé par la Defense Advanced Research Projects Agency (DARPA) situé à l'Institut de génie logiciel de l'Université Carnegie Mellon. Cette agence peut vous aider à résoudre les problèmes de sécurité que vous rencontrez. Cette agence peut également vous diriger vers d'autres équipes de réponse aux urgences informatiques plus à même de répondre à vos besoins spécifiques. Pour des informations de contact, reportez-vous au site Web CERT/CC (http://www.cert.org/contact_cert/).

♦ ♦ ♦ CHAPITRE 2

Protection de l'intégrité des systèmes Oracle Solaris

Les systèmes Oracle Solaris peuvent être protégés contre les modules de noyau non autorisés, les applications de type cheval de Troie ou d'autres menaces chargées sur le système. Ce chapitre décrit les fonctions de sécurité d'Oracle Solaris qui assurent la protection contre ces menaces et préservent l'intégrité du système dans son ensemble. Ce chapitre comprend les sections suivantes :

Utilisation de Verified Boot

Dans Oracle Solaris, Verified Boot sécurise le processus d'initialisation d'un système. Cett fonctionnalité protège le système contre les menaces suivantes :

- Altération des modules de noyau
- Insertion ou substitution de programmes malveillants qui usurpent l'identité des modules de noyau légitimes, tels que des chevaux de Troie, des logiciels espion et des rootkits.
- Installation de modules de noyau tiers non autorisés

Les programmes malveillants peuvent transmettre des informations à des tiers, ainsi que modifier le comportement d'Oracle Solaris. Bien que les modules tiers soit généralement non malveillants, ils peuvent aller à l'encontre des stratégies qui contrôlent les modifications de site. Par conséquent, le système doit également être protégé contre l'installation non autorisée de ces modules.

Signatures Verified Boot et ELF

Dans Oracle Solaris, la vérification de l'initialisation est effectuée au moyen de signatures ou clés `elfsign`. Dans la configuration d'origine, les modules de noyau Oracle Solaris sont signés à l'aide de ces clés. En raison de leur format de fichier, ces modules sont également appelés des objets ELF. La signature est créée à l'aide des sommes de contrôle SHA-1 ou SHA-256 des enregistrements ELF sélectionnés dans un fichier d'objet. Les sommes de contrôle SHA-1 ou SHA-256 sont signées avec une paire de clés publique et privée RSA-2048. La clé publique est distribuée dans `/etc/certs`, tandis que la clé privée n'est pas distribuée.

Toutes les clés sont stockées dans l'**environnement de pré-initialisation**, qui est le logiciel ou le microprogramme qui s'exécute avant l'initialisation d'Oracle Solaris. Le microprogramme charge et initialise `platform/.../unix`.

L'environnement de pré - initialisation est différent pour chaque catégorie de systèmes. L'environnement de pré-initialisation pris en charge pour chaque catégorie est le suivant :

- Systèmes SPARC et x86 hérités : ces systèmes n'ont pas de fonctions de stockage en dehors du système de fichiers de sorte que les paramètres de configuration relatifs à la vérification d'initialisation sont stockés dans le système de fichiers lui-même. Plus précisément, les informations de configuration sont stockées dans `/etc/system`. Les clés sont stockées dans `/etc/certs/*SE` dans le système de fichiers root et l'archive d'initialisation.
- Systèmes SPARC avec prise en charge de la vérification de l'initialisation dans ILOM (Oracle Integrated Lights Out Manager) : les clés et les paramètres de configuration sont stockés dans Oracle ILOM.

  Oracle ILOM étant en dehors du système de fichiers du système d'exploitation, la configuration de l'initialisation vérifiée est protégée des modifications par les utilisateurs du système d'exploitation, y compris par ceux disposant des privilèges d'administrateur (root). Par conséquent, dans cette catégorie de système, Verified boot est plus sécurisée.

  Vous devez vous assurer que l'accès à Oracle ILOM est sécurisé pour empêcher les modifications non autorisées à la configuration de Verified Boot. Pour plus d'informations sur la sécurisation d'Oracle ILOM, reportez-vous à la documentation à l'adresse suivante http://www.oracle.com/goto/ILOM/docs.
- Séries SPARC M5, SPARC M6 et SPARC T5 : les paramètres de configuration sont stockés dans Oracle ILOM du système. Le microprogramme SPARC envoie les informations de configuration dans Oracle Solaris.

Séquence de vérification pendant l'initialisation système

Verified Boot automatise la vérification des signatures `elfsign` des modules de noyau d'Oracle Solaris. Avec verified boot, l'administrateur peut créer une chaîne de confiance

vérifiable dans le processus d'initialisation, à partir de la réinitialisation du système jusqu'à l'achèvement du processus d'initialisation.

Lors d'une initialisation du système, chaque bloc de code démarré dans le processus d'initialisation vérifie le bloc suivant qui doit être chargé. La séquence de vérification et de chargement se poursuit jusqu'à ce que le dernier module de noyau soit chargé.

Lorsqu'un cycle d'alimentation est effectué par la suite sur le système, une nouvelle séquence de vérification commence. L'administrateur peut également configurer Verified Boot afin d'effectuer l'action appropriée en cas d'échec de vérification.

Considérez le flux d'initialisation d'Oracle Solaris sur un système SPAR :

`Firmware -> Bootblock -> /platform/.../unix -> genunix ->` *other kernel modules*

Le microprogramme SPARC est installé en usine. La signature numérique du microprogramme peut également être mise à jour à l'aide de l'utilitaire `fwupdate`. Le microprogramme vérifie, puis charge le module `/platform/.../unix` d'Oracle Solaris, qui est le module Oracle Solaris initial. A son tour, le chargeur d''exécution du noyau Oracle Solaris, `krtld`, qui fait partie du module, vérifie et charge le module UNIX (`genunix`) générique et les modules suivants.

Stratégies relatives à Verified Boot

Deux stratégies permettent de gérer Verified Boot :

- La stratégie d'initialisation régit la vérification des modules UNIX et `genunix`. Ces modules sont les premiers à être chargés durant le processus d'initialisation.
- La stratégie de module détermine la vérification d'autres modules de noyau qui doivent être chargés après le module `genunix`.

Sur les systèmes SPARC et x86 hérités, les stratégies sont définies dans les variables `boot_policy` et `module_policy` du fichier `/etc/system`. Sur les systèmes SPARC avec prise en charge de l'initialisation vérifiée Oracle ILOM, `boot_policy` et `module_policy` sont des propriétés d'Oracle ILOM dans `/HOST`*x*`/verified_boot`, où *x* est le numéro du domaine physique (PDomain).

Les deux variables ou propriétés peuvent être configurées avec l'une des valeurs suivantes :

- `none` : aucune vérification d'initialisation n'est effectuée. Par défaut, `boot_policy` et `module_policy` ne n'étant pas configurées, Verified Boot est désactivée.
- `warning` : la signature `elfsign` de chaque module de noyau est vérifiée avant le chargement du module. En cas d'échec de la vérification sur un module, le module est tout de même chargé. Les écarts sont enregistrés dans la console système ou, s'il est disponible, dans le fichier journal du système. Par défaut, le journal est `/var/adm/messages`.
- `enforce` : la signature `elfsign` de chaque module de noyau est vérifiée avant le chargement du module. En cas d'échec de la vérification sur un module, le module n'est pas chargé. Les

écarts sont enregistrés dans la console système ou, s'il est disponible, dans le fichier journal du système. Par défaut, le journal est `/var/adm/messages`.

En plus de configurer les stratégies, vous pouvez également spécifier les certificats de clés publiques X.509 `elfsign` sur le système. Comme dans le cas des modules, vous spécifiez les certificats en utilisant une variable ou en définissant une propriété Oracle ILOM.

Sur les systèmes avec Oracle ILOM prenant en charge Verified Boot, un fichier de certificat d'initialisation Verified Boot, `/etc/certs/ORCLS11SE`, est fourni avec Oracle ILOM. Sur les systèmes SPARC et x86 hérités, le certificat est disponible sous la forme du fichier Oracle Solaris `/etc/certs/ORCLS11SE`.

Le certificat contient la clé publique RSA servant à vérifier les signatures `elfsign` dans les objets ELF. Toutefois, vous pouvez installer un certificat fournis par la société pour remplacer `/etc/certs/ORCLS11SE`. Tous les certificats sont chargés et gérés sur chaque domaine physique individuel.

Activation de Verified Boot

Par défaut, verified boot est désactivé sur les systèmes. Les procédures permettant d'activer la fonctionnalité varient en fonction de votre système. Pour activer cette fonction, utilisez la procédure décrite dans cette section qui correspond à votre système.

▼ SPARC: Activation de Verified Boot sur les systèmes SPARC avec prise en charge de Verified-Boot Oracle ILOM

Pour les systèmes SPARC avec prise en charge de Verified-Boot Oracle ILOM, les propriétés de Verified Boot se trouvent dans `/HOST`*x*`/verified_boot`, où *x* est le numéro du domaine physique, tel que `HOST0`, `HOST1`, etc.

Remarque - Certains systèmes SPARC ne comptent qu'un seul domaine physique, `/HOST`, alors que d'autres ont plusieurs domaines physiques. Cette procédure part du principe que vous utilisez un système doté de plusieurs domaines physiques et fait référence à un domaine physique en tant que `/HOST`*x*. Pour des fonctions de sécurité propres à votre système, reportez-vous au manuel relatif à la sécurité de votre système.

---

1. **(Facultatif) Déterminez si votre système prend en charge verified boot.**

```
# show /HOSTx/verified_boot
```

```
show: Invalid target /HOST/verified_boot
```

Vous pouvez utiliser `fwupdate` pour mettre à jour le microprogramme Oracle ILOM du système.

2. **En tant qu'administrateur, connectez-vous à l'interface utilisateur d'Oracle ILOM.**

```
% ssh root@ilom
```

Où *ilom* peut être l'adresse IP du processeur de service Oracle ILOM ou l'adresse IP du module de contrôle du châssis.

3. **Configuree les propriétés de Verified Boot.**

```
--> set /HOSTx/verified_boot/boot_policy=warning
--> set /HOSTx/verified_boot/module_policy=warning
```

Remarque - Indiquez `warning` ou `enforce` pour chaque propriété. Les propriétés peuvent avoir différentes configurations. Pour plus d'informations sur ces configurations de stratégies, reportez-vous à la section “Stratégies relatives à Verified Boot” à la page 33.

Si la stratégie d'initialisation est configurée avec `enforce` et si des écarts sont détectés dans les modules UNIX et `genunix`, le système ne s'initialise pas. Au lieu de cela, le système revient à OpenBoot PROM (OBP).

---

4. **Indiquez le certificat que vous souhaitez utiliser à la place du certificat qui est fourni par le système.**

```
--> load /HOSTx/verified_boot/cert -source ftp-location
```

Où *ftp-location* fait référence au serveur FTP et au nom du fichier où le certificat est stocké. *ftp-location* doit être au format URL `ftp://server/filename`.

5. **(Facultatif) Affichez la configuration de Verified Boot.**

```
--> show /HOSTx/verified_boot
/HOST0
Properties:
boot_policy = warning
module_policy = warning
cert = ftp://server/filename
```

▼ Activation de Verified Boot sur les systèmes SPARC et x86 hérités

Utilisez cette procédure si votre système ne peut pas stocker la configuration de la vérification d'initialisation en dehors du système de fichiers local du système.

Lorsque vous activez la vérification d'initialisation sur ce type de système, notez les points suivants :

- Les informations de configuration sont stockées dans le système de fichiers local et sont donc accessibles.
- Tout utilisateur doté de privilèges peut modifier la configuration.
- Vous pouvez modifier les paramètres de stratégie et il est possible de désactiver la vérification d'initialisation elle-même.
- Des clés supplémentaires peuvent être ajoutées et autoriser ainsi tout signataire `elfsign` de signer les modules d'objets.

1. **Modifiez le fichier `/etc/system`.**

   a. **Ajoutez et configurez les variables `boot_policy` et `module_policy`.**

      Par exemple, dans `/etc/system`, vous pouvez saisir ce qui suit (indiqué en caractères gras) :

      ```
      * Verified Boot settings: 1=none (default), 2=warning, 3=enforce
      set boot_policy=2
      set module_policy=2
      ```

      Indiquez le nombre correspondant à la configuration souhaitée pour chaque variable. Les variables peuvent avoir différentes configurations. Pour plus d'informations sur ces configurations de stratégies, reportez-vous à la section “Stratégies relatives à Verified Boot” à la page 33.

      Si la stratégie d'initialisation est configurée avec `enforce` et si des écarts sont détectés dans les modules UNIX et `genunix`, le système ne s'initialise pas. Au lieu de cela, le système revient à OpenBoot PROM (OBP).

   b. **Spécifiez une ou plusieurs certificats de clé `elfsign` X.509 pour la variable `verified_boot_certs`.**

      ```
      set verified_boot_certs="/etc/certs/THIRDPARTYSE"
      ```

      Où *THIRDPARTY* est le nom du fichier de certificat fourni par l'utilisateur.

2. **Mettez à jour le fichier `/etc/system` dans l'archive d'initialisation.**

   ```
   # bootadm update-archive
   ```

3. **(Facultatif) Affichez la configuration de Verified Boot.**

   a. **Montez l'archive.**

      - Pour les systèmes SPARC :

```
# mount -r -F hsfs /platform/sun4v/boot_archive /mnt
```

- Pour les systèmes x86 :

  ```
  # mount -r -F hsfs /platform/x86-type/boot_archive /mnt
  ```

  où *x86-type* est soit `i86pc` ou `amd64`.

b. Affichez la configuration de Verified Boot et les clés `elfsign`.

```
# gzcat /mnt/etc/system | egrep 'verified|policy'
# ls -l /etc/certs
```

Gestion des certificats sur les systèmes prenant en charge Verified-Boot Oracle ILOM

Cette procédure explique comment gérer les certificats Verified Boot du système.

1. **Pour remplacer le certificat préinstallé par un certificat fourni par l'utilisateur, tapez ce qui suit :**

   ```
   --> load /HOSTx/verified_boot/cert -source ftp://server/filename
   ```

2. **Pour enregistrer une copie du certificat actuel dans la source qui est fournie par l'utilisateur, tapez ce qui suit :**

   ```
   --> dump /HOSTx/verified_boot/cert -dest ftp://server/filename
   ```

3. **Pour supprimer les certificats installés par l'utilisateur et restaurer le certificat préinstallé du système, tapez ce qui suit :**

   ```
   --> reset /HOSTx/verified_boot/cert
   ```

Vérification manuelle de la signature `elfsign`

Verified Boot est un mécanisme automatique qui offre un moyen rapide et efficace pour garantir l'intégrité du processus d'initialisation. Cependant, vous pouvez toujours vérifier manuellement la signature d'un module de noyau.

- **Utilisez la syntaxe de commande `elfsign` comme suit :**

  ```
  $ elfsign verify -v kernel_module
  ```

Par exemple :

```
$ elfsign verify -v /kernel/misc/sparcv9/cardbus
elfsign: verification of /kernel/misc/sparcv9/cardbus passed.
format: rsa_sha1.
signer: O=Oracle Corporation, OU=Corporate Object Signing, \
               OU=Solaris Signed Execution, CN=Solaris 11
```

A propos du Module de plate-forme sécurisée (TPM)

Oracle ILOM (TPM) fait référence au périphérique ainsi qu'à l'implémentation au moyen de laquelle les informations de configuration chiffrées propres au système sont stockées. Les informations servent à mesurer les processus lors de l'initialisation du système. Oracle Solaris utilise TPM pour stocker les clés de chiffrement de manière sécurisée.

Les composants suivants implémentent TPM dans Oracle Solaris :

- Le pilote de périphérique TPM communique avec le périphérique TPM.
- La pile logicielle Trusted Computing Group (TCG), ou TTS, fonctionne en tant que canal de communication avec le périphérique TPM par le biais du démon `tcsd`.
- Les bibliothèques PKCS #11 mettent en oeuvre un jeton matériel ou un fournisseur qui utilise TPM pour générer des clés et effectuer des opérations sensibles. Le fournisseur protège tous les objets de données privées en les chiffrant à l'aide de clés ne pouvant être utilisées que dans le périphérique TPM. Les bibliothèques PKCS #11 sont implémentées conformément au standard suivant : Cryptoki (Cryptographic Token Interface, interface de jetons cryptographiques) pour la bibliothèque PKCS #11 de RSA Security Inc.
- La commande `tpmadm` est utilisée pour gérer les aspects liés à TPM à des fins de vérification du processus d'initialisation.

  Pour plus de détails, reportez-vous à la page de manuel `tpmadm`(1M).

Le propriétaire de la plate-forme doit initialiser TPM en définissant un mot de passe de propriétaire qui est utilisé pour autoriser les opérations requérant des privilèges. Le propriétaire de la plate-forme, également appelé propriétaire TPM, se différencie du superutilisateur traditionnel de deux manières :

- Pour accéder aux fonctions TPM, le privilège de processus n'est pas pris en compte. Les opérations requérant des privilèges nécessitent la connaissance du mot de passe du propriétaire quel que soit le niveau de privilège du processus d'appel.
- Le propriétaire TPM ne peut pas remplacer les contrôles d'accès pour les données protégées par les clés TPM. Le propriétaire peut effectivement détruire les données en réinitialisant le TPM. Toutefois, le propriétaire ne peut pas accéder aux données qui ont été chiffrées avec les clés TPM appartenant à d'autres utilisateurs.

Module de plate-forme sécurisée (TPM), ainsi que les autres mesures décrites dans ce guide, protège le système des accès non autorisés par des utilisateurs ou des applications.

Initialisation de TPM sur les systèmes Oracle Solaris

Cette section présente les procédures à suivre pour l'initialisation de TPM sur les systèmes Oracle Solaris. Les procédures sont différentes entre les systèmes x86 et SPARC. Toutefois, pour initialiser TPM, certaines conditions prérequises sont communes aux deux plates-formes.

- Le périphérique TPM `/dev/tpm` doit être installé sur le système.
- TPM doit utiliser la spécification du module de plate-forme sécurisée TCG version 1.2, également désignée sous la référence ISO/IEC 11889-1:2009. Reportez-vous à la spécification publié sur le site http://www.trustedcomputinggroup.org/resources/tpm_main_specification.
- Les packages TPM Oracle Solaris suivants doivent être installés :
  - Pilote du module de plateforme sécurisée (`driver/crypto/TPM`)
  - Logiciel s TrouSerS TCG `library/security/trousers`

  Pour installer ces packages, utilisez les commandes suivantes :

```
# pkg install driver/crypto/tpm
# pkg install library/security/trousers
```

▼ Vérification de la reconnaissance du périphérique TPM par le système d'exploitation

Utilisez cette procédure pour déterminer si Oracle Solaris reconnaît le périphérique TPM installé. Cette procédure s'applique aux systèmes x86 et SPARC.

- **Dans une fenêtre du terminal, exécutez la commande suivante :**

```
# prtconf -v |grep tpm
```

Si le périphérique TPM est reconnu, la commande génère une sortie similaire à la suivante :

```
# prtconf -v |grep tpm
tpm, instance #0
dev_path=/pci@0,0/isa@lf/tpm@0,fed40000:tpm
dev_link=/dev/tpm
```

Si aucune sortie n'est générée, le périphérique est peut-être désactivé. Pour plus d'informations sur l'activation de ce périphérique, reportez-vous à la section “Initialisation de TPM à

l'aide de l'interface Oracle ILOM" à la page 40 ou "Initialisation de TPM à l'aide du BIOS" à la page 41 en fonction de la plate-forme de votre système.

Remarque - Vous pouvez également utiliser la commande `ls` pour obtenir les mêmes informations. Toutefois, la sortie doit contenir moins d'informations que celles fournies par la syntaxe `prtconf`.

```
# ls -l /dev/tpm
lrwxrwxrwx  1 root root  44 May 22 2012 /dev/tpm ->
../devices/pci@0,0/isa@lf/tpm@0,fed40000:tpm
```

SPARC: Initialisation de TPM à l'aide de l'interface Oracle ILOM

Sur les systèmes SPARC, vous utilisez à la fois les interfaces Oracle ILOM et Oracle Solaris pour initialiser le TPM.

1. **A l'invite Oracle ILOM, mettez le système hors tension.**

   ```
   -> stop -f/SYS
   ```

2. **Activez TPM.**

   Activez TPM avec l'un des ensembles de commandes suivants en fonction du système SPARC.

   - Sur les serveurs des séries SPARC M5 et SPARC T5, utilisez la commande suivante :

     ```
     -> set /HOST/tpm mode=activated
     ```

   - Sur les serveurs de la série SPARC M5-32, utilisez la commande suivante :

     ```
     -> set /HOST#/tpm mode=activated
     ```

     où # correspond à un numéro d'instance, par exemple, `HOST0/tpm`.

   - Sur les serveurs SPARC T4, utilisez les commandes suivantes :

     ```
     -> set /HOST/tpm enable=true activate=true
     -> show /HOST/tpm
     ```

3. **A l'invite Oracle Solaris, initialisez TPM.**

   Avec l'initialisation de TPM, vous devenez propriétaire de TPM de sorte qu'il requiert que vous affectiez un mot de passe propriétaire, également appelé Code PIN propriétaire.

   ```
    # tpmadm init
   TPM Owner PIN:
   Confirm TPM Owner PIN
   ```

4. **Vérifiez l'état de TPM.**

```
 # tpmadm status
TPM Version: 1.2 (ATML Rev: 13.9, SpecLevel: 2, ErrataRev: 1)
TPM resources
Contexts: 16/16 available
Sessions: 2/3 available
Auth Sessions: 2/3 available
Loaded Keys: 18/21 available
Platform Configuration Registers (24)
PCR 0: E1 EE 40 D8 66 28 A9 08 B6 22 8E AF DC 3C BC 23 71 15 49 31
PCR 1: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 2: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 3: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 4: AF 98 77 B8 72 82 94 7D BE 09 25 10 2E 60 F9 60 80 1E E6 7C
PCR 5: E1 AA 8C DF 53 A4 23 BF DB 2F 4F 0F F2 90 A5 45 21 D8 BF 27
PCR 6: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 7: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 17: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 18: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 19: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 21: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 22: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

5. **(Facultatif) Activez le fournisseur de chiffrement TPM.**

Remarque - Le fournisseur de chiffrement TPM est plus lent que Oracle Solaris. Effectuez cette étape uniquement si vous souhaitez que TPM effectue les opérations de chiffrement.

```
# cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
# cryptoadm list -mv provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
```

▼ x86: Initialisation de TPM à l'aide du BIOS

Sur les systèmes x86, vous exécutez les étapes sur le BIOS du système avant l'initialisation du service à l'aide d'Oracle Solaris.

1. **A l'invite d'Oracle Solaris, réinitialisez le système.**

```
# reboot -p
```

2. **Lors de l'initialisation du système, appuyez sur F2 pour accéder au menu BIOS.**

3. **A l'aide des options du menu BIOS, configurez TPM.**

   a. **Accédez à l'écran Advanced -> Trusted Computing.**

   b. **Configurez TPM en spécifiant des valeurs pour les options de menu suivantes.**

      ```
      TCG/TPM Support [Yes]
      Execute TPM Command [Enabled]
      ```

   c. **Appuyez sur la touche Echap pour quitter le menu du BIOS.**

   d. **Cliquez sur Save Changes et Exit.**

   e. **Pour poursuivre le processus d'initialisation, choisissez OK.**

4. **Une fois l'initialisation terminée, activez le démon `tcsd`.**

   ```
   # svcadm enable -s svc:/application/security/tcsd
   ```

5. **Initialisez TPM.**

   Avec l'initialisation de TPM, vous devenez propriétaire de TPM de sorte qu'il requiert que vous affectiez un mot de passe du propriétaire.

   ```
   # tpmadm init
   TPM Owner PIN:
   Confirm TPM Owner PIN
   ```

6. **Vérifiez l'état de TPM.**

   ```
    # tpmadm status
   TPM Version: 1.2 (ATML Rev: 13.9, SpecLevel: 2, ErrataRev: 1)
   TPM resources
   Contexts: 16/16 available
   Sessions: 2/3 available
   Auth Sessions: 2/3 available
   Loaded Keys: 18/21 available
   Platform Configuration Registers (24)
   PCR 0: E1 EE 40 D8 66 28 A9 08 B6 22 8E AF DC 3C BC 23 71 15 49 31
   PCR 1: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 2: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 3: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   PCR 4: AF 98 77 B8 72 82 94 7D BE 09 25 10 2E 60 F9 60 80 1E E6 7C
   PCR 5: E1 AA 8C DF 53 A4 23 BF DB 2F 4F 0F F2 90 A5 45 21 D8 BF 27
   PCR 6: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
   ```

```
PCR 7: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR 8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR 17: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 18: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 19: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 21: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 22: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
PCR 23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

7. (Facultatif) Activez le fournisseur de chiffrement TPM.

Remarque - Le fournisseur de chiffrement TPM est plus lent que Oracle Solaris. Par conséquent, effectuez cette étape uniquement si vous souhaitez que TPM effectue les opérations de chiffrement.

```
# cryptoadm install provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
# cryptoadm list -mv provider='/usr/lib/security/$ISA/pkcs11_tpm.so'
```

▼ Autorisation de l'utilisation de TPM en tant que keystore sécurisé par les clients PKCS #11

Avant de commencer Pour effectuer cette procédure, vous devez installer et activer TPM sur le système. Assurez-vous que le démon `tcsd` est aussi en cours d'exécution.

1. Vérifiez que le périphérique TPM est installé.

```
# ls -alF /dev/tpm
lrwxrwxrwx 1 root 39 Dec 27 2011 /dev/tpm -> ../devices/pci@0,0/isa@1/tpm@1,1670:tpm
```

2. Activez le démon `tcsd`.

```
# svcadm enable tcsd
```

3. Initialisez la zone personnelle de stockage de jeton protégée par TPM.

```
$ pktool inittoken currlabel=TPM
```

Remarque - Tous les utilisateurs individuels doivent effectuer cette étape.

4. **Définissez le code PIN de jeton pour l'agent de sécurité.**

```
$ pktool setpin token=tmp/TPM so
```

5. **Définissez le code PIN de l'utilisateur.**

```
$ pktool setpin token=tmp/TPM
```

6. **Générez des clés et certificats qui utilisent le périphérique TPM en spécifiant le nom de jeton que vous avez utilisé lors de l'initialisation du jeton.**

```
$ pktool gencert token=tpm/TPM -i
$ pktool list token=tpm/TPM
```

Les applications existantes qui utilisent déjà toute la structure cryptographique en jetonlibpkcs11 pouvez utiliser la leurs opérations TPM en la transformant en un pour sélectionner le périphérique jeton les applications pour les sessions TPM.

Exemple 2-1 L'activation de consommateurs de ressources {ENT à utiliser : TPM PK11}

Dans cet exemple, le jeton est d'abord affectées TPM un nouveau nom. Par la suite, sur le jeton par la suite, toutes les actions qu'elles utilisent le nouveau nom.

```
$ pktool inittoken currlable=TPM newlabel=JohnDoeTPM
$ pktool setpin token=tmp/JohnDoeTPM so
$ pktool gencert token=tpm/JohnDoeTPM -i
$ pktool list token=tpm/JohnDoeTPM
```

Dépannage de TPM

Utilisez les commandes décrites dans cette section pour surveiller les composants qui vous permettent de différents systèmes d'exploitation soit utilisé correctement et de résoudre les problèmes liés à des problèmes TPM.

- Vérifiez que le démon `tcsd` est en cours d'exécution.

```
# svcs tcsd
STATE      STIME      FMRI
online     Nov_07     svc:/application/security/tcsd:default
```

- Pour vous assurer que le périphérique TPM est installé, procédez comme suit :

```
# ls -alF /dev/tpm
lrwxrwxrwx 1 root 39 Dec 27 2011 /dev/tpm -> ../devices/pci@0,0/isa@1/tpm@1,1670:tpm
```

- TSS software, any programs installed on the pour vérifier que le package est installé, procédez comme suit :

```
# pkg info trousers
Name: library/security/trousers
Summary: TrouSerS TCG software to access a TPM device
Description: The TrouSerS library provides a software stack from the
Trusted Computer Group (TCG) that accesses a Trusted Platform Module
(TPM) hardware device.
Category: System/Security
State: Installed
Publisher: solaris
Version: 0.3.6
Build Release: 5.11
Branch: 0.175.1.0.0.24.0
Packaging Date: September 4, 2012 05:28:21 PM
Size: 3.65 MB
FMRI: pkg://solaris/library/security/
trousers@0.3.6,5.11-0.175.1.0.0.24.0:20120904T1728212
```

- Pour effacer TPM tant qu'exigence après TPM a déjà été réinitialisée.
  - A l'invite d'Oracle Solaris :

    ```
    # tpmadm clear owner
    ```

  - A l'invite d'Oracle ILOM :

    ```
    -> stop /SYS
    -> set /HOST/tpm forceclear=true
    -> start /SYS
    ```

♦ ♦ ♦ CHAPITRE 3

Contrôle de l'accès aux systèmes

Ce chapitre décrit les procédures de contrôle des utilisateurs qui peuvent accéder aux systèmes Oracle Solaris.

Ce chapitre comprend les sections suivantes :

Pour des informations générales sur la sécurité du système, reportez-vous au Chapitre 1, Gestion de la sécurité des machines.

Sécurisation des connexions et des mots de passe

Pour protéger l'accès à votre système, vous pouvez limiter les connexions à distance, exiger que les utilisateurs aient des mots de passe et que le compte `root` ait un mot de passe complexe. Vous pouvez également afficher un message de sécurité aux utilisateurs, contrôler les tentatives d'accès ayant échoué et désactiver temporairement les connexions.

La liste des tâches suivante présente les procédures permettant de contrôler et de désactiver les connexions utilisateur.

TABLEAU 3-1 Sécurisation des connexions et des mots de passe (Liste des tâches)

Tâche	Description	Pour obtenir des instructions
Affichage d'informations relatives à la sécurité du site lors de la connexion des utilisateurs.	Affiche un message texte sur l'écran de connexion contenant des informations sur la sécurité du site.	“ Placement d’un message de sécurité dans les fichiers bannière ” du manuel “ Directives de sécurité d’Oracle Solaris 11 ” “ Placement d’un message de sécurité dans l’écran de connexion au bureau ” du manuel “ Directives de sécurité d’Oracle Solaris 11 ”

Tâche	Description	Pour obtenir des instructions
Affichage de l'état de connexion d'un utilisateur.	Répertorie des informations complètes sur le compte de connexion d'un utilisateur, telles que le nom complet et le vieillissement du mot de passe.	“Affichage de l'état de connexion d'un utilisateur” à la page 48
Recherche d'utilisateurs qui n'ont pas de mot de passe.	Recherche uniquement les utilisateurs dont les comptes n'ont pas besoin d'un mot de passe.	“Affichage des utilisateurs sans mots de passe” à la page 49
Désactivation temporaire des connexions.	Refuse les connexions utilisateur à une machine pendant la fermeture du système ou la maintenance de routine.	“Désactivation temporaire des connexions utilisateur” à la page 50

▼ Affichage de l'état de connexion d'un utilisateur

Avant de commencer

Pour utiliser la commande `logins`, vous devez vous connecter en tant qu'administrateur auquel est affecté le profil de droits User Management (Gestion des utilisateurs) ou User Security (Sécurité des utilisateurs). Par défaut, le rôle `root` dispose de cette autorisation. Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

- **Pour afficher l'état de connexion d'un utilisateur, utilisez la commande `logins`.**

```
# logins -x -l username
```

`-x` Affiche un ensemble étendu d'informations sur l'état de connexion.

`-l` *username* Affiche l'état de connexion pour l'utilisateur spécifié. La variable *username* est le nom de connexion d'un utilisateur. Les noms de connexion multiples sont séparés par des virgules.

La commande `logins` utilise la base de données de mots de passe appropriée pour obtenir l'état de connexion d'un utilisateur. La base de données peut être le fichier `/etc/passwd` local ou une base de données de mots de passe pour le service de noms. Pour plus d'informations, reportez-vous à la page de manuel `logins`(1M) man page.

Exemple 3-1 Affichage de l'état de connexion d'un utilisateur

Dans l'exemple suivant, l'état de connexion de l'utilisateur `jdoe` s'affiche.

```
# logins -x -l jdoe
jdoe       500     staff          10   Jaylee Jaye Doe
/home/jdoe
```

```
/bin/bash
PS 010103 10 7 -1
```

`jdoe`	Identifie le nom de connexion de l'utilisateur.
`500`	Identifie l'ID utilisateur (UID).
`staff`	Identifie le groupe principal de l'utilisateur.
`10`	Identifie l'ID de groupe (GID).
Jaylee Jaye Doe	Identifie le commentaire.
`/home/jdoe`	Identifie le répertoire d'accueil de l'utilisateur.
`/bin/bash`	Identifie le shell de connexion.
`PS 010170 10 7 -1`	Spécifie les informations de vieillissement du mot de passe : ■ Date à laquelle le mot de passe a été modifié pour la dernière fois ■ Nombre de jours qui sont requis entre les modifications ■ Nombre de jours avant qu'une modification ne soit requise ■ Période d'avertissement

▼ Affichage des utilisateurs sans mots de passe

Avant de commencer

Pour utiliser la commande `logins`, vous devez vous connecter en tant qu'administrateur auquel est affecté le profil de droits User Management (Gestion des utilisateurs) ou User Security (Sécurité des utilisateurs). Par défaut, le rôle `root` dispose de cette autorisation. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

- **Pour afficher tous les utilisateurs ne disposant pas de mot de passe, utilisez la commande `logins`.**

```
# logins -p
```

L'option `-p` affiche la liste des utilisateurs dépourvus de mot de passe. La commande `logins` utilise la base de données `passwd` du système local sauf si un service de noms distribué est spécifié dans la propriété `password` du service `system/name-service/switch`.

Exemple 3-2 Affichage des comptes sans mot de passe

Dans l'exemple suivant, l'utilisateur `pmorph` et le rôle `roletop` ne possèdent pas de mot de passe.

```
# logins -p
pmorph          501     other           1       Polly Morph
roletop         211     admin           1       Role Top
#
```

Désactivation temporaire des connexions utilisateur

Désactivez temporairement les connexions utilisateur pendant l'arrêt du système ou de la maintenance de routine.

Remarque - Cette procédure n'a aucune répercussion sur tous les utilisateurs. Les utilisateurs suivants peuvent continuer à se connecter au système malgré la présence du fichier `/etc/nologin` créé par cette procédure.

- Superutilisateur
- Les utilisateurs qui ont reçu le rôle root
- Les utilisateurs ayant reçu l'autorisation `solaris.system.maintenance`

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

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant de l'autorisation `solaris.admin.edit/etc/nologin` authorization. Par défaut, le rôle `root` dispose de cette autorisation. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Créez le fichier `/etc/nologin` dans un éditeur de texte.**

   ```
   # pfedit /etc/nologin
   ```

   Pour obtenir un exemple d'utilisation de l'autorisation `solaris.admin.edit/etc/nologin`, reportez-vous à l'Exemple 3-3, "Désactivation des connexions utilisateur".

2. **Incluez un message sur la disponibilité du système.**

3. **Fermez et enregistrez le fichier.**

Exemple 3-3 Désactivation des connexions utilisateur

Dans cet exemple, un utilisateur est autorisé à écrire la notification de l'indisponibilité du système.

```
% pfedit /etc/nologin
***No logins permitted.***

***The system will be unavailable until 12 noon.***
```

Modification de l'algorithme par défaut pour le chiffrement de mot de passe

Pour utiliser un autre algorithme de chiffrement des mots de passe, modifiez le fichier `/etc/security/policy.conf`. Par défaut, les mots de passe utilisateur sont chiffrés avec l'algorithme `crypt_sha256`. L'algorithme est représenté par l'identificateur `5` affecté au paramètre `CRYPT_DEFAULT` dans le fichier. Pour basculer vers un autre identifiant algorithme, d'affecter une autre. Pour obtenir une liste des algorithmes de chiffrement de mots de passe et de leurs identificateurs, reportez-vous au Tableau 1-1, “Algorithmes de chiffrement de mot de passe”.

Remarque - Lorsque cela est possible, utilisez des algorithmes certifiés FIPS. Reportez-vous à la section “ FIPS 140 Algorithm Lists and Certificate References for Oracle Solaris Systems ” du manuel “ Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ” pour obtenir des listes d'algorithmes certifiés FIPS et d'algorithmes non certifiés.

Notez que le nouvel algorithme s'applique uniquement aux de chiffrement de mot de passe pour les nouveaux utilisateurs. Pour les utilisateurs existants, l'algorithme précédent reste opérationnel s'il reste défini dans le paramètre `CRYPT_ALGORITHMS_ALLOW` et n'est pas `unix`. Pour voir la façon dont le chiffrement est implémenté dans ce cas, reportez-vous à la section “Configuration des algorithmes dans le fichier `policy.conf`” à la page 14. Pour inclure les utilisateurs existants sous le nouvel algorithme de chiffrement des mots de passe, supprimez l'algorithme précédent du paramètre `CRYPT_ALGORITHMS_ALLOW` également.

Pour plus d'informations sur la configuration des sélections d'algorithme, reportez-vous à la page de manuel `policy.conf`(4).

▼ Spécification d'un algorithme de chiffrement de mot de passe

Avant de commencer

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

1. **Dans le fichier `/etc/security/polic.conf`, spécifiez l'identifiant de l'algorithme de chiffrement, sous forme de valeur de la variable `CRYPT_DEFAULT`.**

2. **(Facultatif) Ajouter un commentaire sur la suppression des fichier afin d'expliquer votre choix.**

   Par exemple :

   ```
   # cat  /etc/security/policy.conf
   …
   # Sets the SHA256 (5) algorithm as default.
   # SHA256 supports 255-character passwords.
   # Passwords previously encrypted with MD5 (1) will be encrypted
   # with SHA256 (5) when users change their passwords.
   #CRYPT_DEFAULT=1
   CRYPT_DEFAULT=5
   ```

   Dans cet exemple, la nouvelle valeur de `CRYPT_DEFAULT` est `5`, ce qui correspond à `SHA256`, l'algorithme SHA256. SHA est l'acronyme de Secure Hash Algorithm (algorithme de hachage sécurisé). Cet algorithme est un membre de la famille SHA-2. SHA256 prend en charge des mots de passe à 255 caractères.

3. **(Facultatif) Supprimez l'algorithme précédent de `CRYPT_ALGORITHM_ALLOWED` pour que le nouvel algorithme s'applique également aux utilisateurs existants.**

   Par exemple, pour vous assurer que l'algorithme SHA256 s'applique également aux utilisateurs existants, `CRYPT_ALGORITHM_ALLOWED` doit exclure l'identificateur prédédent pour MD5, `1`.

   Remarque - En outre, pour promouvoir la sécurité FIPS 140, excluez l'algorithme Blowfish (2a) de l'entrée.

   ```
   CRYPT_ALGORITHMS_ALLOW=5,6
   ```

Exemple 3-4 Contrainte des algorithmes de chiffrement de mot de passe dans un environnement hétérogène

Dans cet exemple, l'administrateur sur un réseau qui inclut les systèmes BSD et Linux configure les mots de passe de sorte qu'ils soient utilisables sur tous les systèmes. Etant donné que certaines applications de réseau ne peuvent pas gérer le chiffrement `SHA512`, l'administrateur n'inclut pas son identificateur dans la liste des algorithmes autorisés. L'administrateur conserve l'algorithme `SHA256`, `5`, en tant que valeur de la variable `CRYPT_DEFAULT`. La variable `CRYPT_ALGORITHMS_ALLOW` contient l'identificateur `MD5` qui est compatible avec les systèmes BSD et Linux et l'identificateur Blowfish qui est compatible avec les systèmes BSD. Etant donné que `5` est l'algorithme `CRYPT_DEFAULT`, il n'a pas besoin d'être répertorié dans la liste `CRYPT_ALGORITHMS_ALLOW`. Cependant, pour des raisons de maintenance, l'administrateur place `5` dans la liste `CRYPT_ALGORITHMS_ALLOW` et les identificateurs inutilisés dans la liste `CRYPT_ALGORITHMS_DEPRECATE`.

```
CRYPT_ALGORITHMS_ALLOW=1,2a,5
```

```
#CRYPT_ALGORITHMS_DEPRECATE=__unix__,md5,6
CRYPT_DEFAULT=5
```

Spécification d'un nouvel algorithme de mot de passe pour un domaine NIS

Lorsque les utilisateurs dans un domaine NIS modifient leurs mots de passe, le client NIS consulte sa configuration locale des algorithmes dans le fichier `/etc/security/policy.conf`. Le système client NIS chiffre le mot de passe.

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

1. **Spécifiez l'algorithme de chiffrement de mot de passe dans le fichier `/etc/security/policy.conf` du client NIS.**
2. **Copiez le fichier `/etc/security/policy.conf` modifié sur chaque système client dans le domaine NIS.**
3. **Pour éviter toute confusion, copiez le fichier `/etc/security/policy.conf` modifié sur le serveur root NIS et les serveurs esclaves.**

Spécification d'un nouvel algorithme de mot de passe pour un domaine LDAP

Lorsque le client LDAP est configuré correctement, le client LDAP peut utiliser les nouveaux algorithmes de mot de passe. Le client LDAP se comporte exactement comme un client NIS.

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

1. **Spécifiez un algorithme de chiffrement de mot de passe dans le fichier `/etc/security/policy.conf` du client LDAP.**
2. **Copiez le fichier `policy.conf` modifié pour chaque système client dans le domaine LDAP.**

3. **Assurez-vous que le fichier `/etc/pam.conf` du client n'utilise pas un module `pam_ldap`.**

   Assurez-vous qu'un signe de commentaire (#) précède les entrées incluant `pam_ldap.so.1`. En outre, n'utilisez pas l'option `server_policy` avec le module `pam_authtok_store.so.1`.

   Les entrées PAM du fichier `pam.conf` du client permettent de chiffrer le mot de passe en fonction de la configuration des algorithmes. Les entrées PAM permettent également l'authentification du mot de passe.

   Lorsque les utilisateurs du domaine LDAP modifient leurs mots de passe, le client LDAP consulte sa configuration locale des algorithmes dans le fichier `/etc/security/policy.conf`. Le système client LDAP chiffre le mot de passe. Ensuite, le client envoie le mot de passe chiffré, avec une balise `{crypt}`, pour le serveur. La balise indique au serveur que le mot de passe est déjà chiffré. Le mot de passe est ensuite stocké, tel quel, sur le serveur. Pour l'authentification, le client récupère le mot de passe stocké dans le serveur. Le client compare ensuite le mot de passe stocké avec la version chiffrée que le client vient de générer à partir du mot de passe saisi par l'utilisateur.

   Remarque - Pour tirer parti des commandes de stratégie de mot de passe sur le serveur LDAP, utilisez l'option `server_policy` avec les entrées `pam_authtok_store` dans le fichier `pam.conf`. Les mots de passe sont ensuite chiffrés sur le serveur LDAP. Pour plus d'informations sur cette procédure, reportez-vous au Chapitre 4, “ Configuration d’Oracle Directory Server Enterprise Edition avec les clients LDAP ” du manuel “ Utilisation des services de noms et d’annuaire Oracle Solaris 11.2 : LDAP ”.

Contrôle et restriction de l'accès `root`

Par défaut, le rôle `root` est affecté à l'utilisateur initial et ne peut se connecter directement au système local ou à distance à un système Oracle Solaris.

▼ Contrôle des utilisateurs de la commande `su`

Le fichier `sulog` répertorie chaque utilisation de la commande `su`, et pas seulement les tentatives `su` utilisées pour passer d'utilisateur à `root`.

La journalisation de `su` dans ce fichier est activée par défaut dans l'entrée suivante du fichier `/etc/default/su` :

```
SULOG=/var/adm/sulog
```

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

- **Contrôlez le contenu du fichier `/var/adm/sulog` de façon régulière.**

```
# more /var/adm/sulog
SU 12/20 16:26 + pts/0 stacey-root
SU 12/21 10:59 + pts/0 stacey-root
SU 01/12 11:11 + pts/0 root-rimmer
SU 01/12 14:56 + pts/0 jdoe-root
SU 01/12 14:57 + pts/0 jdoe-root
```

Les entrées affichent les informations suivantes :

- La date et l'heure de la saisie de la commande.
- Si la tentative a réussi. La présence d'un signe plus (+) indique une tentative réussie. Un signe moins (-) indique un échec.
- Le port à partir duquel la commande a été émise.
- Le nom de l'utilisateur et le nom de l'identité commutée.

Erreurs fréquentes Les entrées incluant `???` indiquent que le terminal de contrôle pour la commande `su` ne peut pas être identifié. Généralement, les appels système de la commande `su` avant l'affichage du bureau incluent `???`, comme dans `SU 10/10 08:08 + ??? root-root`. Une fois que l'utilisateur a lancé une session de bureau, la commande `ttynam` renvoie la valeur du terminal de contrôle à `sulog`: `SU 10/10 10:10 + pts/3 jdoe-root`.

Les entrées semblables à ce qui suit peuvent indiquer que la commande `su` n'a pas été appelée sur la ligne de commande : `SU 10/10 10:20 + ??? root-oracle`. Un utilisateur Trusted Extensions est peut-être passé au rôle `oracle` à l'aide d'une interface graphique.

▼ Restriction et contrôle des connexions `root`

Cette méthode détecte immédiatement les tentatives de `root` d'accéder au système local.

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

1. **Affichez l'entrée `CONSOLE` dans le fichier `/etc/default/login`.**

```
CONSOLE=/dev/console
```

Par défaut, le périphérique de console est défini sur `/dev/console`. Avec ce paramètre, `root` peut se connecter à la console. `root` ne peut pas se connecter à distance.

2. Vérifiez que root ne peut pas se connecter à distance.

A partir d'un système distant, essayez de vous connecter en tant que root.

```
mach2 % ssh -l root mach1
Password:      <Type root password of mach1>
Password:
Password:
Permission denied (gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive).
```

Dans la configuration par défaut, root correspond à un rôle et les rôles ne peuvent pas se connecter. De plus, dans la configuration par défaut, le protocole ssh empêche la connexion de l'utilisateur root.

3. Surveillez les tentatives de devenir root.

Par défaut, les tentatives de devenir root sont imprimées sur la console par l'utilitaire SYSLOG.

a. Ouvrez une console de terminal sur le bureau.

b. Dans une autre fenêtre, utilisez la commande su pour devenir l'utilisateur root.

```
% su -
Password:      <Type root password>
#
```

Un message est imprimé sur la console de terminal.

```
Sep 7 13:22:57 mach1 su: 'su root' succeeded for jdoe on /dev/pts/6
```

Exemple 3-5 Journalisation des tentatives d'accès root

Dans cet exemple, les tentatives root ne sont pas consignées par SYSLOG. Par conséquent, l'administrateur consigne ces tentatives en retirant le commentaire de l'entrée #CONSOLE=/dev/console dans le fichier /etc/default/su.

```
# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
CONSOLE=/dev/console
```

Lorsqu'un utilisateur tente de devenir l'utilisateur root, la tentative est imprimée sur la console de terminal.

```
SU 09/07 16:38 + pts/8 jdoe-root
```

Erreurs fréquentes Pour devenir l'utilisateur root à partir d'un système distant lorsque le fichier /etc/default/login contient l'entrée CONSOLE par défaut, les utilisateurs doivent préalablement se connecter

avec leur nom d'utilisateur. Après la connexion avec leur nom d'utilisateur, les utilisateurs peuvent utiliser la commande `su` pour devenir l'utilisateur `root`.

Si la console affiche une entrée similaire à `Last login: Wed Sep 7 15:13:11 2011 from mach2`, le système est configuré pour autoriser les connexions `root` à distance. Pour empêcher l'accès `root` à distance, remplacez l'entrée `#CONSOLE=/dev/console` par `CONSOLE=/dev/console` dans le fichier `/etc/default/login`. Pour rétablir la valeur par défaut du protocole `ssh`, reportez-vous à la page de manuel `sshd_config`(4).

Contrôle de l'accès au matériel du système

Vous pouvez protéger le système physique en exigeant un mot de passe pour accéder aux paramètres du matériel. Vous pouvez également protéger le système en empêchant un utilisateur d'utiliser la séquence d'abandon pour quitter le système de multifenêtrage.

Pour protéger le BIOS, consultez la documentation du fournisseur.

▼ Spécification d'un mot de passe obligatoire pour l'accès au matériel SPARC

Avant de commencer Vous devez vous connecter en tant qu'administrateur système disposant d'un des profil de droits Device Security (sécurité des périphériques), Maintenance and Repair (maintenance et réparations) ou System Administrator (administrateur système). Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Dans une fenêtre de terminal, activez le mode de sécurité de la PROM.**

```
# eeprom security-mode=command

Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

Choisissez la valeur `command` ou `full`. Pour de plus amples détails, reportez-vous à la page de manuel `eeprom`(1M).

Si, lorsque vous saisissez la commande ci-dessus, vous n'êtes pas invité à saisir un mot de passe PROM, le système dispose déjà d'un mot de passe PROM.

2. **(Facultatif) Modifiez le mot de passe d'accès à la PROM.**

Attention - N'oubliez pas le mot de passe de la PROM. Le matériel est inutilisable sans ce mot de passe.

```
# eeprom security-password=       Press Return
Changing PROM password:
New password:       <Type password>
Retype new password:       <Retype password>
```

Les nouveaux mode de sécurité et mot de passe de la PROM entrent en vigueur immédiatement. Cependant, ils sont plus susceptibles d'être pris en compte à la prochaine initialisation.

▼ Désactivation de la séquence d'abandon d'un système

Remarque - Certains systèmes de serveur sont dotés d'un commutateur à clé. Si le commutateur à clé est en position sécurisée, il remplace les paramètres d'abandon du clavier du logiciel. Par conséquent, toutes les modifications que vous apportez à l'aide de la procédure suivante peuvent ne pas être mises en oeuvre.

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant de l'autorisation `solaris.admin.edit/etc/default/kbd`. Par défaut, le rôle `root` dispose de cette autorisation. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Modifiez la valeur de `KEYBOARD_ABORT` en la définissant sur `disable`.**

   Mettez en commentaire la ligne `enable` dans le fichier `/etc/default/kbd`. Ensuite, ajoutez une ligne `disable` :

   ```
   # cat /etc/default/kbd
   …
   # KEYBOARD_ABORT affects the default behavior of the keyboard abort
   # sequence, see kbd(1) for details.  The default value is "enable".
   # The optional value is "disable".  Any other value is ignored.
   …
   #KEYBOARD_ABORT=enable
   KEYBOARD_ABORT=disable
   ```

2. **Mettez à jour les paramètres par défaut du clavier.**

   ```
   # kbd -i
   ```

♦ ♦ ♦ CHAPITRE 4

Contrôle de l'accès aux périphériques

Ce chapitre fournit des instructions étape par étape pour protéger les périphériques, en plus d'une section de référence. Ce chapitre comprend les sections suivantes :

Pour des informations générales sur la protection des périphériques, reportez-vous à la section “Contrôle de l'accès aux périphériques” à la page 16.

Configuration de la stratégie de périphériques

La stratégie de périphériques limite ou empêche l'accès aux périphériques faisant partie intégrante du système. La stratégie est appliquée dans le noyau.

La liste des tâches suivante présente les procédures de configuration des périphériques liées à la stratégie de périphériques.

TABLEAU 4-1 Configuration de la stratégie de périphériques (Liste des tâches)

Tâche	Description	Pour obtenir des instructions
Affichage de la stratégie pour les périphériques de votre système.	Dresse la liste des périphériques et des stratégies correspondantes.	“Affichage de la stratégie de périphériques” à la page 60
Audit des modifications apportées à la stratégie de périphériques.	Enregistre les modifications apportées à la stratégie de périphériques dans la piste d'audit.	“Audit des modifications apportées à la stratégie de périphériques” à la page 60
Accès à `/dev/arp`.	Récupère des informations d'Oracle Solaris IP MIB-II.	“Récupération d'informations IP MIB-II à partir d'un périphérique `/dev/*`” à la page 61

Affichage de la stratégie de périphériques

- **Affichez la stratégie pour tous les périphériques de votre système.**

```
% getdevpolicy | more
DEFAULT
read_priv_set=none
write_priv_set=none
ip:*
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
…
```

Exemple 4-1 Affichage de la stratégie pour un périphérique spécifique

Dans cet exemple, la stratégie pour trois périphériques est affichée.

```
% getdevpolicy /dev/allkmem /dev/ipsecesp /dev/bge
/dev/allkmem
read_priv_set=all
write_priv_set=all
/dev/ipsecesp
read_priv_set=sys_net_config
write_priv_set=sys_net_config
/dev/bge
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
```

Audit des modifications apportées à la stratégie de périphériques

Par défaut, la classe d'audit `as` inclut l'événement d'audit `AUE_MODDEVPLCY`.

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

- **Présélectionnez la classe d'audit incluant l'événement d'audit `AUE_MODDEVPLCY`.**

```
# auditconfig -getflags
current-flags
# auditconfig -setflags current-flags,as
```

Pour obtenir des instructions détaillées, reportez-vous à la section " Présélection des classes d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".

▼ Récupération d'informations IP MIB-II à partir d'un périphérique /dev/*

Les applications qui récupèrent des informations d'Oracle Solaris IP MIB-II doivent ouvrir /dev/arp et pas /dev/ip.

1. **Déterminez la stratégie de périphériques sur /dev/ip et /dev/arp.**

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
/dev/arp
read_priv_set=none
write_priv_set=none
```

Notez que le privilège net_rawaccess est requis pour la lecture et l'écriture sur /dev/ip. Aucun privilège n'est requis pour /dev/arp.

2. **Ouvrez /dev/arp et empilez les modules tcp et udp.**

Aucun privilège n'est requis. Cette méthode revient à ouvrir le fichier /dev/ip et à empiler les modules arp, tcp et udp. Etant donné que l'ouverture du fichier /dev/ip exige désormais un privilège, il est préférable d'utiliser la méthode du fichier /dev/arp.

Gestion de l'allocation de périphériques

L'allocation de périphériques est généralement implémentées sur des sites qui nécessitent un niveau supplémentaire de sécurité des périphériques. Généralement, les utilisateurs doivent avoir l'autorisation d'accéder aux périphériques allouables.

La liste des tâches suivante présente les procédures permettant d'activer, de configurer et de dépanner l'allocation de périphériques. L'allocation de périphériques n'est pas activée par défaut. Une fois l'allocation de périphériques activée, reportez-vous à la section “Allocation de périphériques” à la page 67 pour obtenir les instructions relatives à l'allocation des périphériques.

TABLEAU 4-2 Gestion de l'allocation des périphériques (liste des tâches)

Tâche	Description	Pour obtenir des instructions
Procédure pour rendre un	Permet d'allouer un périphérique à un utilisateur à la fois.	“Activation de l'allocation de périphériques” à la page 62

Tâche	Description	Pour obtenir des instructions
périphérique allouable. Désactivation de l'allocation de périphériques.	Supprime des restrictions d'allocation de tous les périphériques.	
Octroi de l'autorisation d'allouer un périphérique à des utilisateurs.	Attribue des autorisations d'allocation de périphériques aux utilisateurs.	“Autorisation des utilisateurs à allouer un périphérique” à la page 63
Affichage des périphériques allouables sur votre système.	Dresse la liste des périphériques allouables et de leur état.	“Affichage d'informations d'allocation sur un périphérique” à la page 64
Allocation forcée d'un périphérique.	Alloue un périphérique à un utilisateur ayant un besoin immédiat.	“Allocation forcée d'un périphérique” à la page 64
Libération forcée d'un périphérique.	Libère un périphérique actuellement alloué à un utilisateur.	“Libération forcée d'un périphérique” à la page 65
Modification des propriétés d'allocation d'un périphérique.	Modifie les conditions requises pour allouer un périphérique.	“Modification des périphériques pouvant être alloués” à la page 65
Audit de l'allocation de périphériques.	Enregistre l'allocation de périphériques dans la piste d'audit.	“Audit de l'allocation de périphériques” à la page 67
Création d'un script de nettoyage de périphériques.	Purge les données d'un périphérique physique.	“Ecriture de nouveaux scripts de nettoyage de périphériques” à la page 79

▼ Activation de l'allocation de périphériques

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Device Security (sécurité des périphériques). Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. Activez le service d'allocation de périphériques et vérifiez qu'il est bien activé.

```
# svcadm enable svc:/system/device/allocate
# svcs -x allocate
svc:/system/device/allocate:default (device allocation)
State: online since September 10, 2011 01:10:11 PM PDT
See: allocate(1)
See: deallocate(1)
See: list_devices(1)
See: device_allocate(1M)
See: mkdevalloc(1M)
```

```
See: mkdevmaps(1M)
See: dminfo(1M)
See: device_maps(4)
See: /var/svc/log/system-device-allocate:default.log
Impact: None.
```

2. **Pour désactiver le service d'allocation de périphériques, exécutez la sous-commande `disable`.**

```
# svcadm disable device/allocate
```

▼ Autorisation des utilisateurs à allouer un périphérique

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits User Security (sécurité des utilisateurs). Vos profils de droits doivent inclure l'autorisation `solaris.auth.delegate`. Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Créez un profil de droits contenant les commandes et l'autorisation appropriées.**

   En règle générale, vous devez créer un profil de droits comportant l'autorisation `solaris.device.allocate`. Suivez les instructions données dans " Création d'un profil de droits " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 " Donnez au profil de droits les propriétés appropriées, telles que les suivantes :

   - Nom du profil de droits : `Device Allocation`
   - Autorisations accordées : `solaris.device.allocate`
   - Commandes avec des privilèges : `mount` avec le privilège `sys_mount` et `umount` avec le privilège `sys_mount`

2. **(Facultatif) Créez un rôle pour le profil de droits.**

   Suivez les instructions données dans " Attribution de droits aux utilisateurs " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ". Utilisez les propriétés de rôle suivantes, données à titre d'exemple :

   - Nom de rôle : `devicealloc`
   - Nom de rôle complet : `Device Allocator`
   - Description du rôle : `Allocates and mounts allocated devices`
   - Profil de droits : `Device Allocation`

     Ce profil de droits doit figurer en tête de la liste des profils inclus dans le rôle.

3. **Affectez le profil de droits aux utilisateurs autorisés ou rôles autorisés.**

4. **Apprenez aux utilisateurs comment utiliser l'allocation de périphériques.**

   Pour consulter des exemples d'allocation de média amovible, reportez-vous à la section “Allocation des périphériques” à la page 67.

Affichage d'informations d'allocation sur un périphérique

Avant de commencer

Consultez la section “Activation de l'allocation de périphériques” à la page 62.

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Device Security (sécurité des périphériques). Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

- **Affichage des informations sur les périphériques pouvant être alloués sur votre système.**

  ```
  # list_devices device-name
  ```

  où *device-name* est l'un des suivants :

  - `audio`[*n*] : microphone et haut-parleur.
  - `rmdisk`[*n*] : périphérique de média amovible, tel qu'une clé USB.
  - `sr`[*n*] : lecteur de CD-ROM.
  - `st`[*n*] Lecteur de bandes.

Erreurs fréquentes

Si la commande `list__devices` renvoie un message d'erreur identique au suivant, soit l'allocation de périphériques n'est pas activée, soit vous ne disposez pas des autorisations suffisantes pour récupérer les informations.

```
list_devices: No device maps file entry for specified device.
```

Pour que la commande s'exécute correctement, activez l'allocation de périphériques et prenez un rôle bénéficiant de l'autorisation `solaris.device.revoke`.

Allocation forcée d'un périphérique

L'allocation forcée est utilisée lorsque quelqu'un a oublié de libérer un périphérique. L'allocation forcée peut également être utilisée lorsqu'un utilisateur a un besoin immédiat d'un périphérique.

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

1. **Déterminez si vous disposez de l'autorisation appropriée dans votre rôle.**

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2. **Forcez l'allocation du périphérique à l'utilisateur nécessitant le périphérique.**
   Dans cet exemple, un lecteur USB est alloué de force à l'utilisateur `jdoe`.

```
$ allocate -U jdoe
```

▼ Libération forcée d'un périphérique

Les périphériques alloués à un utilisateur ne sont pas automatiquement libérés lorsque le processus se termine ou lorsque l'utilisateur se déconnecte. La libération forcée est utilisée lorsque quelqu'un a oublié de libérer un périphérique.

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

1. **Déterminez si vous disposez de l'autorisation appropriée dans votre rôle.**

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2. **Forcez la libération du périphérique.**
   Dans cet exemple, une libération de l'imprimante est forcée de sorte qu'il peut s'appliquer à l'usage d'un autre utilisateur.

```
$ deallocate -f /dev/lp/printer-1
```

▼ Modification des périphériques pouvant être alloués

Avant de commencer L'allocation de périphériques doit être activée pour cette procédure s'exécute correctement. Pour activer l'allocation de périphériques, reportez-vous à la section "Activation de l'allocation de périphériques" à la page 62. Vous devez prendre le rôle `root`.

- **Modifier le cinquième champ dans l'entrée de périphérique du fichier`device_allocate` pour spécifier si l'autorisation est requise, ou spécifiez l'autorisation `solaris.device.allocate`.**

```
audio;audio;reserved;reserved;solaris.device.allocate;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

où `solaris.device.allocate` indique qu'un utilisateur doit disposer de l'autorisation `solaris.device.allocate` pour utiliser le périphérique.

Exemple 4-2 Attribution de l'autorisation d'allouer un périphérique à n'importe quel utilisateur

Dans l'exemple suivant, tous les utilisateurs du système peuvent allouer tous les périphériques. Le cinquième champ de chaque entrée de périphérique dans le fichier `device_allocate` a été remplacé par un signe arobase (`@`).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;@;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;@;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;@;/etc/security/lib/sr_clean
…
```

Exemple 4-3 Interdiction d'utilisation de certains périphériques

Dans l'exemple suivant, le périphérique audio ne peut pas être utilisé. Le cinquième champ de l'entrée de périphérique audio dans le fichier `device_allocate` a été remplacé par un astérisque (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris device.allocate;/etc/security/lib/sr_clean
…
```

Exemple 4-4 Interdiction d'utilisation de tous les périphériques

Dans l'exemple ci-dessous, aucun périphérique ne peut être utilisé. Le cinquième champ de chaque entrée de périphérique dans le fichier `device_allocate` a été remplacé par un astérisque (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;*;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;*;/etc/security/lib/sr_clean
…
```

▼ Audit de l'allocation de périphériques

Par défaut, les commandes d'allocation de périphériques se trouvent dans la classe d'audit `other`.

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

- **Présélectionnez la classe d'audit `ot`.**

```
$ auditconfig -getflags
current-flags
$ auditconfig -setflags current-flags,ot
```

Pour obtenir des instructions détaillées, reportez-vous à la section " Présélection des classes d'audit " du manuel " Gestion de l'audit dans Oracle Solaris 11.2 ".

Allocation de périphériques

L'allocation de périphériques limite l'utilisation d'un périphérique à un utilisateur à la fois. Les périphériques qui nécessitent un point de montage doivent être montés. Les procédures ci-dessous indiquent aux utilisateurs comment allouer des périphériques.

▼ Allocation des périphériques

Avant de commencer L'allocation de périphériques doit être activée, comme décrit à la section "Activation de l'allocation de périphériques" à la page 62. Si une autorisation est requise, l'utilisateur doit disposer de l'autorisation.

1. **Allouez le périphérique.**

   Spécifiez le périphérique en indiquant son nom.

   ```
   % allocate device-name
   ```

2. **Vérifiez que le périphérique est alloué en répétant la commande.**

   ```
   % allocate device-name
   allocate. Device already allocated.
   ```

Exemple 4-5 Allocation d'un microphone

Dans cet exemple, l'utilisateur `jdoe` alloue un microphone, `audio0`.

```
% whoami
jdoe
% allocate audio0
```

Exemple 4-6 Allocation d'une imprimante

Dans cet exemple, un utilisateur alloue une imprimante. Personne d'autre ne peut imprimer à partir de `printer-1` jusqu'à ce que l'utilisateur libère l'imprimante ou jusqu'à ce que l'imprimante soit allouée de force à un autre utilisateur.

```
% allocate /dev/lp/printer-1
```

Pour obtenir un exemple de libération forcée, reportez-vous à la section “Libération forcée d'un périphérique” à la page 65.

Exemple 4-7 Allocation d'une clé USB

Dans cet exemple, un utilisateur alloue une clé USB, `rmdisk1`.

```
% allocate rmdisk1
```

Erreurs fréquentes

Si la commande `allocate` ne peut pas allouer le périphérique, un message d'erreur s'affiche dans la fenêtre de la console. Pour obtenir une liste des messages d'erreur d'allocation, reportez-vous à la page de manuel `allocate`(1).

▼ Montage d'un périphérique alloué

Les périphériques sont montés automatiquement si les privilèges appropriés vous sont accordés. Suivez cette procédure en cas d'échec du montage du périphérique.

Avant de commencer

Vous avez alloué le périphérique. Vous disposez des privilèges nécessaires pour monter le périphérique, comme décrit à la section “Autorisation des utilisateurs à allouer un périphérique” à la page 63.

1. Prenez un rôle pouvant allouer et monter un périphérique.

```
% su - role-name
Password:       <Type role-name password>
```

```
$
```

2. **Créez et protégez un point de montage dans le répertoire d'accueil du rôle.**

   Vous n'avez besoin d'effectuer cette étape que la première fois que vous nécessitez un point de montage.

   ```
   $ mkdir mount-point ; chmod 700 mount-point
   ```

3. **Répertoriez les périphériques allouables.**

   ```
   $ list_devices -l
   List of allocatable devices
   ```

4. **Allouez le périphérique.**

   Spécifiez le périphérique en indiquant son nom.

   ```
   $ allocate device-name
   ```

5. **Montez le périphérique.**

   ```
   $ mount -o ro -F filesystem-type device-path mount-point
   ```

`-o ro`	Indique que le périphérique doit être monté en lecture seule. Utilisez `-o rw` pour rendre le périphérique accessible en écriture.
`-F` *filesystem-type*	Indique le format du système de fichiers du périphérique. En règle générale, un CD-ROM est formaté avec un système de fichiers HSFS. Une disquette est généralement formatée avec un système de fichiers PCFS.
device-path	Indique le chemin d'accès au périphérique. La sortie de la commande `list_devices -l` inclut le *device-path*.
mount-point	Indique le point de montage que vous avez créé à l'Étape 2.

Exemple 4-8 Allocation d'une unité de CD-ROM

Dans cet exemple, un utilisateur prend un rôle pouvant allouer et monter une unité de CD-ROM, `sr0`. L'unité de disque est formatée en tant que système de fichiers HSFS.

```
% roles
devicealloc
% su - devicealloc
Password:       <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
```

```
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
```

List of the contents of CD-ROM

Erreurs fréquentes Si la commande `mount` ne peut pas monter le périphérique, le message d'erreur `mount: insufficient privileges` s'affiche ; vérifiez alors les points suivants :

- Vérifiez que vous exécutez la commande `mount` dans un shell de profil. Si vous avez pris un rôle, ce dernier a un shell de profil. Si vous êtes un utilisateur auquel un profil a été affecté à l'aide de la commande `mount`, vous devez créer un shell de profil. Pour obtenir la liste des shells de profil disponibles, reportez-vous à la page de manuel `pfexec`(1).
- Vérifiez que vous êtes le propriétaire du point de montage spécifié. Vous devez disposer d'un accès en lecture, écriture et exécution au point de montage.

Contactez votre administrateur si vous ne pouvez toujours pas monter le périphérique alloué. Reportez-vous à la section " Dépannage d'attributions de droits " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

▼ Libération des périphériques

La libération d'un périphérique permet à d'autres utilisateurs d'allouer et d'utiliser le périphérique lorsque vous avez terminé.

Avant de commencer Vous devez avoir alloué le périphérique. Pour plus d'informations, reportez-vous à la section "Allocation des périphériques" à la page 67.

1. Si le périphérique est monté, démontez-le.

```
$ cd $HOME
$ umount mount-point
```

2. Libérez le périphérique.

```
$ deallocate device-name
```

Exemple 4-9 Libération d'un microphone

Dans cet exemple, l'utilisateur `jdoe` libère le microphone, `audio`.

```
% whoami
jdoe
```

```
% deallocate audio0
```

Exemple 4-10 Libération d'une unité de CD-ROM

Dans cet exemple, le rôle Device Allocator permet de libérer une unité de CD-ROM . Une fois que le message imprimé, le CD-ROM est éjecté.

```
$ whoami
devicealloc
$ cd /home/devicealloc
$ umount /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
$
$ deallocate sr0
/dev/sr0:      326o
/dev/rsr0:     326o
…
sr_clean: Media in sr0 is ready.  Please, label and store safely.
```

Protection de périphériques (référence)

Les périphériques dans Oracle Solaris sont protégés par la stratégie de périphériques de noyau. Les périphériques peuvent être protégés par le biais de l'allocation de périphériques. L'allocation de périphériques peut être activée et est appliquée au niveau de l'utilisateur.

Commandes de la stratégie de périphériques

Les commandes de gestion des périphériques permettent de gérer la stratégie de périphériques sur des fichiers locaux. La stratégie de périphériques peut inclure des exigences en matière de privilèges. Les utilisateurs disposant des profils de droits Device Management (gestion des périphériques) et Device Security (sécurité des périphériques) peuvent gérer les périphériques.

Le tableau suivant répertorie les commandes de gestion des périphériques.

TABLEAU 4-3 Commandes de gestion des périphériques

Commande	Description
`add_drv`(1M)	Ajoute un nouveau pilote de périphérique à un système en cours d'exécution. Contient des options pour ajouter une stratégie au nouveau périphérique. En règle générale, cette commande est appelée dans un script lorsqu'un pilote de périphérique est en cours d'installation.
`devfsadm`(1M)	Administre des périphériques et des pilotes de périphériques sur un système en cours d'exécution. Charge également la stratégie de périphériques.

Commande	Description
	La commande `devfsadm` permet de nettoyer des liens `/dev` lâches vers des disques, des bandes, des ports, des périphériques audio et des pseudopériphériques. Des périphériques d'un pilote nommé peuvent également être reconfigurés.
`getdevpolicy`(1M)	Affiche la stratégie associée à un ou plusieurs périphériques. Cette commande peut être exécutée par n'importe quel utilisateur.
`rem_drv`(1M)	Supprime un périphérique ou un pilote de périphérique.
`update_drv`(1M)	Met à jour les attributs d'un pilote de périphérique existant. Contient des options pour mettre à jour la stratégie de périphériques pour le périphérique. En règle générale, cette commande est appelée dans un script lorsqu'un pilote de périphérique est en cours d'installation.

Allocation de périphériques

L'allocation de périphériques peut protéger votre site contre la perte de données, les virus informatiques et d'autres failles de sécurité. Contrairement à la stratégie de périphériques, l'allocation de périphériques est facultative. L'allocation de périphériques utilise des autorisations pour limiter l'accès aux périphériques allouables.

Composants de l'allocation de périphériques

Les composants du mécanisme d'allocation de périphériques sont les suivants :

- Le service `svc:/system/device/allocate`. Pour plus d'informations, reportez-vous à la page de manuel `smf`(5) et aux pages de manuel concernant les commandes d'allocation de périphériques.
- Les commandes `allocate`, `deallocate`, `dminfo` et `list_devices`. Pour plus d'informations, reportez-vous à la section “Commandes d'allocation de périphériques” à la page 73.
- Les profils de droits Device Management (gestion des périphériques) et Device Security (sécurité des périphériques). Pour plus d'informations, reportez-vous à la section “Profils de droits Device Allocation (allocation de périphériques)” à la page 73.
- Les scripts de nettoyage de périphériques pour chaque périphérique allouable.

Ces commandes et scripts utilisent les fichiers locaux suivants pour mettre en oeuvre l'allocation de périphériques :

- Le fichier `/etc/security/device_allocate`. Pour plus d'informations, reportez-vous à la page de manuel `device_allocate`(4).
- Le fichier `/etc/security/device_maps`. Pour plus d'informations, reportez-vous à la page de manuel `device_maps`(4).
- Un fichier de verrouillage, dans le répertoire `/etc/security/dev`, pour chaque périphérique allouable.

- Les attributs modifiés du fichier de verrouillage qui sont associés à chaque périphérique allouable.

Service d'allocation de périphériques

Le service `svc:/system/device/allocate` contrôle l'allocation de périphériques. Ce service est désactivé par défaut.

Profils de droits Device Allocation (allocation de périphériques)

Les profils de droits Device Management (gestion des périphériques) et Device Security (sécurité des périphériques) sont requis pour gérer et allouer des périphériques, respectivement.

Ces profils de droits comprennent les autorisations suivantes :

- `solaris.device.allocate` : nécessaire pour allouer un périphérique
- `solaris.device.cdrw` : nécessaire pour lire et écrire un CD-ROM
- `solaris.device.config` : nécessaire pour configurer les attributs d'un périphérique
- `solaris.device.mount.alloptions.fixed` : nécessaire pour spécifier des options de montage lors du montage d'un périphérique fixe
- `solaris.device.mount.alloptions.removable` : nécessaire pour spécifier des options de montage lors du montage d'un périphérique amovible
- `solaris.device.mount.fixed` : nécessaire pour monter un périphérique fixe
- `solaris.device.mount.removable` : nécessaire pour monter un périphérique amovible
- `solaris.device.revoke` : nécessaire pour révoquer ou récupérer un périphérique

Commandes d'allocation de périphériques

Avec les options en majuscules, les commandes `allocate`, `deallocate` et `list_devices` sont des commandes d'administration. Dans le cas contraire, ces commandes sont des commandes d'utilisateur. Le tableau suivant répertorie les commandes d'allocation de périphériques.

TABLEAU 4-4 Commandes d'allocation de périphériques

Page de manuel pour les commandes	Description
`allocate`(1)	Réserve un périphérique allouable pour une utilisation par un autre utilisateur.

Page de manuel pour les commandes	Description
	Par défaut, un utilisateur doit disposer de l'autorisation `solaris.device.allocate` pour allouer un périphérique. Vous pouvez modifier le fichier `device_allocate` pour ne pas exiger l'autorisation de l'utilisateur. Tout utilisateur du système peut demander que le périphérique soit alloué pour l'utilisation.
`deallocate`(1)	Supprime la réserve d'allocation d'un autre périphérique.
`dminfo`(1M)	Recherche un périphérique allouable par type, nom et nom du chemin d'accès complet.
`list_devices`(1)	Répertorie les statuts des périphériques allouables. Répertorie tous les fichiers spécifiques à un périphérique qui sont associés à tout périphérique répertorié dans le fichier `device_maps`. Avec l'option `-U`, répertorie les périphériques qui sont allouables ou alloués à l'ID utilisateur indiqué. Cette option vous permet de vérifier les périphériques allouables ou alloués à un autre utilisateur. Vous devez avoir l'autorisation `solaris.device.revoke`.

Autorisations pour les commandes d'allocation

Par défaut, les utilisateurs doivent avoir l'autorisation `solaris.device.allocate` pour réserver un périphérique allouable. Pour créer un profil de droits afin d'inclure l'autorisation `solaris.device.allocate`, reportez-vous à la section “Autorisation des utilisateurs à allouer un périphérique” à la page 63.

Les administrateurs doivent disposer de l'autorisation `solaris.device.revoke` pour modifier l'état d'allocation d'un périphérique. Par exemple, l'option `-U` des commandes `allocate` et `list_devices` et l'option `-F` de la commande `deallocate` nécessitent l'autorisation `solaris.device.revoke`.

Pour plus d'informations, reportez-vous à la section “ Commandes sélectionnées nécessitant des autorisations ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

Etat d'erreur d'allocation

Un périphérique est placé dans un *état d'erreur d'allocation* en cas d'échec des commandes `deallocate` ou `allocate` . Lorsqu'un périphérique allouable est dans un état d'erreur d'allocation, le périphérique doit être libéré de force. Seul un utilisateur ou un rôle bénéficiant du profil de droits Device Management (gestion des périphériques) ou Device Security (sécurité des périphériques) peut gérer un état d'erreur d'allocation.

La commande `deallocate` avec l'option `-F` force la libération. Vous pouvez également utiliser `allocate -U` pour affecter le périphérique à un utilisateur. Une fois le périphérique alloué, vous

pouvez analyser les messages d'erreur qui s'affichent. Après la correction des problèmes liés au périphérique, vous pouvez forcer la libération.

Fichier `device_maps`

Les listes de périphériques sont créées lors de la configuration de l'allocation de périphériques. Le fichier `/etc/security/device_maps` inclut les noms de périphérique, types de périphérique, fichiers spécifiques au périphérique qui sont associés à chaque périphérique allouable.

Le fichier `device_maps` définit les mappages de fichiers spécifiques à un périphérique pour chaque périphérique, ce qui n'est pas intuitif dans de nombreux cas. Ce fichier permet aux programmes de découvrir les fichiers spécifiques à un périphérique à mapper aux périphériques. Vous pouvez utiliser la commande `dminfo`, par exemple, pour récupérer le nom et le type de périphérique, et les fichiers spécifiques au périphérique à spécifier lorsque vous paramétrez un périphérique allouable. La commande `dminfo` utilise le fichier `device_maps` pour rapporter ces informations.

Chaque périphérique est représenté par une entrée sur une seule ligne, au format suivant :

device-name:*device-type*:*device-list*

EXEMPLE 4-11 Exemple d'entrée `device_maps`

L'exemple suivant montre une entrée dans un fichier `device_maps`.

```
audio0:\
audio:\
/dev/audio /dev/audioctl /dev/dsp /dev/dsp0 /dev/mixer0 /dev/sound/0
/dev/sound/0ctl /dev/sound/audio810\:0mixer /dev/sound/audio810\:0dsp
/dev/sound/audio810\:0 /dev/sound/audio810\:0ctl
```

Dans le fichier `device_maps`, les lignes peuvent être terminées par une barre oblique inverse (\) pour poursuivre l'entrée sur la ligne suivante. Des commentaires peuvent également être inclus. Un signe dièse (#) introduit des commentaires sur le texte suivant jusqu'à la prochaine nouvelle ligne qui n'est pas immédiatement précédée d'un backslash. Les espaces en début et fin sont autorisés dans n'importe quel champ. Les champs sont définis de la manière suivante :

device-name — Spécifie le nom du périphérique. Pour obtenir une liste des noms de périphériques courants, reportez-vous à la section “Affichage d'informations d'allocation sur un périphérique” à la page 64.

device-type — Spécifie le type de périphérique générique. Le nom générique est le nom de la classe de périphériques, comme `st`, `fd`, `rmdisk` ou `audio`. Le champ *device-type* regroupe logiquement les périphériques liés.

device-list Répertorie les fichiers spécifiques à un périphérique qui sont associés au périphérique physique. *device-list* doit contenir tous les fichiers spécifiques qui permettent d'accéder à un périphérique en particulier. Si la liste est incomplète, un utilisateur malveillant peut toujours obtenir ou modifier des informations privées. Les entrées valides pour le champ *device-list* reflètent les fichiers de périphériques qui sont situés dans le répertoire `/dev`.

Fichier `device_allocate`

Vous pouvez modifier le fichier `/etc/security/device_allocate` pour rendre des périphériques allouables non allouables ou pour ajouter de nouveaux périphériques.

Une entrée dans le fichier `device_allocate` ne signifie pas que le périphérique peut être alloué, sauf si cette entrée le définit comme tel.

Dans le fichier `device_allocate`, chaque périphérique est representé par une entrée sur une seule ligne dans le format suivant :

device-name`;`*device-type*`;reserved;reserved;`*auths*`;`*device-exec*

Voici un exemple de fichier `device_allocate`.

```
st0;st;;;;/etc/security/lib/st_clean
fd0;fd;;;;/etc/security/lib/fd_clean
sr0;sr;;;;/etc/security/lib/sr_clean
audio;audio;;;*;/etc/security/lib/audio_clean
```

Notez l'astérisque (*) dans le cinquième champ de l'entrée de périphérique `audio`.

Dans le fichier `device_allocate`, les lignes peuvent être terminées par une barre oblique inverse (\) pour poursuivre l'entrée sur la ligne suivante. Des commentaires peuvent également être inclus. Un signe dièse (#) introduit des commentaires sur le texte suivant jusqu'à la prochaine nouvelle ligne qui n'est pas immédiatement précédée d'un backslash. Les espaces en début et fin sont autorisés dans n'importe quel champ. Les champs sont définis de la manière suivante :

device-name Spécifie le nom du périphérique. Pour obtenir une liste des noms de périphériques courants, reportez-vous à la section “Affichage d'informations d'allocation sur un périphérique” à la page 64.

device-type Spécifie le type de périphérique générique. Le nom générique est le nom de la classe de périphériques, tel que `st`, `fd` et `sr`. Le champ *device-type* regroupe logiquement les périphériques liés. Lorsque vous rendez un périphérique allouable, récupérez le nom du périphérique du champ *device-type* dans le fichier `device_maps`.

`réservé`	Oracle réserve les deux champs qui sont marqués `reserved` pour une utilisation ultérieure.
auths	Indique si le périphérique peut être alloué. Un astérisque (`*`) dans ce champ indique que le périphérique n'est pas allouable. Une chaîne d'autorisation ou un champ vide indique que le périphérique est allouable. Par exemple, la chaîne `solaris.device.allocate` dans le champ *auths* indique que l'autorisation `solaris.device.allocate` est requise pour allouer le périphérique. Un signe arobase (`@`) dans ce fichier indique que le périphérique est allouable par n'importe quel utilisateur.
device-exec	Fournit le nom de chemin d'un script à invoquer pour une manipulation spéciale, telle que le nettoyage et la protection contre la réutilisation des objets durant le processus d'allocation. Le script *device-exec* est exécuté chaque fois qu'une commande `deallocate` est effectuée sur le périphérique.

Par exemple, l'entrée suivante pour le périphérique `sr0` indique que l'unité de CD-ROM est allouable par un utilisateur ayant l'autorisation `solaris.device.allocate` :

```
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Vous pouvez accepter les périphériques par défaut et leurs caractéristiques définies. Après l'installation d'un nouveau périphérique, vous pouvez modifier les entrées. Tout périphérique devant être alloué avant l'utilisation doit être défini dans les fichiers `device_allocate` et `device_maps` pour le système de ce périphérique. Actuellement, les lecteurs de bande de cartouche, unités de disquette, unités de CD-ROM, périphériques de médias amovibles et puces audio sont considérés comme allouables. Ces types de périphériques disposent de scripts de nettoyage de périphériques.

Remarque - Les lecteurs de bande Xylogics et Archive utilisent également le script `st_clean` fourni pour les périphériques SCSI. Vous devez créer vos propres scripts de nettoyage de périphériques pour d'autres périphériques, tels que des terminaux, des tablettes graphiques et d'autres périphériques allouables. Le script doit remplir des critères de réutilisation des objets pour ce type de périphérique.

Scripts de nettoyage de périphériques

L'allocation de périphériques satisfait en partie ce que les auditeurs de sécurité appellent les besoins en matière de *réutilisation des objets*. Le script device-clean remplit l'exigence de sécurité selon laquelle toutes les données utilisables doivent être purgées d'un périphérique physique avant sa réutilisation. Les données sont effacées avant que le périphérique ne devienne allouable par un autre utilisateur. Par défaut, les lecteurs de bande de cartouche, les unités de disquette, les unités de CD-ROM et les périphériques audio nécessitent des scripts de nettoyage

de périphériques, qui sont fournis par Oracle Solaris. Cette section décrit les actions effectuées par les scripts de nettoyage de périphériques.

Script de nettoyage de périphériques pour bandes

Le script de nettoyage de périphériques `st_clean` prend en charge trois périphériques à bande :

- Bande SCSI ¼ pouces
- Bande Archive ¼ pouces
- Bande Open-reel ½ pouces

Le script `st_clean` utilise l'option `rewoffl` avec la commande `mt` pour nettoyer le périphérique. Pour plus d'informations, reportez-vous à la page de manuel `mt`(1). Si le script s'exécute pendant l'initialisation du système, il interroge le périphérique pour déterminer si celui-ci est en ligne. Si le périphérique est en ligne, le script détermine si le périphérique dispose de supports. Les périphériques à bande ¼ pouces disposant de médias à l'intérieur sont placés dans l'état d'erreur d'allocation. L'état d'erreur d'allocation oblige l'administrateur à nettoyer manuellement le périphérique.

En fonctionnement normal du système, lorsque la commande `deallocate` est exécutée en mode interactif, l'utilisateur est invité à supprimer le média. La libération est reportée jusqu'à ce que le média soit supprimé du périphérique.

Scripts de nettoyage de périphériques pour disquettes et unités de CD-ROM

Les scripts suivants de nettoyage de périphériques sont fournis pour les unités de disquette et de CD-ROM :

- **`fd_clean`**, script – Script de nettoyage de périphériques pour les disquettes.
- **`sr_clean`**, script – Script de nettoyage de périphériques pour les lecteurs de CD-ROM.

Les scripts utilisent la commande `eject` pour supprimer les médias de l'unité. Si la commande `eject` échoue, le périphérique est placé dans l'état d'erreur d'allocation. Pour plus d'informations, reportez-vous à la page de manuel `eject`(1).

Script de nettoyage de périphériques audio

Les périphériques audio sont nettoyés à l'aide d'un script `audio_clean`. Le script effectue un appel système ioctl `AUDIO_GETINFO` pour lire le périphérique. Le script effectue ensuite un appel système ioctl `AUDIO_SETINFO` pour rétablir la configuration par défaut d'un périphérique.

Ecriture de nouveaux scripts de nettoyage de périphériques

Si vous ajoutez plusieurs périphériques allouables au système, vous devrez peut-être créer vos propres scripts de nettoyage de périphériques. La commande `deallocate` transmet un paramètre aux scripts de nettoyage de périphériques. Le paramètre, qui est indiqué ici, est une chaîne qui contient le nom du périphérique. Pour plus d'informations, reportez-vous à la page de manuel `device_allocate`(4).

clean-script `-[I|i|f|S]` *device-name*

Les scripts de nettoyage de périphériques doivent renvoyer la valeur "`0`" en cas d'exécution correcte et une valeur supérieure à "`0`" en cas d'échec. Les options `-I`, `-f` et `-S` déterminent le mode d'exécution du script :

`-I` Nécessaire uniquement lors de l'initialisation du système. Toutes les sorties doivent aller à la console du système. L'échec ou l'incapacité à éjecter de force le média doivent mettre le périphérique dans l'état d'erreur d'allocation.

`-i` Similaire à l'option `-I`, à l'exception du fait que la sortie est supprimée.

`-f` Pour le nettoyage forcé. L'option est interactive et suppose que l'utilisateur est disponible pour répondre aux invites. Un script exécuté avec cette option doit tenter de terminer le nettoyage si une partie du nettoyage échoue.

`-S` Nettoyage standard. L'option est interactive et suppose que l'utilisateur est disponible pour répondre aux invites.

♦ ♦ ♦ CHAPITRE 5

Service d'analyse antivirus

Le présent chapitre donne des informations sur l'utilisation des logiciels antivirus et traite des sujets suivants :

A propos de l'analyse antivirus

Les données sont protégées contre les virus par un service d'analyse, `vscan`, qui utilise différents *moteurs d'analyse*. Un Moteur d'analyse est une application tierce, résidant sur un hôte externe, qui examine un fichier à la recherche de virus connus. Un fichier est candidat pour l'analyse antivirus si le système de fichiers prend en charge le service `vscan`, si ce service a été activé et si le type de ce fichier n'a pas été exempté. L'analyse antivirus est ensuite exécutée sur un fichier lors des opérations d'ouverture et de fermeture si le fichier n'a pas été analysé précédemment avec les signatures de virus actuelles ou si le fichier a été modifié depuis sa dernière analyse.

Le service `vscan` peut être configuré pour utiliser plusieurs moteurs d'analyse. Nous vous recommandons d'utiliser un minimum de deux moteurs d'analyse. Les demandes pour les analyses de virus sont réparties entre tous les moteurs d'analyse disponibles.

La commande `vscanadm show` affiche la liste des moteurs d'analyse configurés sur le système.

```
# vscanadm show
max-size=1GB max-size-action=allow
types=+*
no scan engines configured
```

A propos du service vscan

L'avantage de la méthode d'analyse en temps réel est qu'un fichier est analysé avec les dernières définitions de virus *avant* d'être utilisé. Avec cette approche, les virus peuvent être détectés avant qu'ils ne puissent compromettre les données.

Lorsqu'un utilisateur ouvre un fichier à partir du client, le traitement fonctionne analyse antivirus comme suit :

1. le service vscan détermine si le fichier doit être analysé, selon que le fichier a déjà été analysé avec les signatures de virus actuelles et qu'il a été modifié ou non depuis sa dernière analyse.

   En cas de scannage ne soit pas nécessaire, puis, le processus se termine et l'utilisateur est autorisé à accéder au fichier
2. En cas de scannage est nécessaire, le fichier est transféré vers le moteur d'analyse.

   Si le transfert est établie, le moteur analyse le fichier à l'aide des définitions de virus actuelles afin de déterminer si le fichier est infecté.

   Si le transfert échoue, le processus se poursuit de la manière suivante :

   - Il est transféré vers le moteur de détection disponible suivant le balayage des fichiers, qui peuvent exécuter la.
   - En l'absence d'avenant, ou si aucune autre sont disponibles, les moteurs analyse antivirus est considérée comme étant en échec et l'accès au fichier risquent d'être refusées.
3. Si le fichier n'est pas infecté, il est marqué avec un timbre d'analyse et le client est autorisé y à accéder.

   Si un virus est détecté, le fichier est marqué comme étant mis en quarantaine. Un fichier mis en quarantaine ne peut pas être lu, exécuté ou renommé, mais il peut être supprimé. Le journal système enregistre le nom du fichier mis en quarantaine et le nom du virus et, si l'audit a été activé, un enregistrement d'audit avec les mêmes informations est créé.

Utilisation du service vscan

L'analyse des fichiers à la recherche de virus est disponible lorsque les conditions suivantes sont réunies :

- Au moins un moteur d'analyse est installé et configuré.
- Les fichiers sont stockés dans un système de fichiers qui prend en charge l'analyse antivirus.
- L'analyse antivirus est activée sur le système de fichiers.
- Le service vscan est activé.

- Le service `vscan` est configuré pour analyser les fichiers du type de fichier spécifié.

Le tableau suivant indique les tâches à effectuer pour configurer le service `vscan`.

Tâche	Description	Pour obtenir des instructions
Installation d'un moteur d'analyse.	Installe et configure un ou plusieurs produits antivirus tiers pris en charge OSOL ENT : entre accolades {}.	Consultez la documentation fournie avec le produit.
Activation du système de fichiers afin d'autoriser les analyses de virus.	Active les analyses de virus sur un système de fichiers ZFS. Par défaut, les analyses sont désactivés.	“Activation de l'analyse antivirus sur un système de fichiers” à la page 83
Activation du service `vscan`.	Démarre le service d'analyse.	“Activation du service `vscan`” à la page 84
Ajout d'un moteur d'analyse au service `vscan`.	Ajout de moteurs d'analyse spécifiques dans le service `vscan`.	“Ajout d'un moteur d'analyse” à la page 84
Configuration du service `vscan`.	Affichage et modification des propriétés de `vscan`.	“Affichage des propriétés vscan” à la page 84 “Limitation de la taille des fichiers analysés” à la page 85
Configuration du service `vscan` pour des types de fichier spécifiques.	Indique les types de fichier à inclure et exclure dans une analyse.	“Exclusion de fichiers des analyses antivirus” à la page 86

▼ Activation de l'analyse antivirus sur un système de fichiers

Utilisez la commande du système de fichiers afin d'autoriser les analyses de virus des fichiers. Par exemple, pour inclure la création d'un système de fichiers ZFS dans une analyse de virus, utilisez la commande `zfs`(1M).

Le système de fichiers ZFS permet à certaines tâches d'administration d'être déléguées à des utilisateurs spécifiques. Pour plus d'informations sur l'administration déléguée, reportez-vous au Chapitre 8, “ Administration déléguée de ZFS dans Oracle Solaris ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits ZFS File System Management (gestion de système de fichiers ZFS) ou ZFS Storage Management (gestion de stockage ZFS). Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

- **Activez l'analyse antivirus sur un système de fichiers ZFS.**

```
# zfs set vscan=on zfs-file-system
```

Par exemple, si le système de fichiers ZFS est *path*`/pool/volumes/vol1`, saisissez la commande suivante :

```
# zfs set vscan=on path/pool/volumes/vol1
```

Activation du service vscan

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

- **Activez le service d'analyse antivirus.**

```
# svcadm enable vscan
```

Ajout d'un moteur d'analyse

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

- **un moteur d'analyse au service `vscan` avec les propriétés par défaut, tapez :**

```
# vscanadm add-engine engineID
```

Pour plus d'informations, reportez-vous à la page de manuel `vscanadm`(1M).

Affichage des propriétés vscan

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

- **Affichez les propriétés du service `vscan`, de tous les moteurs d'analyse ou d'un moteur d'analyse spécifique.**

- **Pour afficher les propriétés d'un moteur d'analyse spécifique, tapez :**

  ```
  # vscanadm get-engine engineID
  ```

- **Pour visualiser les propriétés de tous les moteurs d'analyse, tapez :**

  ```
  # vscanadm get-engine
  ```

- **Pour afficher l'une des propriétés du service `vscan`, tapez :**

  ```
  # vscanadm get -p property
  ```

  où *property* est l'un des paramètres décrits dans la page de manuel pour la commande `vscanadm`(1M).

  Par exemple, si vous voulez connaître la taille maximale d'un fichier qui peut être analysé, tapez :

  ```
  # vscanadm get max-size
  ```

Limitation de la taille des fichiers analysés

Puisque de nombreux moteurs d'analyse limitent la taille des fichiers qu'ils analysent, la propriété `max-size` du service `vscan` doit être définie sur une valeur inférieure ou égale à la taille maximale autorisée du moteur d'analyse. Ensuite, vous définissez si les fichiers dont la taille dépasse la taille maximale, et ne sont donc pas analysés, sont accessibles.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant du profil de droits VSCAN Management (gestion VSCAN). Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Visualiser les propriétés en cours.**

   ```
   # vscanadm show
   ```

2. **Définissez la taille maximale pour les analyses de virus.**

   Par exemple, pour définir une limite de 128 méga-octets , procédez comme suit :

   ```
   # vscanadm set -p max-size=128M
   ```

3. **Spécifiez que l'accès est refusé à tout fichier qui n'est pas analysé en raison de sa taille.**

   ```
   # vscanadm set -p max-size-action=deny
   ```

Pour plus d'informations, reportez-vous à la page de manuel vscanadm(1M).

▼ Exclusion de fichiers des analyses antivirus

Lorsque vous activez une protection antivirus, vous pouvez indiquer que tous les fichiers de types spécifiques doivent être exclus de l'analyse antivirus. Le service vscan affecte les performances du système, mais vous pouvez préserver les ressources système en ciblant des types de fichiers spécifiques pour les analyses de virus.

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

1. **Affichez la liste de tous les types de fichiers inclus dans la recherche de virus.**

   ```
   # vscanadm get -p types
   ```

2. **Spécifiez les types de fichiers devant faire l'objet d'une analyse de virus.**

   Par exemple :

   - **Excluez un type de fichier spécifique, par exemple le type JPEG, de la recherche de virus.**

     ```
     # vscanadm set -p types=-jpg,+*
     ```

   - **Incluez un type de fichier spécifique, par exemple les fichiers exécutables, dans la recherche de virus.**

     ```
     # vscanadm set -p types=+exe,-*
     ```

   Pour plus d'informations, reportez-vous à la page de manuel vscanadm(1M).

Glossaire de la sécurité

AES Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des Etats-Unis a adopté la variante Rijndael de l'algorithme comme norme de chiffrement en octobre 2000. AES remplace le chiffrement Principal d'utilisateur comme norme administrative.

algorithme Algorithme cryptographique. Il s'agit d'une procédure de calcul récursive établie qui chiffre ou hache une entrée.

algorithme cryptographique Voir algorithme.

allocation de périphériques Protection des périphériques au niveau de l'utilisateur. L'allocation de périphériques met en oeuvre l'utilisation exclusive d'un périphérique par un utilisateur à la fois. Les données des périphériques sont purgées avant toute réutilisation d'un périphérique. Des autorisations peuvent être utilisées pour limiter les utilisateurs autorisés à allouer un périphérique.

Amorce Valeur numérique de départ pour la génération de nombres aléatoires. Lorsque cette valeur provient d'une source aléatoire, l'amorce est appelée *amorce aléatoire*.

Application privilégiée Application pouvant remplacer les contrôles système. L'application vérifie les attributs de sécurité, tels que des UID spécifiques, des ID de groupe, des autorisations ou des privilèges.

Attributs de sécurité Remplacements de la stratégie de sécurité qui permettent à une commande d'administration de s'exécuter correctement lorsqu'elle est exécutée par un utilisateur autre que le superutilisateur. Dans le modèle de superutilisateur, les programmes `setuid root` et `setgid` sont des attributs de sécurité. Lorsque ces attributs sont appliqués à une commande, la commande s'exécute correctement, quel que soit l'utilisateur qui l'exécute. Dans le Modèle de privilège, les privilèges du noyau et les autres droits remplacent les programmes `setuid root` comme attributs de sécurité. Le modèle de privilège est compatible avec le modèle de superutilisateur dans la mesure où le modèle de privilège reconnaît également les programmes `setuid` et `setgid` comme des attributs de sécurité.

Authentificateur Des authentificateurs sont transmis par des clients lors de la demande de tickets (à un KDC) et de services (à un serveur). Ils contiennent des informations générées par l'utilisation d'une clé de session connue uniquement du client et du serveur, dont l'origine récente peut être prouvée, indiquant ainsi que la transaction est sécurisée. Lorsqu'un authentificateur est utilisé avec un

ticket, il peut permettre d'authentifier un principal d'utilisateur. Un authentificateur inclut le nom du principal de l'utilisateur, l'adresse IP de l'hôte de l'utilisateur, ainsi qu'un horodatage. A la différence d'un ticket, un authentificateur ne peut servir qu'une seule fois, généralement lorsque l'accès à un service est demandé. Un authentificateur est chiffré à l'aide de la clé de session pour ce client et ce serveur.

Authentification Processus de vérification de l'identité déclarée d'un principal.

Autorisation 1. Dans Kerberos, processus consistant à déterminer si un principal peut utiliser un service et à définir les objets auxquels il peut accéder, ainsi que le type d'accès autorisé pour chaque objet.

2. Dans la gestion des droits des utilisateurs, autorisation pouvant être attribuée à un rôle ou un utilisateur (ou intégrée dans un profil de droits) en vue de l'exécution d'une classe d'opérations autrement interdites par la stratégie de sécurité. Les "feux verts" sont mises en oeuvre au niveau de l'application utilisateur, et non dans le noyau.

Blowfish Algorithme de chiffrement par bloc symétrique de longueur de clé variable (entre 32 et 448 bits). Son créateur, Bruce Schneier, affirme que Blowfish est optimisé pour les applications pour lesquelles la clé n'a pas besoin d'être régulièrement modifiée.

Cache d'informations d'identification Espace de stockage (généralement un fichier) contenant des informations d'identification reçues de KDC.

champ d'application du service de noms Champ d'application dans lequel un rôle est autorisé à fonctionner, c'est-à-dire un hôte particulier ou tous les hôtes desservis par un service de noms spécifié, tel que NIS LDAP.

Chiffrement par clé privée Dans le cas du chiffrement par clé privée, l'expéditeur et le destinataire utilisent la même clé de chiffrement. Voir également chiffrement par clé publique.

chiffrement par clé publique Modèle de chiffrement où chaque utilisateur dispose de deux clés, l'une publique et l'autre privée. Dans le cas du chiffrement par clé publique, l'expéditeur chiffre le message à l'aide de la clé publique du destinataire, et ce dernier se sert d'une clé privée pour le déchiffrer. Le service Kerberos est un système à clé privée. Voir également Chiffrement par clé privée.

clé de service Clé de chiffrement partagée par un principal de service et le KDC, et distribuée en dehors des limites du système. Voir également Touche.

Clé de session Clé générée par le service d'authentification ou le service d'octroi de ticket. Une clé de session est générée dans le but de sécuriser les transactions entre un client et un service. La durée de vie d'une clé de session est limitée à une seule session de connexion. Voir également Touche.

Clé privée Chaque principal d'utilisateur reçoit une clé qui n'est connue que du KDC et de l'utilisateur du principal. Pour les principaux d'utilisateur, la clé est basée sur le mot de passe de l'utilisateur. Voir également Touche.

Clé secrète Voir Clé privée.

client Au sens strict, il s'agit d'un processus utilisant un service réseau pour le compte d'un utilisateur, par exemple, une application utilisant `rlogin`. Dans certains cas, un serveur peut être lui-même le client d'un autre serveur ou service.

Au sens large, il s'agit d'un hôte qui a) reçoit des informations d'identification Kerberos et b) utilise un service fourni par un serveur.

Dans la pratique, ce terme désigne un principal utilisant un service.

Confidentialité Voir confidentialité.

confidentialité Un service de sécurité, dans lequel les données transmises sont chiffrées avant leur envoi. La confidentialité inclut également l'intégrité des données et l'authentification de l'utilisateur. Voir également Authentification, intégrité, service.

Conscient des privilèges Programmes, scripts et commandes qui activent et désactivent l'utilisation des privilèges dans leur code. Dans un environnement de production, les privilèges qui sont activés doivent être fournis au processus, par exemple, en demandant aux utilisateurs du programme d'utiliser un profil de droits qui ajoute les privilèges au programme. Pour une description complète des privilèges, reportez-vous à la page de manuel `privileges`(5).

credential Package d'informations comprenant un ticket et une clé de session correspondante. Informations utilisées pour authentifier l'identité d'un principal. Voir également ticket, Clé de session.

DES Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique développée en 1975 et standardisée par l'ANSI en 1981 comme ANSI X.3.92. Le DES utilise une clé de 56 bits.

Destinataire Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, un consommateur est un utilisateur des services cryptographiques provenant de fournisseurs. Les consommateurs peuvent être des applications, des utilisateurs finaux ou des opérations de noyau. Kerberos, IKE et IPsec sont des exemples de consommateurs. Pour consulter des exemples de fournisseurs, reportez-vous à la section fournisseur.

domaine (realm) 1. Réseau logique desservi par une seule base de données Kerberos et un ensemble de centre de distribution des clés (KDC).

2. Troisième partie d'un nom de principal. Pour le nom de principal `jdoe/admin@CORP.EXAMPLE.COM`, le domaine est `CORP.EXAMPLE.COM`. Voir également Nom de principal.

droits Alternative au modèle tout ou rien des superutilisateurs. La gestion des droits des utilisateurs et la gestion des droits de processus permettent à une organisation de répartir les privilèges du superutilisateur et que vous les affectez aux utilisateurs ou rôles. Les droits dans Oracle Solaris sont implémentés en tant que privilèges de noyau, d'autorisation et de capacité à exécuter un

processus sous la forme d'un UID ou GID spécifique. Les droits peuvent être regroupés dans un Profil de droits et un rôle.

DSA Algorithme de signature numérique (Digital Signature Algorithm). Algorithme de clé publique dont la longueur de clé varie de 512 à 4 096 bits. La norme du gouvernement américain, DSS, atteint 1 024 bits. L'algorithme DSA repose sur l'algorithme SHA1 en entrée.

écart d'horloge Ecart maximal toléré entre les horloges système internes de tous les hôtes participant au système d'authentification Kerberos. Si l'écart d'horloge est dépassé entre des hôtes participants, les demandes sont rejetées. L'écart d'horloge est spécifié dans le fichier `krb5.conf`.

ECDSA Algorithme de signature numérique de courbe elliptique. Algorithme de clé publique basé sur une courbe elliptique mathématique. Une clé ECDSA est de beaucoup plus petite taille qu'une clé publique DSA nécessaire pour générer une signature de la même longueur.

Escalade des privilèges Accès aux ressources situées en dehors de la plage, les ressources qui y compris les droits qui vous sont affectés qui remplacent les valeurs par défaut, droits y autorisent. Il en résulte qu'un processus peut effectuer des actions non autorisées.

Evénement d'audit asynchrone Les événements asynchrones constituent la minorité des événements système. Ces événements ne sont associés à aucun processus, de sorte qu'aucun processus ne peut être bloqué puis réactivé ultérieurement. L'initialisation système initiale et les événements d'entrée et de sortie PROM sont des exemples d'événements asynchrones.

événement d'audit non allouable Evénement d'audit dont l'initiateur ne peut pas être déterminé, tel que l'événement AUE_BOOT.

événement d'audit synchrone Majorité des événements d'audit. Ces événements sont associés à un processus dans le système. Un événement non allouable associé à un processus est un événement synchrone, tel que l'échec d'une connexion.

fichier de ticket Voir Cache d'informations d'identification.

fichier keytab Fichier de table de clés contenant une ou plusieurs clés (principaux). Un hôte ou un service utilise un fichier keytab à peu près de la même façon qu'un utilisateur se sert d'un mot de passe.

fichier stash Un fichier stash contient une copie chiffrée de la clé principale pour le KDC. Cette clé principale est utilisée lorsqu'un serveur est réinitialisé pour authentifier automatiquement le KDC avant qu'il ne démarre les processus `kadmind` et `krb5kdc`. Etant donné que le fichier stash inclut la clé principale, ce fichier et toutes ses sauvegardes doivent être sécurisés. Si le chiffrement est compromis, la clé peut être utilisée pour accéder à la base de données KDC ou la modifier.

fichiers d'audit Journaux d'audit binaires. Les fichiers d'audit sont stockés séparément dans un système de fichiers d'audit.

fournisseur Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, service de cryptographie fourni aux consommateurs. Les bibliothèques PKCS #11, les modules cryptographiques du noyau et les accélérateurs de matériel sont des exemples de fournisseurs. Les fournisseurs se connectent à la structure cryptographique et sont donc également appelés *plug-ins*. Pour consulter des exemples de consommateurs, voir Destinataire.

Fournisseur de logiciels Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, module logiciel de noyau ou bibliothèque PKCS#11 fournissant des services cryptographiques. Voir également fournisseur.

Fournisseur de matériel Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, un pilote de périphérique et son accélérateur matériel. Les fournisseurs de matériel déchargent le système informatique d'opérations cryptographiques coûteuses, libérant ainsi les ressources de la CPU pour d'autres utilisations. Voir également fournisseur.

FQDN Nom de domaine complet. Par exemple, `central.example.com` (et pas simplement `denver`).

GSS-API Interface de programmation d'application générique de service de sécurité. Couche réseau assurant la prise en charge de différents services de sécurité modulaires, y compris le service Kerberos. GSS-API fournit des services d'authentification, d'intégrité et de confidentialité. Voir également Authentification, intégrité, confidentialité.

hôte Système accessible par l'intermédiaire d'un réseau.

Hôte principal Instance spécifique d'un principal de service dans lequel le principal (indiqué par le nom primaire `host`) est configuré de manière à fournir une gamme de services réseau, comme `ftp`, `rcp` ou `rlogin`. `host/central.example.com@EXAMPLE.COM` est un exemple d'hôte principal. Voir également principal de serveur.

Image système unique Une image système unique est utilisée dans l'audit d'Oracle Solaris afin de décrire un groupe de systèmes audités utilisant le même service de noms. Ces systèmes envoient leurs enregistrements d'audit à un serveur d'audit central où les enregistrements peuvent être comparés comme s'ils provenaient d'un même système.

instance Deuxième partie d'un nom de principal, une instance qualifie le primaire du principal. Dans le cas d'un principal de service, l'instance est requise. L'instance est le nom de domaine complet de l'hôte, comme dans `host/central.example.com`. Pour les principaux d'utilisateur, une instance est facultative. Notez, cependant, que `jdoe` et `jdoe/admin` sont des principaux uniques. Voir également primaire, Nom de principal, principal de service, Principal d'utilisateur.

intégrité Service de sécurité qui assure, outre l'authentification de l'utilisateur, la validité des données transmises par le biais de sommes de contrôle cryptographiques. Voir également Authentification, confidentialité.

jeu autorisé Jeu des privilèges disponibles pour l'utilisation par un processus.

jeu de base Jeu de privilèges affecté à un processus d'utilisateur lors de la connexion. Sur un système non modifié, le jeu héritable initial de chaque utilisateur correspond au jeu de base défini au moment de la connexion.

Jeu de privilèges Ensemble de privilèges. Chaque processus comporte quatre jeux de privilèges qui déterminent s'il peut utiliser un privilège particulier. Voir jeu limite, jeu effectif, jeu autorisé et jeu hérité.

De même, le jeu de base de privilèges est l'ensemble des privilèges affectés aux processus d'un utilisateur au moment de la connexion.

jeu effectif Jeu de privilèges actuellement en vigueur sur un processus.

jeu hérité Jeu de privilèges dont un processus peut hériter en appelant `exec`.

jeu limite Limite extérieure des privilèges disponibles pour un processus et ses enfants.

KDC Centre de distribution de clés (Key Distribution Center). Machine disposant de trois composants Kerberos V5.

- Principal et base de données de clés
- Service d'authentification
- Service d'octroi de tickets

Chaque domaine dispose d'un KDC maître et doit avoir un ou plusieurs KDC esclaves.

KDC esclave Copie d'un KDC maître capable de réaliser la plupart des fonctions du maître. Chaque domaine dispose généralement de plusieurs KDC esclaves et d'un seul KDC maître. Voir également KDC, KDC maître.

KDC maître KDC maître dans chaque domaine, comprenant un serveur d'administration Kerberos, `kadmind` et un démon d'authentification et d'octroi de tickets, `krb5kdc`. Chaque domaine doit disposer d'au moins un KDC maître, et peut avoir plusieurs KDC de duplication ou esclaves fournissant des services d'authentification aux clients.

Kerberos Service d'authentification, protocole utilisé par ce service ou code servant à mettre en oeuvre ce service.

Mise en oeuvre Kerberos d'Oracle Solaris étroitement basée sur la mise en oeuvre Kerberos V5.

Bien que techniquement différents, "Kerberos" et "Kerberos V5" sont souvent utilisés de façon interchangeable dans la documentation Kerberos.

Dans la mythologie grecque, Kerberos (en français Cerbère) était un chien féroce tricéphale qui gardait la porte des Enfers.

keystore Un keystore contient des mots de passe, des phrases de passe, des certificats et d'autres objets d'authentification pour l'extraction par des applications. Il peut être spécifique à une technologie, ou à un emplacement utilisé par plusieurs applications.

kvno Numéro de version de la clé. Numéro de série faisant le suivi d'une clé spécifique selon l'ordre dans lequel elle a été générée. Plus le numéro kvno est élevé, plus la clé est récente.

liste de contrôle d'accès (ACL) Une liste de contrôle d'accès (ACL) offre une sécurité des fichiers plus précise que la protection de fichier UNIX conventionnelle. Par exemple, une ACL vous permet d'autoriser l'accès en lecture de groupe à un fichier, tout en autorisant un seul membre de ce groupe à écrire dans le fichier.

MAC 1. Voir MAC.

2. Egalement appelé étiquetage. Dans la terminologie de sécurité gouvernementale, MAC signifie Mandatory Access Control (contrôle d'accès obligatoire). Les étiquettes telles que Top Secret et Confidential sont des exemples de MAC. MAC diffère de DAC (Discretionary Access Control, contrôle d'accès discrétionnaire). Les autorisations UNIX constituent un exemple de DAC.

3. Dans le matériel, il s'agit de l'adresse système unique sur un réseau local (LAN). Si le système est sur un réseau Ethernet, le MAC est l'adresse Ethernet.

MAC MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.

MD5 Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest. Son utilisation a été désapprouvée.

mécanisme 1. Package logiciel spécifiant des techniques cryptographiques pour assurer l'authentification ou la confidentialité des données. Exemples : Kerberos V5, clé publique Diffie-Hellman

2. Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, mise en oeuvre d'un algorithme destiné à un usage particulier. Par exemple, un mécanisme DES appliqué à l'authentification, tel que CKM_DES_MAC, est un mécanisme distinct d'un mécanisme DES appliqué au chiffrement, CKM_DES_CBC_PAD.

Mécanisme de sécurité Voir mécanisme.

minimisation Installation du système d'exploitation minimal nécessaire pour l'exécution du serveur. Tout logiciel n'étant pas directement lié au fonctionnement du serveur n'est pas installé, ou est supprimé après l'installation.

Modèle de privilège Modèle de sécurité plus strict que le modèle superutilisateur sur un système informatique. Dans le modèle de privilège, les processus nécessitent des privilèges pour s'exécuter. L'administration du système peut être divisée en quatre parties discrètes basées sur les privilèges dont les administrateurs disposent dans leurs processus. Des privilèges peuvent être affectés au processus de connexion d'un administrateur, ou des privilèges peuvent être affectés de manière à ne s'appliquer qu'à certaines commandes.

modèle de superutilisateur Modèle de sécurité UNIX standard sur un système informatique. Dans le modèle de superutilisateur, un administrateur dispose d'un contrôle de type tout ou rien sur le système.

En règle générale, pour l'administration de la machine, un utilisateur se connecte en tant que superutilisateur (`root`) et peut effectuer toutes les activités d'administration.

moindre privilège Modèle de sécurité qui octroie à un processus spécifié uniquement un sous-ensemble de pouvoirs de superutilisateur. Le modèle de moindre privilège octroie aux utilisateurs standard les privilèges suffisants pour qu'ils puissent effectuer des tâches d'administration personnelles, telles que le montage de systèmes de fichiers et la modification de l'appartenance des fichiers. Par ailleurs, les processus s'exécutent uniquement avec les privilèges dont ils ont besoin pour terminer la tâche, et non avec tous les pouvoirs du superutilisateur, c'est-à-dire, tous les privilèges. Les dommages causés par les erreurs de programmation, comme les débordements de la mémoire tampon, peuvent être limités à un utilisateur non root, qui n'a pas accès à des fonctions essentielles comme la lecture ou l'écriture de fichiers système protégés ou l'arrêt de la machine.

Moteur d'analyse Application tierce, résidant sur un hôte externe, qui examine un fichier à la recherche de virus connus.

Nom de principal 1. Le nom d'un principal, au format *primary/instance@REALM*. Voir également instance, primaire, domaine (realm).

2. (RPCSEC_GSS API) Voir principal de client, principal de serveur.

NTP Network Time Protocol. Logiciel de l'Université de l'Etat du Delaware qui vous permet de gérer avec précision la synchronisation de l'heure ou de l'horloge réseau, ou les deux, dans un environnement réseau. Vous pouvez utiliser le protocole NTP pour préserver l'écart d'horloge dans un environnement Kerberos. Voir également écart d'horloge.

Objet public Fichier appartenant à l'utilisateur `root` et lisible par tout le monde, tel que n'importe quel fichier du répertoire `/etc`.

PAM Module d'authentification enfichable (Pluggable Authentication Module). Structure permettant d'utiliser plusieurs mécanismes d'authentification sans recompilation des services recourant à ces mécanismes. PAM permet l'initialisation de la session SEAM au moment de son ouverture

phrase de passe Phrase utilisée pour vérifier qu'une clé privée a été créée par l'utilisateur de la phrase de passe. Une bonne phrase de passe contient 10 à 30 caractères alphanumériques et évite les noms et proses simples. Vous êtes invité à saisir la phrase de passe pour authentifier l'utilisation de la clé privée pour chiffrer et déchiffrer les communications.

piste de vérification Collection de tous les fichiers d'audit provenant de tous les hôtes.

Politique d'audit Paramètres globaux et par utilisateur qui déterminent les événements d'audit enregistrés. Les paramètres globaux s'appliquant au service d'audit déterminent généralement les informations facultatives à inclure dans la piste d'audit. Deux paramètres, `cnt` et `ahlt`, affectent le fonctionnement du système lorsque la file d'attente de l'audit est pleine. Par exemple, la stratégie d'audit peut exiger qu'un numéro de séquence fasse partie de chaque enregistrement d'audit.

primaire Première partie du nom d'un nom de principal. Voir également instance, Nom de principal, domaine (realm).

principal 1. Client/utilisateur dont le nom est unique ou instance de serveur/service participant à une communication en réseau. Les transactions Kerberos impliquent des interactions entre des principaux (principaux de service et d'utilisateur) ou entre des principaux et des KDC. En d'autres termes, un principal est une entité unique à laquelle Kerberos peut attribuer des tickets. Voir également Nom de principal, principal de service, Principal d'utilisateur.

2. (RPCSEC_GSS API) Voir principal de client, principal de serveur.

Principal admin Principal d'utilisateur dont le nom est au format *nom_utilisateur*`/admin` (comme dans `jdoe/admin`). Un principal admin peut disposer de davantage de privilèges (de modification de stratégies par exemple) qu'un principal d'utilisateur standard. Voir également Nom de principal et Principal d'utilisateur.

Principal d'utilisateur Principal attribué à un utilisateur particulier. Le nom primaire d'un principal d'utilisateur est un nom d'utilisateur et son instance facultative est un nom utilisé pour décrire l'utilisation prévue des informations d'identification correspondantes (`jdoe` ou `jdoe/admin` par exemple). Egalement appelé instance d'utilisateur. Voir également principal de service.

principal de client (RPCSEC_GSS API) Client (utilisateur ou application) utilisant des services réseau sécurisés RPCSEC_GSS. Les noms de principaux client sont stockés sous forme de structures `rpc_gss_principal_t`.

principal de serveur (RPCSEC_GSS API) Principal fournissant un service. Le principal de serveur est stocké sous forme d'une chaîne de caractères ASCII dont le format est *service*`@`*hôte*. Voir également principal de client.

principal de service Principal assurant l'authentification Kerberos pour un ou plusieurs services. Pour les principaux de service, le nom primaire est un nom de service, tel que `ftp`, et son instance est le nom d'hôte complet du système fournissant le service. Voir également Hôte principal, Principal d'utilisateur.

principe du moindre privilège Voir moindre privilège.

privilège En règle générale, les d'alimentation 1. capable d'effectuer une opération ou sur un système informatique qui se situe au-delà de la puissance de un utilisateur standard. Les privilèges de superutilisateur sont tous les droits octroyés au superutilisateur. Application privilégiée par un utilisateur doté de privilèges ou est un utilisateur ou application qui a reçu des droits supplémentaires.

2. Droit discret dans le cadre d'un processus dans un système Oracle Solaris. Les privilèges offrent un contrôle des processus plus détaillé que `root`. Les privilèges sont définis et appliqués dans le noyau. Les privilèges sont également appelés *privilèges de processus* ou *privilèges*

de noyau. Pour une description complète des privilèges, reportez-vous à la page de manuel `privileges`(5).

Profil de droits On parle aussi de profil. Ensemble de remplacements de sécurité pouvant être affecté à un rôle ou à un utilisateur. Un profil de droits peut se composer d'autorisations, privilèges, de commandes avec des attributs de sécurité et d'autres profils de droits sont appelés les profils supplémentaires.

Profil de droits authentifiés Profil de droits qui nécessite que l'utilisateur ou le rôle qui lui est affecté saisisse un mot de passe avant d'exécuter une opération à partir du profil. Ce comportement est similaire au comportement de `sudo`. La durée de temps pendant laquelle le mot de passe est valide est configurable.

protocole Diffie-Hellman Egalement appelé cryptographie par clé publique. Protocole d'accord de clés cryptographiques asymétriques mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par Kerberos.

QOP Qualité de la protection. Paramètre servant à sélectionner les algorithmes cryptographiques utilisés en association avec le service d'intégrité ou de confidentialité.

RBAC Contrôle d'accès basé sur les rôles, fonction de gestion des droits des utilisateurs d'Oracle Solaris. Reportez - vous à la section droits.

Réauthentification Mot de passe qu'il soit nécessaire de fournir une opération. pour effectuer un ordinateur En règle générale, les opérations `sudo` nécessitent une réauthentification. Les profils de droits peuvent contenir authentifiés des commandes qui nécessitent la réauthentification. Voir Profil de droits authentifiés .

relation Variable ou relation de configuration définie dans les fichiers `kdc.conf` ou `krb5.conf`.

renforcement Modification de la configuration par défaut du système d'exploitation pour supprimer les failles de sécurité inhérentes à l'hôte.

rôle Identité spéciale destinée à l'exécution d'applications privilégiées et ne pouvant être prise que par des utilisateurs assignés.

RSA Méthode permettant d'obtenir des signatures numériques et des systèmes de cryptographie par clé publique. Cette méthode datant de 1978 a été décrite par trois développeurs (Rivest, Shamir et Adleman).

SEAM Nom de produit pour la version initiale de Kerberos sur les systèmes Solaris. Ce produit est à partir de la technologie Kerberos V5 développé au Massachusetts Institute of Technology. SEAM est maintenant appelé le service Kerberos. Il continue d'être légèrement différent de l'version MIT.

Secure Shell, shell sécurisé Un protocole particulier pour une connexion à distance sécurisée et d'autres services de réseau sécurisé via un réseau non sécurisé.

Séparation des tâches Composante de la notion de moindre privilège. La séparation des tâches permet d'empêcher un utilisateur d'exécuter ou d'approuver les opérations terminant une transaction. Par exemple, dans RBAC, vous pouvez séparer la création d'un utilisateur de connexion de l'affectation des remplacements de sécurité. Un rôle crée l'utilisateur. Un autre rôle peut affecter les attributs de sécurité, tels que des profils de droits, des rôles et des privilèges aux utilisateurs existants.

Serveur Principal fournissant une ressource aux clients réseau. Si vous vous connectez par `ssh` au système `central.example.com` par exemple, ce système est le serveur fournissant le service `ssh`. Voir également principal de service.

serveur d'application réseau Serveur fournissant une application réseau, telle que `ftp`. Un domaine peut contenir plusieurs serveurs d'application réseau.

Serveur d'applications Voir serveur d'application réseau.

service 1. Ressource fournie aux clients du réseau, souvent par plusieurs serveurs. Si vous vous connectez par `rlogin` à la machine `central.example.com` par exemple, cette machine est le serveur fournissant le service `rlogin`.

2. Service de sécurité (d'intégrité ou de confidentialité) fournissant un niveau de protection supérieur à l'authentification. Voir également intégrité et confidentialité.

service de sécurité Voir service.

SHA1 Secure Hashing Algorithm, algorithme de hachage sécurisé. L'algorithme s'applique à toute longueur d'entrée inférieure à 2^{64} afin d'obtenir une synthèse des messages. L'algorithme SHA1 sert d'entrée à DSA.

Shell de profil Dans la gestion des droits, shell permettant à un rôle (ou un utilisateur) d'exécuter, à partir de la ligne de commande, toutes les applications privilégiées affectées au profil de droits du rôle. Les versions du shell de profil correspondent aux shells disponibles sur le système, comme la version `pfbash` de `bash`

stratégie En règle générale, plan ou ensemble d'actions qui influence ou détermine les décisions et actions. Pour les systèmes informatiques, la stratégie fait généralement référence à la stratégie de sécurité. La stratégie de sécurité de votre site constitue un ensemble de règles qui définissent la sensibilité des informations traitées et les mesures prises pour protéger les informations contre tout accès non autorisé. Par exemple, la stratégie de sécurité peut exiger que les systèmes soient audités, que les périphériques soient protégés par des privilèges et que les mots de passe soient modifiés toutes les six semaines.

Pour l'implémentation des stratégies dans des zones spécifiques du Oracle Solaris (SE), voir Politique d'audit, stratégie dans la structure cryptographique, stratégie de périphériques, Stratégie Kerberos, stratégie de mot de passe et Stratégie de droits.

stratégie dans la structure cryptographique Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, la stratégie correspond à la désactivation de mécanismes de chiffrement existants. Les mécanismes ne peuvent ensuite plus être utilisés. La stratégie de la structure cryptographique peut empêcher l'utilisation d'un mécanisme particulier tel que `CKM_DES_CBC` provenant d'un fournisseur tel que DES.

Stratégie de droits Stratégie de sécurité associée à une commande. Actuellement, `solaris` est la stratégie valide pour Oracle Solaris. La stratégie `solaris` reconnaît les privilèges et la stratégie de privilège étendue, les autorisations et les attributs de sécurité de `setuid`.

stratégie de mot de passe Algorithmes de chiffrement pouvant être utilisés pour générer des mots de passe. Peut également faire référence à des questions plus générales concernant les mots de passe, telles que la fréquence à laquelle le mot de passe doit être modifié, le nombre de tentatives autorisées de saisie d'un mot de passe et d'autres considérations relatives à la sécurité. La stratégie de sécurité requiert des mots de passe. La stratégie de mot de passe peut requérir des mots de passe chiffrés avec l'algorithme AES, et imposer d'autres exigences relatives à la force des mots de passe.

stratégie de périphériques Protection d'un périphérique au niveau du noyau. La stratégie de périphériques repose sur deux jeux de privilèges pour un périphérique. Un jeu de privilèges contrôle l'accès en lecture au périphérique. Le deuxième jeu de privilèges contrôle l'accès en écriture sur le périphérique. Voir également stratégie.

stratégie de sécurité Voir stratégie.

Stratégie Kerberos Ensemble de règles régissant l'utilisation des mots de passe dans le service Kerberos. Les stratégies peuvent réguler les accès des principaux ou des paramètres de ticket, tels que la durée de vie.

stratégie pour technologies à clé publique Dans la structure de gestion des clés (KMF), la stratégie correspond à la gestion de l'utilisation des certificats. La base de données de stratégies KMF peut définir des contraintes s'appliquant à l'utilisation des clés et des certificats gérés par la bibliothèque KMF.

Stratégie RBAC Reportez-vous à la section Stratégie de droits.

stratégies de réseau Paramètres configurés par les utilitaires réseau pour protéger le trafic réseau. Pour plus d'informations sur la sécurité réseau, reportez-vous à la section “ Sécurisation du réseau dans Oracle Solaris 11.2 ”.

synthèse Voir Synthèse de message.

Synthèse de message Valeur de hachage calculée à partir d'un message. La valeur de hachage identifie le message de manière presque unique. Une synthèse permet de vérifier l'intégrité d'un fichier.

TGS Service d'octroi de tickets (Ticket-Granting Service) Partie du KDC responsable de l'émission des tickets.

TGT Ticket d'octroi de tickets (Ticket-Granting Ticket) Ticket émis par le KDC, permettant au client de demander des tickets pour d'autres services.

ticket Paquet d'informations servant à transmettre en toute sécurité l'identité d'un utilisateur à un serveur ou un service. Un ticket n'est valable que pour un client et un service particulier sur un serveur spécifique. Il contient le nom de principal du service, le nom de principal de l'utilisateur, l'adresse IP de l'hôte de l'utilisateur, un horodatage et une valeur définissant la durée de vie du ticket. La création d'un ticket s'effectue à l'aide d'une clé de session aléatoire utilisée par le client et le service. Une fois le ticket créé, il peut être réutilisé jusqu'à son expiration. Un ticket sert uniquement à authentifier un client lorsqu'il est présenté avec un nouvel authentificateur. Voir également Authentificateur, credential, service, Clé de session.

ticket initial Ticket émis de manière directe, et pas à partir d'un ticket d'octroi de tickets. Certains services, tels que les applications modifiant les mots de passe, peuvent nécessiter des tickets marqués comme étant `initiaux` afin d'assurer que le client peut démontrer qu'il connait sa clé secrète. Cette garantie est importante car un ticket initial indique que le client s'est récemment authentifié et ne dépend pas d'un ticket d'octroi de tickets qui peut exister depuis un certain temps.

ticket non valide Ticket postdaté n'étant pas encore utilisable. Un ticket non valide est rejeté par un serveur d'application jusqu'à ce qu'il soit validé. Pour être validé, un ticket non valide doit être présenté au KDC par le client dans une demande de TGS, avec l'indicateur `VALIDATE`, après l'heure de début. Voir également Ticket postdaté.

Ticket postdaté Un ticket postdaté ne devient valide qu'un certain temps après sa création. Par exemple, un tel ticket peut être utile avec les tâches exécutées par lots la nuit car le ticket, s'il est volé, ne peut pas être utilisé tant que l'exécution de ces tâches n'a pas eu lieu. Lorsqu'un ticket postdaté est émis, il est émis en tant que `non valide` et le reste jusqu'à ce que a) son heure de début soit dépassée et b) le client demande la validation par le KDC. Un ticket postdaté est normalement valide jusqu'à l'heure d'expiration du ticket d'octroi de tickets. Toutefois, si le ticket postdaté est marqué comme `renouvelable`, sa durée de vie est normalement égale à la durée de vie entière du ticket d'octroi de tickets. Voir également ticket non valide, Ticket renouvelable.

Ticket renouvelable Etant donné que tout ticket dont la durée de vie est très longue peut présenter un risque pour la sécurité, les tickets peuvent être conçus pour être `renouvelables`. Un ticket renouvelable possède deux moments d'expiration : a) l'heure à laquelle l'instance courante du ticket expire et b) la durée de vie maximale de tout ticket. Si un client souhaite continuer à utiliser un ticket, il peut le renouveler avant sa première expiration. Par exemple, un ticket peut être valide pendant une heure, et tous les tickets ont une durée de vie maximale de dix heures. Si le client détenant le ticket souhaite le conserver plus d'une heure, il doit le renouveler. Lorsqu'un ticket atteint sa durée de vie maximale, celui-ci expire automatiquement et ne peut pas être renouvelé.

Ticket transmissible Ticket pouvant être utilisé par un client pour demander un ticket sur un hôte distant sans devoir se soumettre au processus complet d'authentification sur l'hôte concerné. Par exemple, si l'utilisateur `david` obtient un ticket transmissible sur la machine de l'utilisatrice `jennifer`, il peut se connecter à sa propre machine sans devoir demander un nouveau ticket (et donc s'authentifier à nouveau). Voir également Ticket utilisable avec proxy.

Ticket utilisable avec proxy
Ticket pouvant être utilisé par un service pour le compte d'un client afin d'effectuer une opération pour ce dernier. On dit alors que le service agit en tant que proxy du client. Grâce à ce ticket, le service peut prendre l'identité du client. Le service peut utiliser un tel ticket afin d'obtenir un ticket de service d'un autre service, mais non un ticket d'octroi de tickets. La différence entre un ticket utilisable avec proxy et un ticket transmissible réside dans le fait que le premier n'est valide que pour une seule opération. Voir également Ticket transmissible.

Touche
1. En règle générale, l'un des deux principaux types de clés :

- *clé symétrique* : clé de chiffrement identique à la clé de déchiffrement. Les clés symétriques sont utilisées pour chiffrer des fichiers.
- *clé asymétrique* ou *clé publique* : clé utilisée dans les algorithmes à clé publique, tels que Diffie-Hellman ou RSA. Les clés publiques contiennent une clé privée, connue uniquement d'un utilisateur, une clé publique utilisée par le serveur ou des ressources générales, et une paire de clés publique-privée combinant les deux. Une clé privée est également qualifiée de clé *secrète*. La clé publique est également qualifiée de clé *partagée* ou *commune*.

2. Entrée (nom de principal) dans un fichier keytab. Voir également fichier keytab.

3. Dans Kerberos, clé de chiffrement dont il existe trois types :

- *Clé privée* : clé de chiffrement partagée par un principal et le KDC, et distribuée en dehors des limites du système. Voir également Clé privée.
- *Clé de service* : clé remplissant la même fonction que la clé privée, mais utilisée par des serveurs et des services. Voir également clé de service.
- *Clé de session* : clé de chiffrement temporaire utilisée entre deux principaux, avec une durée de vie limitée à la durée d'une seule session de connexion. Voir également Clé de session.

Utilisateur privilégié
Droits un utilisateur disposant des droits d'utilisateur standard au-delà de la sur un système informatique. Voir également Utilisateurs de confiance.

Utilisateurs de confiance
Que vous avez décidé des utilisateurs avec lesquels vous pouvez effectuer des tâches d'administration à un certain niveau d'approbation. Les connexions aux fins en général, les administrateurs d'abord créer et affecter des utilisateurs de confiance des droits d'administration qui correspondent au niveau de confiance des utilisateurs et leur capacité. Ces utilisateurs aider à configurer et de tenir à jour le système. Egalement appelés *utilisateurs privilégiés*.

variante
Historiquement, la *variante de sécurité* et la *variante d'authentification* désignaient la même chose, lorsqu'une variante indiquait un type d'authentification (AUTH_UNIX, AUTH_DES, AUTH_KERB). RPCSEC_GSS est également une variante de sécurité, même s'il permet d'assurer des services d'intégrité et de confidentialité, en plus de l'authentification.

Variante de sécurité
Voir variante.

VPN
Réseau privé virtuel assurant une communication sécurisée en utilisant les mécanismes de chiffrement et de mise en tunnel pour connecter les utilisateurs via un réseau public.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Z