Guide d'administration système : Services de sécurité

Référence : E23285
Août 2011

ORACLE

Copyright © 2002, 2011, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

111013@25097

Table des matières

Préface

Le *System Administration Guide: Security Services* est l'un des volumes traitant de l'administration du système d'exploitation Oracle Solaris (Oracle Solaris). Ce manuel suppose que vous avez déjà installé la version actuelle et configuré le logiciel réseau que vous envisagez d'utiliser. Le système d'exploitation Oracle Solaris fait partie de la famille de produits Oracle Solaris qui comprend de nombreuses fonctionnalités, telles qu'Oracle Solaris Secure Shell.

Remarque – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Pour connaître les systèmes pris en charge, reportez-vous aux *Oracle Solaris OS: Hardware Compatibility Lists*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Dans ce document, les termes relatifs à x86 ont la signification suivante :

- x64 désigne la famille des produits compatibles x86 64 et 32 bits.
- x64 concerne spécifiquement les UC compatibles x86 64 bits.
- `32-bit x86` renvoie aux informations 32 bits spécifiques relatives aux systèmes x86.

Pour connaître les systèmes pris en charge, reportez-vous aux listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*.

Utilisateurs de ce manuel

Ce manuel s'adresse à ceux qui ont la charge d'administrer un ou plusieurs systèmes fonctionnant sous Oracle Solaris. Pour utiliser ce manuel, vous devez disposer d'au moins deux ans d'expérience en administration de systèmes UNIX. Les cours de formation en administration de systèmes UNIX peuvent se révéler utiles.

Organisation des guides d'administration système

La liste des différents sujets traités par les guides d'administration système est la suivante.

Titre du manuel	Sujets
Guide d'administration système : administration de base	Comptes et groupes d'utilisateur, prise en charge de serveur et de client, arrêt et initialisation d'un système et gestion des services
Guide d'administration système : Administration avancée	Terminaux et modems, ressources système (quotas d'utilisation de disque, comptabilisation et crontabs), processus système et dépannage du logiciel Oracle Solaris
System Administration Guide: Devices and File Systems	Supports amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
Guide d'administration système : services IP	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP, IP mobile, multiacheminement sur réseau IP (IPMP) et IPQoS
Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)	Services d'annuaire et de nommage DNS, NIS et LDAP, et transition de NIS à LDAP et de NIS+ à LDAP
System Administration Guide: Naming and Directory Services (NIS+)	Services d'annuaire et de nommage NIS+
Guide d'administration système : Services réseau	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
System Administration Guide: Printing	Tâches et sections concernant l'impression, l'utilisation des services, les outils, protocoles et technologies permettant de configurer et de gérer les imprimantes et services d'impression
Guide d'administration système : services de sécurité	Audit, gestion des périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique Oracle Solaris, privilèges, RBAC, SASL et shell sécurisé Oracle Solaris
Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris	Gestion des ressources pour les projets et les tâches, comptabilisation étendue, contrôles de ressources, ordonnanceur FSS, contrôle de la mémoire physique à l'aide du démon d'allocation restrictive des ressources (rcapd) et pools de ressources ; virtualisation au moyen de la technologie de partitionnement du logiciel Solaris Zones et des zones marquées `lx`
Guide d'administration Oracle Solaris ZFS	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger des fichiers ZFS, utilisation de Solaris ZFS sur un système Oracle Solaris avec des zones installées, volumes émulés et dépannage et récupération de données

Titre du manuel	Sujets
Procédures de l'administrateur Oracle Solaris Trusted Extensions	Administration système spécifique aux fonctionnalités d'extension sécurisée d'Oracle Solaris
Guide de configuration d'Oracle Solaris Trusted Extensions	À partir de la version Solaris 10 5/08, ce guide décrit la planification, l'activation et la configuration initiale de la fonction d'extension sécurisée d'Oracle Solaris.

Références connexes aux sites Web de logiciels tiers

Des URL de sites tiers, qui renvoient à des informations complémentaires connexes, sont référencés dans ce document.

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

Accès au support technique Oracle

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

Conventions typographiques

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

TABLEAU P–1 Conventions typographiques

Type de caractères	Signification	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`

TABLEAU P–1 Conventions typographiques *(Suite)*

Type de caractères	Signification	Exemple
AaBbCc123	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

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

TABLEAU P–2 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour superutilisateur	`#`
C shell	`machine_name%`
C shell pour superutilisateur	`machine_name#`

PARTIE I

Présentation de la sécurité

Ce manuel traite des fonctions qui renforcent la sécurité dans le système d'exploitation Oracle Solaris. Ce manuel s'adresse aux administrateurs système et aux utilisateurs de ces fonctions de sécurité. Le Chapitre 1, “Services de sécurité (présentation) ” présente les sujets abordés dans le manuel.

◆ ◆ ◆ CHAPITRE 1

Services de sécurité (présentation)

Pour préserver la sécurité du système d'exploitation Oracle Solaris (SE Oracle Solaris), le logiciel propose les fonctionnalités suivantes :

- "Sécurité du système " à la page 32 : la possibilité d'empêcher les intrusions, de protéger les ressources de la machine et les périphériques contre les utilisations inappropriées et de protéger les fichiers contre les modifications malveillantes ou involontaires par des utilisateurs ou des intrus.

  Pour une discussion sur la sécurité du système local, reportez-vous au Chapitre 2, "Gestion de la sécurité de la machine (présentation)".
- "Services cryptographiques" à la page 33 : capacité de brouiller les données afin que seul l'expéditeur et le destinataire désigné puissent lire le contenu, et de gérer les fournisseurs cryptographiques et les objets de clé publique
- "Services d'authentification " à la page 34 : capacité d'identifier un utilisateur de manière sécurisée, ce qui nécessite le nom de l'utilisateur et une forme quelconque de preuve, en général un mot de passe
- "Authentification avec le chiffrement" à la page 35 : capacité de s'assurer que les parties authentifiées peuvent communiquer sans interception, modification ou usurpation d'identité
- "Audit" à la page 35 : capacité d'identifier l'origine des modifications de sécurité apportées au système, y compris l'accès aux fichiers, les appels système associés à la sécurité, et les échecs d'authentification
- "Stratégie de sécurité" à la page 35 : conception et mise en œuvre des directives de sécurité pour un système ou un réseau de systèmes

Sécurité du système

La sécurité du système permet de s'assurer que les ressources du système sont correctement utilisées. Des contrôles d'accès permettent de limiter l'accès aux ressources du système à des utilisateurs autorisés. Les fonctions du SE Oracle Solaris pour la sécurité du système et le contrôle de l'accès sont les suivantes :

- **Outils d'administration de connexion** : commandes de surveillance et de contrôle de la capacité d'un utilisateur à se connecter. Reportez-vous à la section "Sécurisation des connexions et des mots de passe (liste des tâches)" à la page 64.
- **Hardware access** : commandes de limitation de l'accès à la PROM et de restriction des utilisateurs autorisés à démarrer le système. Reportez-vous à la section "SPARC : Contrôle de l'accès au matériel système (liste des tâches) " à la page 79.
- **Resource access** : outils et stratégies permettant d'optimiser l'utilisation appropriée des ressources de la machine tout en minimisant l'utilisation inappropriée de ces ressources. Reportez-vous à la section "Contrôle de l'accès aux ressources de la machine" à la page 50.
- **Contrôle d'accès basé sur les rôles (RBAC)** : architecture permettant de créer des comptes utilisateur restreints spécifiques, qui sont autorisés à effectuer des tâches d'administration. Reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186.
- **Privilèges** : droits discrets sur les processus pour effectuer des opérations. Ces droits sur les processus sont appliqués dans le noyau. Reportez-vous à la section "Privilèges (présentation)" à la page 197.
- **Gestion des périphériques** : la *stratégie* relative aux périphériques protège en outre les périphériques qui sont déjà protégés par des autorisations UNIX. L'*allocation* des périphériques contrôle l'accès aux périphériques, tels qu'un microphone ou une unité de CD-ROM. Lors de l'annulation de l'allocation, les scripts de nettoyage de périphérique peuvent ensuite effacer toutes les données du périphérique. Reportez-vous à la section "Contrôle de l'accès aux périphériques " à la page 47.
- **Outil de rapport d'audit de base (BART)** : instantané, appelé *manifeste*, des attributs des fichiers d'un système. En comparant les manifestes sur l'ensemble des systèmes ou sur un système dans le temps, les modifications apportées aux fichiers peuvent être surveillées pour réduire les risques de sécurité. Reportez-vous au Chapitre 5, "Utilisation de l'outil de génération de rapports d'audit de base (tâches) ".
- **Autorisations de fichier** : attributs d'un fichier ou d'un répertoire. Les autorisations limitent les utilisateurs et les groupes qui sont autorisés à lire, écrire ou exécuter un fichier, ou effectuer une recherche dans un répertoire. Reportez-vous au Chapitre 6, "Contrôle de l'accès aux fichiers (tâches)".
- **Scripts d'amélioration de la sécurité** : à l'aide des scripts, vous pouvez modifier de nombreux fichiers et paramètres système pour réduire les risques de sécurité. Reportez-vous au Chapitre 7, "Utilisation d'Automated Security Enhancement Tool (Tâches)".

Services cryptographiques

La cryptographie est la science du chiffrement et du déchiffrement des données. La cryptographie est utilisée pour assurer l'intégrité, la confidentialité et l'authenticité des données. L'intégrité signifie que les données n'ont pas été modifiées. La confidentialité signifie que les données ne sont pas accessibles en lecture par d'autres utilisateurs. L'authenticité des données signifie que ce qui a été reçu est ce qui a été envoyé. L'authentification utilisateur signifie que l'utilisateur a fourni une ou plusieurs preuves de son identité. Les mécanismes d'authentification vérifient mathématiquement la source de données ou la preuve de l'identité. Les mécanismes de chiffrement brouillent les données afin que les données ne soient pas lisibles par un observateur. Les services cryptographiques fournissent des mécanismes d'authentification et de chiffrement aux applications et aux utilisateurs.

Les algorithmes cryptographiques utilisent le hachage, le chaînage et d'autres techniques mathématiques pour créer des chiffrements difficiles à déchiffrer. Les mécanismes d'authentification nécessitent que l'expéditeur et le destinataire calculent un nombre identique à partir des données. Les mécanismes de chiffrement s'appuient sur le partage par l'expéditeur et le destinataire des informations sur la méthode de chiffrement. Ces informations permettent uniquement au destinataire et à l'expéditeur de décrypter le message. Oracle Solaris fournit une structure cryptographique centralisée et offre des mécanismes de chiffrement qui sont liés à des applications particulières.

- **Structure cryptographique Oracle Solaris** : structure centrale des services cryptographiques pour les consommateurs au niveau du noyau et au niveau de l'utilisateur, qui est basée sur les normes suivantes : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). Les utilisations comprennent les mots de passe, IPsec et des applications tierces. La structure centralise les sources matérielles et logicielles pour le chiffrement. La bibliothèque PKCS 11 fournit une API pour les développeurs tiers pour la connexion de la cryptographie requise pour leurs applications. Reportez-vous au Chapitre 13, “Structure cryptographique Oracle Solaris (présentation)”.
- **Mécanismes de chiffrement par application** :
  - Pour l'utilisation de DES dans l'appel de procédure à distance sécurisé, reportez-vous à la section “Présentation du RPC sécurisé” à la page 327.
  - Pour l'utilisation de DES, 3DES, AES et ARCFOUR dans le service Kerberos, reportez-vous au Chapitre 21, “Introduction au service Kerberos”.
  - Pour l'utilisation de RSA, DSA et de chiffrement tels que Blowfish dans Secure Shell, reportez-vous au Chapitre 19, “Utilisation d'Oracle Solaris Secure Shell (tâches)”.
  - Pour l'utilisation d'algorithmes de chiffrement dans les mots de passe, consultez la section “Modification de l'algorithme de mot de passe (liste des tâches) ” à la page 72.

À partir de la version Solaris 10 8/07, la structure de gestion des clés (KMF) constitue un utilitaire central permettant de gérer les objets de clé publique, y compris les stratégies, les clés et les certificats. KMF gère ces objets pour les technologies à clé publique OpenSSL, NSS et PKCS 11. Reportez-vous au Chapitre 15, “Structure de gestion des clés Oracle Solaris”.

Services d'authentification

L'authentification est un mécanisme qui identifie un utilisateur ou un service en fonction de critères prédéfinis. Les services d'authentification vont de simples paires nom-mot de passe à des systèmes de stimulation-réponse, tels que les cartes à jeton et la biométrie. Les mécanismes d'authentification forte reposent sur l'indication par un utilisateur d'informations connues de lui seul et sur un objet qui peut être vérifié. Un nom d'utilisateur est un exemple d'information que la personne connaît. Une carte à puce ou une empreinte digitale, par exemple, peut être vérifiée. Les fonctionnalités d'Oracle Solaris pour l'authentification sont les suivantes :

- **Appel de procédure à distance sécurisé** : mécanisme d'authentification qui utilise le protocole Diffie-Hellman pour protéger les montages NFS et un service de nommage, tel que NIS ou NIS+. Reportez-vous à la section "Présentation du RPC sécurisé" à la page 327.
- **Module d'authentification enfichable (PAM)** : une structure qui permet à diverses technologies d'authentification d'être connectées à un service d'entrée système sans recompiler le service. Certains services d'entrée système comprennent `login` et `ftp`. Reportez-vous au Chapitre 17, "Utilisation de PAM".
- **SASL (Simple Authentication and Security Layer)** : structure qui fournit des services d'authentification et de sécurité aux protocoles de réseau. Reportez-vous au Chapitre 18, "Utilisation de SASL".
- **Secure Shell** : protocole de connexion et de transmission à distance qui chiffre les communications sur un réseau non sécurisé. Reportez-vous au Chapitre 19, "Utilisation d'Oracle Solaris Secure Shell (tâches)".
- **Service Kerberos** : architecture client-serveur qui fournit le chiffrement avec authentification. Reportez-vous au Chapitre 21, "Introduction au service Kerberos".
- **Carte à puce Solaris** Une carte en plastique dotée d'un microprocesseur et d'une mémoire qui permettent à un lecteur de carte d'accéder aux systèmes. Reportez-vous au *Solaris Smartcard Administration Guide*.

Authentification avec le chiffrement

L'authentification avec le chiffrement est la base de la communication sécurisée. L'authentification permet de s'assurer que la source et la destination sont les parties prévues. Le chiffrement code la communication à la source et décode la communication à la destination. Le chiffrement empêche les intrus de lire les transmissions qu'ils ont pu intercepter. Les fonctionnalités d'Oracle Solaris pour la communication sécurisée incluent les éléments suivants :

- **Secure Shell** : protocole de protection des transmissions de données et des sessions réseau utilisateur interactives contre les écoutes, le détournement de session et les attaques Man-in-the-middle. L'authentification forte est fournie par l'intermédiaire de la cryptographie par clé publique. Les services X Window et d'autres services réseau peuvent être délivrés par tunnel de manière sécurisée sur les connexions Secure Shell pour ajouter un niveau de protection supplémentaire. Reportez-vous au Chapitre 19, “Utilisation d'Oracle Solaris Secure Shell (tâches)”.
- **Service Kerberos** : architecture client-serveur qui assure l'authentification avec le chiffrement. Reportez-vous au Chapitre 21, “Introduction au service Kerberos”.
- **Architecture IPsec (Internet Protocol Security Architecture)** : architecture qui fournit une protection des datagrammes IP. Les protections comprennent la confidentialité, un niveau élevé d'intégrité des données, l'authentification des données et l'intégrité des séquences partielles. Reportez-vous au Chapitre 19, “Architecture IPsec (présentation)” du *Guide d'administration système : services IP*.

Audit

L'audit est un concept fondamental de la sécurité des systèmes et de la maintenance. L'audit est le processus d'analyse de l'historique des actions et des événements sur un système afin de déterminer ce qui s'est passé. L'historique est conservé dans un journal répertoriant ce qui a été effectué, quand, par qui, et ce qui a été affecté. Reportez-vous au Chapitre 28, “Audit Oracle Solaris (présentation) ”.

Stratégie de sécurité

La stratégie de sécurité des expressions, ou stratégie, est utilisée dans l'ensemble de ce manuel pour faire référence aux directives sur la sécurité d'une entreprise. 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. Les technologies de sécurité telles que Secure Shell, l'authentification, RBAC, l'autorisation, les privilèges et le contrôle des ressources fournissent des mesures de protection des informations.

Certaines technologies de sécurité utilisent également le mot stratégie lors de la description des aspects spécifiques de leur mise en œuvre. Par exemple, Oracle Solaris utilise des options de

stratégie d'audit pour configurer certains aspects de la stratégie d'audit. Le tableau ci-dessous répertorie des entrées de glossaire, des pages de manuel et des informations sur les fonctions qui utilisent le mot stratégie pour décrire des aspects spécifiques de leur mise en œuvre.

TABLEAU 1–1 Utilisation de stratégies dans le SE Oracle Solaris

Définition du glossaire	Pages de manuel sélectionnées	Informations supplémentaires
stratégie d'audit	`audit_control`(4), `audit_user`(4), `auditconfig`(1M)	Chapitre 28, "Audit Oracle Solaris (présentation) "
stratégie dans la structure cryptographique	`cryptoadm`(1M)	Chapitre 13, "Structure cryptographique Oracle Solaris (présentation)"
stratégie de périphériques	`getdevpolicy`(1M)	"Contrôle de l'accès aux périphériques " à la page 47
stratégie Kerberos	`krb5.conf`(4)	Chapitre 25, "Administration des principaux et des stratégies Kerberos (tâches) "
stratégies de réseau	`ipfilter`(5), `ifconfig`(1M), `ike.config`(4), `ipsecconf`(1M), `routeadm`(1M)	Partie IV, "IPsec" du *Guide d'administration système : services IP*
stratégie de mot de passe	`passwd`(1), `nsswitch.conf`(4), `crypt.conf`(4), `policy.conf`(4)	"Gestion du contrôle de connexion " à la page 41
stratégie pour technologies à clé publique	`kmfcfg`(1)	Chapitre 15, "Structure de gestion des clés Oracle Solaris"
stratégie RBAC	`rbac`(5). `policy.conf`(4)	"Fichier `policy.conf`" à la page 254

PARTIE II

Sécurité du système, des fichiers et des périphériques

Cette section couvre la sécurité qui peut être configurée sur un système autonome. Les chapitres traitent de la planification, de la surveillance et du contrôle de l'accès au disque, aux fichiers et aux périphériques.

◆ ◆ ◆ CHAPITRE 2

Gestion de la sécurité de la machine (présentation)

Le maintien de la sécurité des informations d'une machine constitue une responsabilité importante de l'administration du système. Ce chapitre fournit des informations de présentation sur la gestion de la sécurité de la machine.

Vous trouverez ci-après une liste des informations de présentation contenues dans ce chapitre.

Améliorations apportées à la sécurité de la machine dans la version Solaris10

Depuis la version Solaris 9, les fonctionnalités suivantes ont été introduites pour améliorer la sécurité du système :

- Le chiffrement de mot de passe fort est disponible et configurable. Pour plus d'informations, reportez-vous à la section "Chiffrement du mot de passe " à la page 43.
- La stratégie de périphériques est appliquée avec des privilèges. Pour plus d'informations, reportez-vous à la section "Stratégie de périphériques (présentation) " à la page 48.

  Pour l'allocation des périphériques, le répertoire `/etc/security/dev` peut ne pas être pris en charge dans les versions futures d'Oracle Solaris.
- L'outil de génération de rapports d'audit de base (BART) permet de surveiller l'authenticité des fichiers sur votre système. Pour plus d'informations, reportez-vous au Chapitre 5, "Utilisation de l'outil de génération de rapports d'audit de base (tâches) ".

- Les fichiers peuvent être protégés par un chiffrement fort. Pour plus d'informations, reportez-vous à la section "Protection des fichiers par chiffrement" à la page 55.
- Les privilèges mettent en œuvre les droits de processus au niveau du noyau. Pour plus d'informations, reportez-vous à la section "Privilèges (présentation)" à la page 197.
- La structure cryptographique centralise des services cryptographiques pour fournisseurs et consommateurs. Pour plus d'informations, reportez-vous au Chapitre 13, "Structure cryptographique Oracle Solaris (présentation)".
- La structure PAM offre des fonctionnalités pour de nombreux programmes, tels que Secure Shell. Pour plus d'informations, reportez-vous à la section "Modifications apportées à PAM pour la version de Solaris10 " à la page 341.
- La gestion des zones et ressources d'Oracle Solaris contrôle l'accès aux ressources de la machine. Pour plus d'informations, reportez-vous à la section *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Contrôle de l'accès à un système informatique

Dans le lieu de travail, 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 avez besoin de 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 est le contrôle de l'accès à votre système.

Vous pouvez contrôler et surveiller l'accès au système en effectuant les opérations 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 "Mot de passe obligatoire pour l'accès au matériel" à la page 79.

Gestion du contrôle de connexion

Vous devez également empêcher toute connexion non autorisée à un système ou au réseau, par le biais de l'affectation d'un mot de passe ou du contrôle de connexion. Tous les comptes sur un système doivent disposer d'un mot de passe. Un mot de passe est un mécanisme d'authentification simple. 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 nommage approprié ou la base de données du service d'annuaire en fonction d'informations répertoriées dans le fichier `/etc/nsswitch.conf`. Ce fichier peut inclure les entrées suivantes :

- `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
- `nisplus` : désigne la base de données NIS+ sur le serveur root NIS+

Pour une description du fichier `nsswitch.conf`, reportez-vous à la page de manuel `nsswitch.conf(4)`. Pour plus d'informations sur les services de nommage et les services d'annuaire, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* ou au *System Administration Guide: Naming and Directory Services (NIS+)* .

La commande `login` vérifie le nom d'utilisateur et le mot de passe indiqués par l'utilisateur. Si le nom d'utilisateur ne figure pas dans le fichier de 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, reportez-vous au Chapitre 17, "Utilisation de PAM".

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 58.

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 gardés secrets. Les mots de passe ne doivent être connus que des utilisateurs. Vous devez demander à vos utilisateurs de choisir leurs mots de passe avec soin. Les utilisateurs doivent modifier leurs mots de passe 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 des informations plus détaillées sur la gestion des mots de passe, reportez-vous au Chapitre 4, “Gestion des comptes utilisateur et des groupes (présentation) ” du *Guide d'administration système : administration de base* et à la page de manuel `passwd(1)`.

Mots de passe locaux

Si votre réseau utilise des fichiers locaux pour authentifier des 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 d'autres informations sont conservées dans le fichier `/etc/passwd`. Le mot de passe chiffré lui-même est conservé dans un autre fichier *shadow* appelé `/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 toute personne pouvant se connecter à un système, seul le superutilisateur ou un rôle équivalent 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 et 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.

Si votre réseau utilise NIS+ pour authentifier les utilisateurs, les informations de mot de passe sont conservées dans la base de données NIS+. Les informations dans la base de données NIS+ peuvent être protégées en limitant l'accès aux utilisateurs autorisés uniquement. Vous pouvez utiliser la commande `passwd -r nisplus` pour modifier le mot de passe d'un utilisateur qui est stocké dans une base de données NIS+.

Mots de passe LDAP

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

La stratégie de mot de passe est appliquée sur le Sun Java System Directory Server. Plus précisément, le module `pam_ldap` du client suit les contrôles de stratégie de mot de passe mis en œuvre sur le Sun Java System Directory Server. Pour plus d'informations, reportez-vous à la section "Modèle de sécurité des services de nommage LDAP" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et 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, MD5 et SHA assurent un chiffrement de mot de passe plus robuste que l'algorithme UNIX.

Identificateurs d'algorithmes de mot de passe

Vous spécifiez la configuration des algorithmes pour votre site 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`.

TABLEAU 2–1 Algorithmes de chiffrement de mot de passe

Identificateur	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 sur les systèmes BSD.	`crypt_bsdbf(5)`
`md5`	Algorithme Sun MD5 considéré comme plus fort 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.	`crypt_sha256(5)`
`6`	Algorithme SHA512.	`crypt_sha512(5)`
`__unix__`	Algorithme de chiffrement UNIX conventionnel. Cet algorithme est le module par défaut dans le fichier `policy.conf`.	`crypt_unix(5)`

Configuration d'algorithmes dans le fichier policy.conf

L'exemple suivant montre la configuration d'algorithmes par défaut dans le fichier `policy.conf` :

```
#
...
# 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 Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
...
```

Lorsque 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 leurs mots 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=1` . Le tableau ci-dessous montre quel algorithme sera utilisé pour générer le mot de passe chiffré.

Identificateur = Algorithme de mot de passe		
Mot de passe initial	**Mot de passe modifié**	**Explication**
`1` = `crypt_bsdmd5`	Utilise le même algorithme	L'identificateur `1` est également la valeur de `CRYPT_DEFAULT`. 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 `m5a` 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 est chiffré avec l'algorithme `crypt_sha256`.
`6` = `crypt_sha512`	Utilise le même algorithme	L'identificateur `6` est dans la liste `CRYPT_ALGORITHMS_ALLOW`. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme `crypt_sha512`.

Identificateur = Algorithme de mot de passe		
Mot de passe initial	**Mot de passe modifié**	**Explication**
`__unix__ = crypt_unix`	Utilise l'algorithme `crypt_bsdmd5`	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 le mot de passe, les algorithmes de chiffrement des mots de passe, consultez "Modification de l'algorithme de mot de passe (liste des tâches) " à la page 72.

Comptes système spéciaux

Le compte `root` est l'un des nombreux comptes *système*. 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. Un compte qui est livré avec `NP` ou `*LK*sys` dans le deuxième champ du fichier `shadow` indique un compte système.

Le tableau suivant répertorie des comptes système et leurs utilisations. Les comptes système exécutent des fonctions spéciales. Chaque compte possède un ID utilisateur inférieur à 100.

TABLEAU 2–2 Comptes de connexion système et leurs utilisations

Compte de connexion	GID	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 la connexion `root` doit être très soigneusement protégé. Le compte `root`, superutilisateur, 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.
`lp`	`71`	Est propriétaire des fichiers de données d'objet et des fichiers de données mis en spool pour l'imprimante.

TABLEAU 2–2 Comptes de connexion système et leurs utilisations *(Suite)*

Compte de connexion	GID	Utilisation
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	Est utilisé par les systèmes distants pour se connecter au système et démarrer des transferts de fichiers.

Connexions distantes

Les connexions distantes constituent une cible tentante pour les intrus. Oracle Solaris fournit plusieurs commandes pour surveiller, limiter et désactiver les connexions distantes. Pour plus d'informations sur les procédures, reportez-vous à la section "Sécurisation des connexions et des mots de passe (liste des tâches)" à la page 64.

Par défaut, les connexions distantes ne peuvent pas 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)`.

Connexions commutées

Lorsqu'un ordinateur est accessible par le biais d'un modem ou d'un port d'accès à distance, vous pouvez ajouter une couche supplémentaire de sécurité. Vous pouvez exiger un *mot de passe d'accès à distance* pour les utilisateurs qui accèdent à un système par le biais d'un modem ou d'un port d'accès à distance. Un utilisateur doit fournir ce mot de passe supplémentaire avant d'être autorisé à accéder au système.

Seul le superutilisateur peut créer ou modifier un mot de passe d'accès à distance. Pour garantir l'intégrité du système, le mot de passe doit être modifié environ une fois par mois. Le moyen le plus efficace d'utiliser cette fonction est d'exiger un mot de passe d'accès à distance pour accéder à un système de passerelle. Pour définir des mots de passe d'accès à distance, reportez-vous à la section "Création d'un mot de passe d'accès à distance" à la page 70.

Deux fichiers sont impliqués dans la création d'un mot de passe d'accès à distance : `/etc/dialups` et `/etc/d_passwd`. Le fichier `dialups` contient une liste des ports nécessitant un mot de passe d'accès à distance. Le fichier `d_passwd` contient une liste des programmes shell nécessitant un mot de passe chiffré comme mot de passe d'accès à distance complémentaire. Les informations contenues dans ces deux fichiers sont traitées de la manière suivante :

- Si le shell de connexion d'utilisateur dans `/etc/passwd` correspond à une entrée dans `/etc/d_passwd`, l'utilisateur doit fournir un mot de passe d'accès à distance.
- Si le shell de connexion d'utilisateur dans `/etc/passwd` n'est pas dans `/etc/d_passwd`, l'utilisateur doit fournir le mot de passe par défaut. Le mot de passe par défaut est l'entrée pour `/usr/bin/sh`.
- Si le champ du shell de connexion dans `/etc/passwd` est vide, l'utilisateur doit fournir le mot de passe par défaut. Le mot de passe par défaut est l'entrée pour `/usr/bin/sh`.

- Si `/etc/d_passwd` ne contient pas d'entrée pour `/usr/bin/sh`, les utilisateurs dont le champ du shell de connexion dans `/etc/passwd` est vide ou ne correspond pas aucune entrée dans `/etc/d_passwd` ne sont pas invités à indiquer de mot de passe d'accès à distance.
- Les connexions commutées sont désactivées sir / `/etc/d_passwd` comporte uniquement une entrée `/usr/bin//sh:*:`

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 peuvent également présenter des problèmes de sécurité. Par exemple, des interfaces réseau telles que `hme0` sont considérées comme des périphériques intégrés.

Le logiciel Oracle Solaris offre deux méthodes de contrôle d'accès aux périphériques. La *stratégie de périphériques* restreint ou empêche l'accès aux périphériques faisant partie intégrante de l'ordinateur. La stratégie de périphériques est appliquée dans le noyau. L'*allocation des périphériques* restreint ou empêche l'accès aux périphériques. L'allocation des périphériques est appliquée lors de l'allocation des utilisateurs.

La stratégie de périphériques utilise des privilèges pour protéger des périphériques sélectionnés du noyau. Par exemple, la stratégie des périphériques sur des interfaces réseau telles que `hme` exige tous les privilèges pour la lecture ou l'écriture.

L'allocation des périphériques utilise des autorisations pour protéger des périphériques, tels que des imprimantes ou des microphones. Par défaut, l'allocation des périphériques n'est pas activée. Une fois l'option activée, l'allocation des périphériques peut être configurée de sorte à empêcher l'utilisation d'un périphérique ou demander l'autorisation d'accès à ce périphérique. Lorsqu'un périphérique est alloué pour utilisation, aucun autre utilisateur ne peut y accéder jusqu'à ce que l'utilisateur courant le libère.

Un système Oracle Solaris peut être configuré en plusieurs domaines pour contrôler l'accès aux périphériques :

- **Définir la stratégie de périphériques** : dans Oracle Solaris, 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** : lorsque vous activez l'allocation des périphériques, vous pouvez limiter l'utilisation d'un périphérique à un utilisateur à la fois. Vous pouvez également requérir que l'utilisateur remplisse certaines exigences en matière de sécurité. Par exemple, vous pouvez 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. Un ordinateur kiosque peut être un candidat approprié pour rendre certains périphériques indisponibles pour l'utilisation.
- **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 "Utilisation de périphériques dans les zones non globales" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*. Pour une analyse plus générale des périphériques et des zones, reportez-vous à la section "Périphériques configurés dans des zones" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Stratégie de périphériques (présentation)

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 `hme0` 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 section "Privilèges (présentation)" à la page 197.

Dans les versions antérieures, les nœuds de périphérique étaient protégés uniquement par les autorisations du fichier. Par exemple, les périphériques appartenant au groupe `sys` ne pouvaient être ouverts que par les membres du groupe `sys`. Aujourd'hui, les autorisations de fichier ne prédisent pas qui peut ouvrir un périphérique. Au lieu de cela, 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 :

- “Configuration de la stratégie de périphériques (liste des tâches) ” à la page 84
- “Commandes de la stratégie de périphériques” à la page 98
- “Privilèges et périphériques ” à la page 205

Allocation des périphériques (présentation)

Le mécanisme d'allocation des périphériques vous permet de limiter l'accès à un périphérique, tel qu'un CD-ROM. Vous gérez ce mécanisme au niveau local. 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 une disquette ou un CD-ROM.
- 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 “Écriture de nouveaux scripts de nettoyage de périphériques” à la page 105.

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 des périphériques, reportez-vous aux sections suivantes :

- “Gestion de l'allocation des périphériques (liste des tâches) ” à la page 87
- “Allocation de périphériques” à la page 99
- “Commandes d'allocation de périphériques ” à la page 100

Contrôle de l'accès aux ressources de la machine

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.

Limitation et surveillance du 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 rubrique “Contrôle et restriction du superutilisateur (liste des tâches)” à la page 76.

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

Le contrôle d'accès basé sur les rôles (RBAC) est conçu pour limiter les capacités du superutilisateur. Le superutilisateur, utilisateur `root`, a accès à toutes les ressources du système. Avec RBAC, vous pouvez remplacer `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. Lorsque vous avez établi un rôle pour gérer une fonction ou un ensemble de fonctions, vous pouvez supprimer ces fonctions des capacités de l'utilisateur `root`.

Chaque rôle exige qu'un utilisateur connu se connecte avec son nom d'utilisateur et son mot de passe. Une fois connecté, l'utilisateur endosse le rôle avec un mot de passe spécifique. Par conséquent, toute personne connaissant le mot de passe `root` a une capacité limitée d'endommager votre système. Pour plus d'informations sur le contrôle RBAC, reportez-vous à la section “Contrôle d'accès basé sur les rôles (présentation) ” à la page 186.

Prévention des mauvaises utilisations involontaires des ressources de la machine

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

Vous devez veiller à définir correctement la variable PATH. Autrement, vous risquez d'exécuter par mégarde un programme introduit par un tiers. Le programme intrusif peut corrompre vos données ou endommager votre système. Ce type de programme, qui crée un risque de sécurité, 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. Étant 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 à la connexion. Le chemin d'accès est défini par les fichiers de démarrage `.login`, `.profile` et `.cshrc`. 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 de superutilisateur ne doit pas inclure de répertoire courant.

L'outil ASET examine les fichiers de démarrage pour s'assurer que la variable PATH est correctement définie. ASET vérifie également que la variable PATH ne contient pas d'entrée de point (`.`).

Affectation d'un shell restreint à des utilisateurs

Le shell standard permet à un utilisateur d'ouvrir des fichiers, exécuter des commandes, et ainsi de suite. 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 à son répertoire personnel, 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 vise uniquement 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

Étant donné qu'Oracle Solaris est un environnement multiutilisateur, la sécurité du système de fichiers constitue le risque de sécurité le plus élémentaire sur un système. 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.

Vous voulez peut-être permettre à certains utilisateurs de lire des fichiers et autoriser 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 6, “Contrôle de l'accès aux fichiers (tâches)” explique comment définir les autorisations de fichier.

Restriction des fichiers exécutables `setuid`

Les fichiers exécutables peuvent constituer des risques pour la sécurité. De nombreux programmes exécutables doivent être exécutés en tant que `root`, c'est-à-dire, en tant que superutilisateur, 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.

À l'exception des exécutables fournis par Oracle avec le bit `setuid` défini sur `root`, vous devez interdire 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, consultez “Prévention des problèmes de sécurité causés par les fichiers exécutables” à la page 141. Pour plus d'informations sur les procédures, reportez-vous à la section “Protection contre les programmes présentant des risques de sécurité (liste des tâches)” à la page 154.

Utilisation d'Automated Security Enhancement Tool

Le package de sécurité ASET fournit des outils d'administration automatisés permettant de contrôler et surveiller la sécurité de votre système. ASET propose trois niveaux de sécurité : faible, moyen et élevé. Vous spécifiez un niveau de sécurité ASET. À chaque niveau supérieur, les fonctions de contrôle de fichiers d'ASET augmentent afin de réduire l'accès aux fichiers et de renforcer la sécurité de votre système. Pour plus d'informations, reportez-vous au Chapitre 7, “Utilisation d'Automated Security Enhancement Tool (Tâches)”.

Utilisation de la Oracle Solaris Security Toolkit

Si ASET peut être utilisé pour apporter un petit nombre de modifications de sécurité à un système, Oracle Solaris Security Toolkit propose un mécanisme souple et extensible pour réduire, renforcer et sécuriser un système Oracle Solaris. Le logiciel Oracle Solaris Security Toolkit, couramment appelé kit d'outils JASS, est un outil qui permet à l'utilisateur d'effectuer des modifications de sécurité sur un système. L'outil peut fournir un rapport sur l'état de sécurité d'un système Oracle Solaris. L'outil permet également d'annuler ses exécutions précédentes. Le kit d'outils JASS peut être téléchargé sur le site Oracle et Sun (`http://www.oracle.com/us/sun/index.htm`). Cliquez sur le téléchargement de Sun : liste de A à Z, puis recherchez la chaîne `Solaris Security Toolkit` dans la liste alphabétique des téléchargements.

Le kit d'outils est décrit en détail dans *Securing Systems with the Solaris Security Toolkit* par Alex Noordergraaf et Glenn Brunette, ISBN 0-13-141071-7, juin 2003. Le manuel fait partie de la série Sun BluePrints publiée par Sun Microsystems Press.

Utilisation de la configuration Secure by Default

Par défaut, lorsque la version Solaris10 est installée, un grand nombre de services réseau sont activés. Pour limiter la connectivité réseau d'un système, vous exécutez la commande `netservices limited`. Cette commande active une configuration "Secure by Default" (SBD). 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 requêtes locales. Pour activer des services réseau individuels, comme `ftp`, vous utilisez l'utilitaire de gestion des services (SMF). Pour plus d'informations, reportez-vous aux pages de manuel `netservices(1M)` et `smf(5)`.

Utilisation des fonctions de gestion des ressources

Le logiciel Oracle Solaris offre des 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 d'Oracle Solaris, 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 Partie I, “Gestion des ressources” du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

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 SE Oracle Solaris. Cela empêche les processus exécutés dans une zone de contrôler 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 Partie II, “Zones” du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Surveillance de l'utilisation des ressources de la machine

En tant qu'administrateur système, vous devez surveiller l'activité 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, reportez-vous au Chapitre 28, “Audit Oracle Solaris (présentation) ”.

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 5, “Utilisation de l'outil de génération de rapports d'audit de base (tâches) ”.

Contrôle de l'accès aux fichiers

Oracle Solaris est un environnement multiutilisateur. Dans un environnement multiutilisateur, 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 6, “Contrôle de l'accès aux fichiers (tâches)”. Pour obtenir des instructions détaillées sur la définition des autorisations de fichiers appropriées, reportez-vous à la section “Protection des fichiers (liste des tâches)” à la page 142.

Protection des fichiers par chiffrement

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 superutilisateur. 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 support hors ligne.

La structure cryptographique fournit les commandes `digest`, `mac` et `encrypt` pour protéger les fichiers. Pour plus d'informations, reportez-vous au Chapitre 13, “Structure cryptographique Oracle Solaris (présentation)”.

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 les autorisations de fichiers suivantes :

- 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 plus d'informations sur l'utilisation des ACL, reportez-vous à la section "Utilisation des ACL pour protéger les fichiers UFS" à la page 138.

Partage de fichiers entre des machines

Un serveur de fichiers réseau peut contrôler les fichiers disponibles pour le 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`.

Le fichier `/etc/dfs/dfstab` sur le serveur de fichiers répertorie les systèmes de fichiers mis à disposition des clients sur le réseau par le serveur. Pour plus d'informations sur le partage des systèmes de fichiers, reportez-vous à la section "Partage automatique des systèmes de fichiers" du *Guide d'administration système : Services réseau*.

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 au Chapitre 3, "Différences entre les systèmes de fichiers Oracle Solaris ZFS et classiques" du *Guide d'administration Oracle Solaris ZFS*.

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 l'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 des capacités de superutilisateur sur un système de fichiers partagé par 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 6, “Accès aux systèmes de fichiers réseau (référence) ” du *Guide d'administration système : Services réseau*.

Contrôle de l'accès réseau

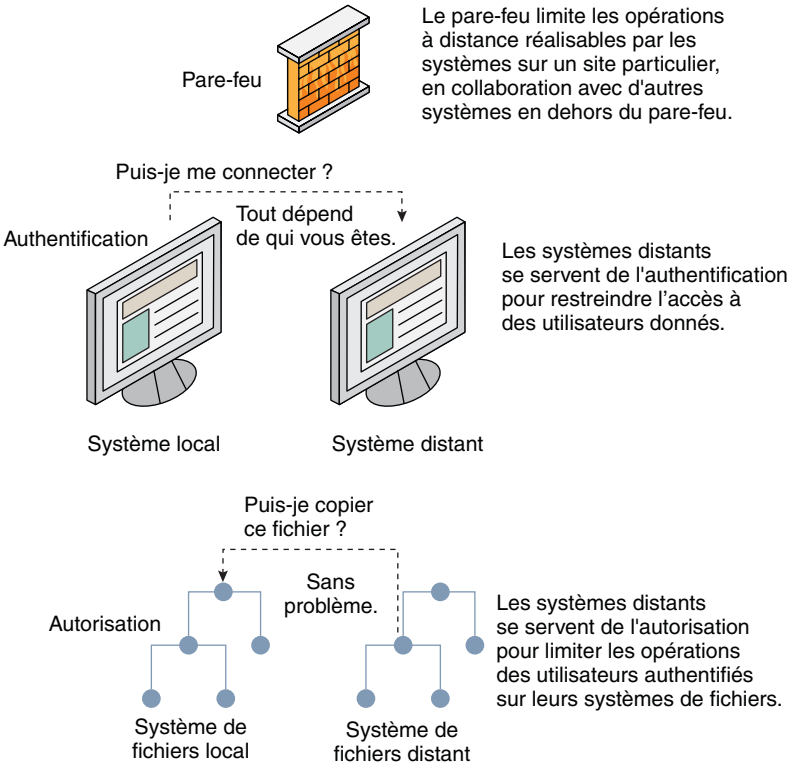
Les ordinateurs font souvent partie d'un *réseau* d'ordinateurs. Un réseau permet aux ordinateurs connectés d'échanger des informations. Les ordinateurs en réseau peuvent accéder aux données et à des ressources sur d'autres ordinateurs du réseau. Les réseaux d'ordinateurs créent un environnement informatique puissant et sophistiqué. Toutefois, ils rendent la sécurité informatique plus difficile à assurer.

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 2–1 Restrictions de sécurité sur les opérations à distance



Authentification et autorisation pour l'accès à distance

L'*authentification* est un moyen de restreindre l'accès à des utilisateurs spécifiques lorsque ces utilisateurs accèdent 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 2–3 Services d'authentification et d'autorisation pour l'accès à distance

Service	Description	Pour plus d'informations
IPsec	IPsec propose une authentification par certificat basée sur les hôtes et le chiffrement du trafic réseau.	Chapitre 19, "Architecture IPsec (présentation)" du *Guide d'administration système : services IP*

TABLEAU 2–3 Services d'authentification et d'autorisation pour l'accès à distance *(Suite)*

Service	Description	Pour plus d'informations
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" à la page 398.
LDAP et NIS+	Le service d'annuaire LDAP et le service de nommage NIS+ peuvent fournir à la fois l'authentification et l'autorisation au niveau du réseau.	*Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* et *System Administration Guide: Naming and Directory Services (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 29, "Accès aux systèmes distants (tâches)" du *Guide d'administration système : Services réseau*
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.	"SASL (présentation)" à la page 353
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 système d'authentification UNIX, DES ou Kerberos pour le RPC sécurisé.	"Présentation du RPC sécurisé" à la page 327
	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. Il utilise l'authentification Diffie-Hellman pour les clés publiques.	"Services NFS et sécurisé " à la page 327
Secure Shell	Secure Shell chiffre le trafic réseau sur un réseau non sécurisé. Secure Shell assure l'authentification par l'emploi de mots de passe, de clés publiques ou des deux. Secure Shell utilise l'authentification RSA et DSA pour les clés publiques.	"Oracle Solaris Secure Shell (présentation)" à la page 357

Le mécanisme de *port privilégié* d'Oracle Solaris constitue une alternative au RPC sécurisé. 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 autorisés. 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. Il intervient en tant que passerelle pour transmettre des données entre les réseaux, et en tant que barrière pour bloquer le passage des données vers le réseau et en provenance de celui-ci. Le pare-feu requiert qu'un utilisateur sur le réseau interne se connecte au système 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.

Un pare-feu peut également être utile entre certains réseaux internes. Par exemple, vous pouvez configurer un pare-feu ou un ordinateur passerelle sécurisé pour restreindre le transfert de paquets. La passerelle peut interdire l'échange de paquets entre deux réseaux, à moins que l'ordinateur passerelle ne soit l'adresse source ou l'adresse de destination du paquet. Un pare-feu doit également être configuré pour transférer des paquets pour des protocoles particuliers uniquement. Par exemple, vous pouvez autoriser des paquets pour le transfert de courrier, mais pas pour la commande `telnet` ou `rlogin`. ASET, lorsqu'il est exécuté sur le niveau de sécurité élevé, désactive la transmission de paquets IP (Internet Protocol).

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 – Un pare-feu empêche les utilisateurs non autorisés d'accéder aux hôtes sur votre réseau. Les mesures de sécurité appliquées sur le pare-feu doivent être strictes et rigides mais peuvent être plus souples sur d'autres hôtes du réseau. Néanmoins, un intrus capable de pénétrer dans votre système pare-feu peut ensuite accéder à tous les hôtes sur le réseau interne.

Un système 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.

Les technologies suivantes peuvent être utilisées pour sécuriser un système dans un pare-feu :

- ASET applique le niveau de sécurité élevé sur un système pare-feu système, comme décrit au Chapitre 7, “Utilisation d'Automated Security Enhancement Tool (Tâches)”.
- Le logiciel Oracle Solaris Security Toolkit, également appelé kit d'outils JASS, peut renforcer la sécurité d'un système Oracle Solaris avec un pare-feu. Le kit d'outils peut être téléchargé à partir du site Web de téléchargement de Sun à l'adresse Oracle Sun (`http://www.oracle.com/us/sun/index.htm`).
- Les filtres IPsec et Oracle Solaris IP peuvent fournir une protection par pare-feu. Pour plus d'informations sur la protection du trafic réseau, reportez-vous à la Partie IV, “IPsec” du *Guide d'administration système : services IP*.

Chiffrement et systèmes pare-feu

La plupart des réseaux locaux transmettent des données entre des ordinateurs sous la forme de blocs, également appelés *paquets*. Par l'intermédiaire d'une procédure appelée l'*éclatement de paquets*, les utilisateurs non autorisés à extérieur du réseau peuvent altérer ou détruire des données.

L'éclatement de paquets consiste à capturer les paquets avant qu'ils n'atteignent leur destination. L'intrus injecte ensuite des données arbitraires dans le contenu, puis les renvoie à leur course initiale. 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. Les attaques impliquant l'écoute électronique ne compromettent pas l'intégrité des données. Un système d'écoute électronique enregistre des conversations pour une rediffusion ultérieure. Un tel système n'emprunte pas l'identité d'un utilisateur. 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 19, “Utilisation d'Oracle Solaris Secure Shell (tâches)”.
- Pour chiffrer et authentifier des données sur un réseau, reportez-vous au Chapitre 21, “Introduction au service Kerberos”.
- Pour chiffrer des datagrammes IP, reportez-vous au Chapitre 19, “Architecture IPsec (présentation)” du *Guide d'administration système : services IP*.

Génération de rapports sur les problèmes de sécurité

Si vous suspectez une violation de sécurité, 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 3

Contrôle de l'accès aux systèmes (tâches)

Ce chapitre décrit les procédures de contrôle des utilisateurs qui peuvent accéder aux systèmes Oracle Solaris. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour des informations générales sur la sécurité système, reportez-vous au Chapitre 2, "Gestion de la sécurité de la machine (présentation)".

Contrôle de l'accès système (liste des tâches)

Un ordinateur est aussi sécurisé que son point d'entrée le plus faible. La liste des tâches suivante présente les zones que vous devez contrôler et sécuriser.

Tâche	Description	Voir
Contrôle, autorisation et refus d'une connexion utilisateur	Contrôle les activités de connexion inhabituelles. Empêche temporairement les connexions. Gère les connexions commutées.	"Sécurisation des connexions et des mots de passe (liste des tâches)" à la page 64
Garantie du chiffrement de mot de passe fort	Indique les algorithmes permettant de chiffrer les mots de passe utilisateur. Installe des algorithmes supplémentaires.	"Modification de l'algorithme de mot de passe (liste des tâches) " à la page 72
Contrôle et restriction des activités superutilisateur	Contrôle régulièrement l'activité superutilisateur. Empêche la connexion à distance par un utilisateur `root`.	"Contrôle et restriction du superutilisateur (liste des tâches)" à la page 76

Tâche	Description	Voir
Déni d'accès aux paramètres du matériel	Maintient les utilisateurs standard hors de la PROM.	“SPARC : Contrôle de l'accès au matériel système (liste des tâches) ” à la page 79

Sécurisation des connexions et des mots de passe (liste des tâches)

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

Tâche	Description	Voir
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.	“Procédure d'affichage de l'état de connexion d'un utilisateur” à la page 65
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 66
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 66
Enregistrement des tentatives de connexion ayant échoué	Crée un journal des utilisateurs qui n'ont pas réussi à fournir le bon mot de passe après cinq tentatives.	“Contrôle des tentatives de connexion ayant échoué” à la page 67
Enregistrement de toutes les tentatives de connexion ayant échoué	Crée un journal des échecs de tentative de connexion.	“Contrôle de toutes les tentatives de connexion ayant échoué” à la page 68
Création d'un mot de passe d'accès à distance	Demande un mot de passe supplémentaire pour les utilisateurs qui se connectent à distance par le biais d'un modem ou d'un port commuté.	“Création d'un mot de passe d'accès à distance” à la page 70
Désactivation temporaire des connexions commutées	Empêche les utilisateurs de se connecter à distance via un modem ou un port.	“Désactivation temporaire des informations de connexion d'accès à distance” à la page 72

Sécurisation des connexions et des mots de passe

Vous pouvez limiter les connexions à distance et exiger des utilisateurs qu'ils disposent d'un mot de passe. Vous pouvez également contrôler les tentatives d'accès ayant échoué et désactiver temporairement les connexions.

▼ Procédure d'affichage de l'état de connexion d'un utilisateur

1 Endossez le rôle d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Affichez l'état de connexion d'un utilisateur à l'aide de 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. Plusieurs noms de connexion doivent être spécifiés dans une liste de valeurs séparées par une virgule.

La commande `logins` utilise la base de donnée 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 nommage. Pour plus d'informations, reportez-vous à la page de manuel `logins(1M)`.

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

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

```
# logins -x -l rimmer
rimmer       500     staff           10   Annalee J. Rimmer
                     /export/home/rimmer
                     /bin/sh
                     PS 010103 10 7 -1
```

`rimmer` 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).

`Annalee J. Rimmer` Identifie le commentaire.

`/export/home/rimmer` Identifie le répertoire personnel de l'utilisateur.

`/bin/sh` 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

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Affichez tous les utilisateurs ne disposant pas de mot de passe à l'aide de la commande `logins`.**

```
# logins -p
```

L'option `-p` affiche une liste des utilisateurs sans mot de passe. La commande `logins` utilise la base de données de mots de passe du système local à moins qu'un service de nommage ne soit activé.

Exemple 3–2 Affichage des utilisateurs sans mot de passe

Dans l'exemple suivant, l'utilisateur `pmorph` n'a pas de mot de passe.

```
# logins -p
pmorph          501     other           1       Polly Morph
#
```

▼ Désactivation temporaire des connexions utilisateur

Désactivez temporairement les connexions utilisateur pendant l'arrêt du système ou de la maintenance de routine. Les connexions superutilisateur ne sont pas affectées. Pour plus d'informations, reportez-vous à la page de manuel `nologin(4)`.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

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

   ```
   # vi /etc/nologin
   ```

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

4. **Fermez et enregistrez le fichier.**

Exemple 3–3 Désactivation des connexions utilisateur

Dans cet exemple, les utilisateurs sont informés de l'indisponibilité du système.

```
# vi /etc/nologin
(Add system message here)

# cat /etc/nologin
***No logins permitted.***

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

Vous pouvez également mettre le système au niveau d'exécution 0, en mode monoutilisateur, pour désactiver les connexions. Pour plus d'informations sur l'exécution du système en mode monoutilisateur, reportez-vous au Chapitre 10, “Arrêt d'un système (tâches)” du *Guide d'administration système : administration de base*.

▼ Contrôle des tentatives de connexion ayant échoué

Cette procédure permet de capturer les échecs de tentative de connexion à partir des fenêtres de terminal. Cette procédure ne capture pas les connexions ayant échoué à partir d'un CDE ou à partir d'une tentative de connexion.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Créez le fichier `loginlog` dans le répertoire `/var/adm`.**

   ```
   # touch /var/adm/loginlog
   ```

3 **Définissez les autorisations en lecture-écriture pour l'utilisateur `root` sur le fichier `loginlog`.**

```
# chmod 600 /var/adm/loginlog
```

4 **Modifiez l'appartenance à un groupe en `sys` dans le fichier `loginlog`.**

```
# chgrp sys /var/adm/loginlog
```

5 **Vérifiez que le journal fonctionne.**

Par exemple, connectez-vous au système cinq fois avec un mot de passe incorrect. Ensuite, affichez le fichier `/var/adm/loginlog`.

```
# more /var/adm/loginlog
jdoe:/dev/pts/2:Tue Nov  4 10:21:10 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:21 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:30 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:40 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:49 2010
#
```

Le fichier `loginlog` contient une entrée pour chaque tentative infructueuse. Chaque entrée contient le nom de connexion de l'utilisateur, le périphérique tty et l'heure de la tentative infructueuse. Si un utilisateur fait moins de cinq tentatives infructueuses, aucune d'elles n'est consignée.

Un fichier `loginlog` croissant peut indiquer une tentative de s'introduire dans le système informatique. Par conséquent, vérifiez et effacez le contenu de ce fichier régulièrement. Pour plus d'informations, reportez-vous à la page de manuel `loginlog(4)`.

▼ Contrôle de toutes les tentatives de connexion ayant échoué

Cette procédure permet de capturer toutes les tentatives de connexion ayant échoué dans un fichier `syslog`.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Configurez le fichier `/etc/default/login` avec les valeurs souhaitées pour `SYSLOG` et `SYSLOG_FAILED_LOGINS`**

Modifiez le fichier `/etc/default/login` pour modifier l'entrée. Vérifiez que **`SYSLOG=YES`** n'est pas mise en commentaire.

```
# grep SYSLOG /etc/default/login
# SYSLOG determines whether the syslog(3) LOG_AUTH facility
```

```
# should be used
SYSLOG=YES
...
SYSLOG_FAILED_LOGINS=0
#
```

3 Créez un fichier avec les autorisations correctes pour contenir les informations de journalisation.

a. Créez le fichier `authlog` dans le répertoire `/var/adm`.

```
# touch /var/adm/authlog
```

b. Définissez des autorisations en lecture-écriture pour l'utilisateur `root` dans le fichier `authlog`.

```
# chmod 600 /var/adm/authlog
```

c. Modifiez l'appartenance à un groupe sur `sys` dans le fichier `authlog`.

```
# chgrp sys /var/adm/authlog
```

4 Modifiez le fichier `syslog.conf` pour consigner les tentatives infructueuses de saisie de mot de passe.

Les échecs doivent être envoyés dans le fichier `authlog`.

a. Tapez l'entrée suivante dans le fichier `syslog.conf`.

Les champs de la même ligne dans `syslog.conf` sont séparés par des tabulations.

`auth.notice` <*Press Tab*> `/var/adm/authlog`

b. Actualisez les informations de configuration pour le démon `syslog`.

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

5 Vérifiez que le journal fonctionne.

Par exemple, en tant qu'utilisateur standard, connectez-vous au système à l'aide d'un mot de passe incorrect. Ensuite, dans le rôle d'administrateur principal ou en tant que superutilisateur, affichez le fichier `/var/adm/authlog`.

```
# more /var/adm/authlog
Nov  4 14:46:11 example1 login: [ID 143248 auth.notice]
 Login failure on /dev/pts/8 from example2, stacey
#
```

6 Vérifiez le fichier `/var/adm/authlog` de façon régulière.

Exemple 3–4 Journalisation des tentatives d'accès après trois échecs de connexion

Suivez la procédure indiquée ci-dessus, à la différence près que vous devez définir la valeur de `SYSLOG_FAILED_LOGINS` sur `3` dans le fichier `/etc/default/login`.

Exemple 3–5 Fermeture de la connexion après trois échecs de connexion

Annulez la mise en commentaire de l'entrée `RETRIES` dans le fichier `/etc/default/login`, puis définissez la valeur de `RETRIES` sur `3`. Vos modifications prennent effet immédiatement. Après trois essais de connexion dans une session, le système ferme la connexion.

▼ Création d'un mot de passe d'accès à distance

Attention – Lorsque vous créez un mot de passe de connexion d'accès à distance, veillez à rester connecté à au moins un port. Testez le mot de passe sur un autre port. Si vous vous déconnectez pour tester le nouveau mot de passe, vous ne pourrez peut-être pas vous connecter à nouveau. Si vous n'êtes pas encore connecté à un autre port, vous pouvez revenir en arrière et corriger l'erreur.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Créez un fichier `/etc/dialups` contenant une liste de périphériques série.**

   Incluez tous les ports qui sont protégés par des mots de passe de connexion d'accès à distance. Le fichier `/etc/dialups` doit ressembler à ce qui suit :

   ```
   /dev/term/a
   /dev/term/b
   /dev/term/c
   ```

3. **Créez un fichier `/etc/d_passwd` contenant les programmes de connexion pour lesquels un mot de passe de connexion d'accès à distance est nécessaire.**

   Il s'agit des programmes shell qu'un utilisateur peut exécuter au moment de la connexion, par exemple, `uucico`, `sh`, `ksh` et `csh`. Le fichier `/etc/d_passwd` doit ressembler à ce qui suit :

   ```
   /usr/lib/uucp/uucico:encrypted-password:
   /usr/bin/csh:encrypted-password:
   /usr/bin/ksh:encrypted-password:
   /usr/bin/sh:encrypted-password:
   /usr/bin/bash:encrypted-password:
   ```

Dans la suite de la procédure, vous allez ajouter le mot de passe chiffré pour chaque programme de connexion.

4 Définissez la propriété sur `root` dans les deux fichiers.

```
# chown root /etc/dialups /etc/d_passwd
```

5 Définissez la propriété de groupe sur `root` dans les deux fichiers.

```
# chgrp root /etc/dialups /etc/d_passwd
```

6 Définissez les autorisations en lecture-écriture pour `root` dans les deux fichiers.

```
# chmod 600 /etc/dialups /etc/d_passwd
```

7 Créez les mots de passe chiffrés.

a. Créez un utilisateur temporaire.

```
# useradd username
```

b. Créez un mot de passe pour l'utilisateur temporaire.

```
# passwd username
New Password:      <Type password>
Re-enter new Password:       <Retype password>
passwd: password successfully changed for username
```

c. Capturez le mot de passe chiffré.

```
# grep username /etc/shadow > username.temp
```

d. Modifiez le fichier *username.temp*.

Supprimez tous les champs à l'exception du mot de passe chiffré. Le deuxième champ contient le mot de passe chiffré.

Par exemple, dans la ligne suivante, le mot de passe chiffré est `U9gp9SyA/JlSk`.

```
temp:U9gp9SyA/JlSk:7967:::::7988:
```

e. Supprimez l'utilisateur temporaire.

```
# userdel username
```

8 Copiez le mot de passe chiffré du fichier *username*`.temp` dans le fichier `/etc/d_passwd`.

Vous pouvez créer un mot de passe différent pour chaque shell de connexion. Vous pouvez également utiliser le même mot de passe pour chaque shell de connexion.

9 Informez vos utilisateurs se connectant à distance du mot de passe.

Vous devez vous assurer que votre moyen d'informer les utilisateurs ne peut pas être modifié.

▼ Désactivation temporaire des informations de connexion d'accès à distance

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Mettez l'entrée d'une seule ligne suivante dans le fichier `/etc/d_passwd` :**

```
/usr/bin/sh:*:
```

Modification de l'algorithme de mot de passe (liste des tâches)

La liste des tâches suivante présente les procédures d'administration des algorithmes de mot de passe.

Tâche	Voir
Garantie du chiffrement de mot de passe fort	"Spécification d'un algorithme de chiffrement de mot de passe" à la page 73
Garantie d'un chiffrement de mot de passe fort avec un service de nommage	"Spécification d'un nouvel algorithme de mot de passe pour un domaine NIS " à la page 74
	"Spécification d'un nouvel algorithme de mot de passe pour un domaine NIS+" à la page 74
	"Spécification d'un nouvel algorithme de mot de passe pour un domaine LDAP" à la page 74
Ajout d'un nouveau module de chiffrement de mot de passe	"Installation d'un module de chiffrement de mot de passe tiers" à la page 75

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

Par défaut, les mots de passe utilisateur sont chiffrés avec l'algorithme `crypt_unix`. Vous pouvez utiliser un algorithme de chiffrement plus fort, tel que MD5 ou Blowfish, en modifiant l'algorithme de chiffrement de mot de passe par défaut.

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

Dans cette procédure, la version BSD-Linux de l'algorithme MD5 est l'algorithme de chiffrement par défaut qui est utilisé lorsque les utilisateurs modifient leurs mots de passe. Cet algorithme est adapté à un réseau mixte de machines qui exécutent les versions Oracle Solaris, BSD et Linux d'UNIX. Pour obtenir une liste des algorithmes de mot de passe et des identificateurs d'algorithme, reportez-vous au Tableau 2–1.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Spécifiez l'identificateur de l'algorithme de chiffrement choisi.

Saisissez l'identificateur en tant que valeur pour la variable `CRYPT_DEFAULT` du fichier `/etc/security/policy.conf`.

Vous pouvez ajouter un commentaire au fichier afin d'expliquer votre choix.

```
# cat  /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#
# Use the version of MD5 that works with Linux and BSD systems.
# Passwords previously encrypted with __unix__ will be encrypted with MD5
# when users change their passwords.
#
#
CRYPT_DEFAULT=__unix__
CRYPT_DEFAULT=1
```

Dans cet exemple, la configuration des algorithmes assure que l'algorithme le plus faible, `crypt_unix`, n'est jamais utilisé pour chiffrer un mot de passe. Les utilisateurs dont les mots de passe ont été chiffrés avec le module `crypt_unix` obtiennent un mot de passe chiffré par `crypt_bsdmd5` lorsqu'ils changent leurs mots de passe.

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

Exemple 3–6 Utilisation de l'algorithme Blowfish pour le chiffrement de mot de passe

Dans cet exemple, l'identificateur de l'algorithme Blowfish, `2a`, est spécifié en tant que valeur pour la variable `CRYPT_DEFAULT` dans le fichier `policy.conf` :

```
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=2a
```

Cette configuration est compatible avec les systèmes BSD qui utilisent l'algorithme Blowfish.

▼ 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`. La machine client NIS chiffre le mot de passe.

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 machine 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 NIS+

Lorsque les utilisateurs dans un domaine NIS+ modifient leurs mots de passe, le service de nommage NIS+ consulte la configuration des algorithmes dans le fichier `/etc/security/policy.conf` sur le maître NIS+. Le maître NIS+, qui exécute le démon `rpc.nispasswd`, crée le mot de passe chiffré.

1. **Spécifiez l'algorithme de chiffrement de mot de passe dans le fichier `/etc/security/policy.conf` sur le maître NIS+.**
2. **Pour minimiser la confusion, copiez le fichier `/etc/security/policy.conf` du maître NIS+ pour tous les hôtes du domaine NIS+.**

▼ 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.

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 machine 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 la nouvelle 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`. L'ordinateur 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 alors chiffrés sur le serveur en utilisant le mécanisme cryptographique de Sun Java System Directory Server. Pour plus d'informations sur cette procédure, reportez-vous au Chapitre 11, "Configuration de Sun Java System Directory Server avec les clients LDAP (tâches)" du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

▼ Installation d'un module de chiffrement de mot de passe tiers

Un algorithme de chiffrement de mot de passe tiers est généralement fourni sous forme de module dans un package logiciel. Lorsque vous exécutez la commande `pkgadd`, les scripts du fournisseur doivent modifier le fichier `/etc/security/crypt.conf`. Vous devez ensuite modifier le fichier `/etc/security/policy.conf` pour inclure le nouveau module et son identificateur.

1 **Ajoutez le logiciel à l'aide de la commande `pkgadd`.**

Pour obtenir des instructions détaillées sur la procédure à suivre pour ajouter des logiciels, reportez-vous à la section "Ajout ou suppression d'un package de logiciels (pkgadd)" du *Guide d'administration système : administration de base*.

2 **Vérifiez que le nouveau module et son identificateur ont été ajoutés.**

Lisez la liste des algorithmes de chiffrement dans le fichier `/etc/security/crypt.conf`.

Par exemple, les lignes suivantes montrent qu'un module qui met en œuvre l'algorithme `crypt_rot13` a été installé.

```
# crypt.conf
#
md5 /usr/lib/security/$ISA/crypt_md5.so
rot13 /usr/lib/security/$ISA/crypt_rot13.so

# For *BSD - Linux compatibility
# 1 is MD5,  2a is Blowfish
1 /usr/lib/security/$ISA/crypt_bsdmd5.so
2a /usr/lib/security/$ISA/crypt_bsdbf.so
```

3 **Ajoutez l'identificateur de l'algorithme qui vient d'être installé au fichier `/etc/security/policy.conf`.**

Les lignes suivantes présentent des extraits du fichier `policy.conf` qui doivent être modifiés pour ajouter l'identificateur `rot13`.

```
# Copyright 1999-2002 Sun Microsystems, Inc.  All rights reserved.
# ...
#ident  "@(#)policy.conf        1.12     08/05/14 SMI"
# ...
# crypt(3c) Algorithms Configuration
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6,,rot13
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=md5
```

Dans cet exemple, l'algorithme `rot13` est utilisé si le mot de passe en cours a été chiffré avec l'algorithme `crypt_rot13`. Les nouveaux mots de passe utilisateur sont chiffrés avec l'algorithme `crypt_sunmd5`. Cette configuration d'algorithme fonctionne sur les réseaux exclusivement Solaris.

Contrôle et restriction du superutilisateur (liste des tâches)

La liste des tâches ci-dessous explique comment contrôler et limiter la connexion de l'utilisateur `root`.

Tâche	Description	Voir
Contrôle des personnes qui utilisent la commande `su`	Analyse le fichier `sulog` de façon régulière.	"Contrôle de l'utilisateur de la commande su" à la page 77
Affichage de l'activité superutilisateur sur la console	Contrôle les tentatives d'accès en tant que superutilisateur au moment ou elles sont tentées.	"Restriction et contrôle des connexions superutilisateur" à la page 78

Contrôle et restriction du superutilisateur

Une alternative à l'utilisation du compte de superutilisateur est de définir le contrôle de l'accès basé sur le rôle. Le contrôle de l'accès basé sur le rôle est appelé RBAC. Pour obtenir des informations générales sur le RBAC, reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186. Pour configurer RBAC, reportez-vous au Chapitre 9, "Utilisation du contrôle d'accès basé sur les rôles (tâches)".

▼ Contrôle de l'utilisateur de la commande `su`

Le fichier `sulog` répertorie chaque utilisation de la commande `su`, et pas seulement les tentatives `su` qui sont utilisées pour passer de l'utilisateur au superutilisateur.

- **Contrôle du 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 pmorph-root
SU 01/12 14:57 + pts/0 pmorph-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.

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

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

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`. L'utilisateur est peut-être passé au rôle `oracle` à l'aide d'une interface graphique.

▼ Restriction et contrôle des connexions superutilisateur

Cette méthode détecte immédiatement les tentatives du superutilisateur d'accéder au système local.

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.

À partir d'un système distant, essayez de vous connecter en tant que superutilisateur.

```
mach2 % rlogin -l root mach1
Password:      <Type root password of mach1>
Not on system console
Connection closed.
```

3 Contrôlez les tentatives de devenir superutilisateur.

Par défaut, les tentatives de devenir superutilisateur 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 superutilisateur.

```
% 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 3–7 Journalisation des tentatives d'accès superutilisateur

Dans cet exemple, les tentatives superutilisateur 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 superutilisateur, la tentative est imprimée sur la console de terminal.

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

Erreurs fréquentes Pour devenir superutilisateur à partir d'un système distant lorsque le fichier `/etc/default/login` contient l'entrée `CONSOLE` par défaut, les utilisateurs doivent d'abord se connecter avec leur nom d'utilisateur. Après la connexion avec leur nom d'utilisateur, les utilisateurs peuvent utiliser la commande `su` pour devenir superutilisateur.

Si la console affiche une entrée similaire à `Mar 16 16:20:36 mach1 login: ROOT LOGIN /dev/pts/14 FROM mach2.Example.COM`, le système autorise les connexions `root` à distance. Pour empêcher l'accès superutilisateur à distance, modifiez l'entrée `#CONSOLE=/dev/console` en `CONSOLE=/dev/console` dans le fichier `/etc/default/login`.

SPARC : Contrôle de l'accès au matériel système (liste des tâches)

La liste des tâches ci-dessous explique comment protéger la PROM contre un accès illégitime.

Tâche	Description	Voir
Empêchement des modifications des paramètres du matériel système par les utilisateurs	Demande un mot de passe pour modifier les paramètres PROM.	"Mot de passe obligatoire pour l'accès au matériel" à la page 79
Désactivation de la séquence d'abandon	Empêche les utilisateurs d'accéder à la PROM.	"Désactivation de la séquence d'abandon d'un système" à la page 80

Contrôle de l'accès au matériel du système

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

▼ Mot de passe obligatoire pour l'accès au matériel

Sur un système x86, l'équivalent à la protection de la PROM est de protéger le BIOS. Reportez-vous aux manuels de votre machine pour savoir comment protéger le BIOS.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle incluant le profil de sécurité des périphériques, le profil de maintenance et de réparation ou le profil d'administrateur système.**

Le profil d'administrateur système comprend le profil de maintenance et de réparation. Pour créer un rôle incluant le profil d'administrateur système et affecter le rôle à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 **Dans une fenêtre de terminal, saisissez 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.

3 **(Facultatif) Pour changer le mot de passe PROM, tapez la commande suivante :**

```
# 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 au prochain démarrage.

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

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

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 œuvre.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 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
```

3 Mettez à jour les paramètres par défaut du clavier.

```
# kbd -i
```

◆ ◆ ◆ CHAPITRE 4

Contrôle de l'accès aux périphériques (tâches)

Ce chapitre fournit des instructions étape par étape pour protéger les périphériques, en plus d'une section de référence. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour des informations générales sur la protection des périphériques, reportez-vous à la section “Contrôle de l'accès aux périphériques ” à la page 47.

Configuration des périphériques (liste des tâches)

La liste des tâches suivante présente les tâches de gestion de l'accès aux périphériques.

Tâche	Voir
Gestion de la stratégie de périphériques	“Configuration de la stratégie de périphériques (liste des tâches) ” à la page 84
Gestion de l'allocation de périphériques	“Gestion de l'allocation des périphériques (liste des tâches) ” à la page 87
Utilisation de l'allocation de périphériques	“Allocation de périphériques (liste des tâches) ” à la page 93

Configuration de la stratégie de périphériques (liste des tâches)

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

Tâche	Description	Voir
Affichage de la stratégie pour les périphériques de votre système	Dresse la liste des périphériques et des stratégies correspondantes.	"Procédure d'affichage de la stratégie de périphériques " à la page 84
Demande de privilège pour l'utilisation de périphériques	Utilise des privilèges pour protéger un périphérique.	"Procédure de modification de la stratégie pour un périphérique existant" à la page 85
Suppression des exigences concernant les privilèges pour un périphérique	Supprime ou réduit les privilèges requis pour accéder à un périphérique	Exemple 4–3
Audit des modifications apportées à la stratégie de périphériques	Enregistre les modifications apportées à la stratégie de périphériques dans la piste d'audit	"Procédure d'audit des modifications apportées à la stratégie de périphériques " à la page 86
Accès à `/dev/arp`	Récupère des informations d'Oracle Solaris IP MIB-II.	"Procédure de récupération d'informations IP MIB-II à partir d'un périphérique `/dev/*` " à la page 86

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.

▼ Procédure d'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/hme
/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/hme
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
```

▼ Procédure de modification de la stratégie pour un périphérique existant

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits Device Security.

Le rôle d'administrateur principal inclut le profil de droits Device Security (Sécurité des périphériques). Vous pouvez créer un rôle et lui attribuer le profil de droits Device Security. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à l'Exemple 9–3.

2 Ajoutez une stratégie à un périphérique.

`# update_drv -a -p` *policy device-driver*

`-a`	Spécifie une *policy* pour un *device-driver*.
`-p` *policy*	Stratégie de périphériques pour le *device-driver*. La stratégie de périphériques spécifie deux ensembles de privilèges. L'un des ensembles est nécessaire pour lire le périphérique, l'autre pour écrire dessus.
device-driver	Pilote du périphérique.

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

Exemple 4–2 Ajout d'une stratégie à un périphérique existant

Dans l'exemple suivant, une stratégie est ajoutée au périphérique `ipnat`.

```
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=none
        write_priv_set=none
# update_drv -a \
-p 'read_priv_set=net_rawaccess write_priv_set=net_rawaccess' ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
```

Exemple 4–3 Suppression d'une stratégie d'un périphérique

Dans l'exemple suivant, l'ensemble de privilèges en lecture est supprimé de la stratégie de périphériques pour le périphérique `ipnat`.

```
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess
# update_drv -a -p write_priv_set=net_rawaccess ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
        read_priv_set=none
        write_priv_set=net_rawaccess
```

▼ Procédure d'audit des modifications apportées à la stratégie de périphériques

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

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

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

   Ajoutez la classe `as` à la ligne `flags` du fichier `audit_control`. Le fichier ressemble à ce qui suit :

   ```
   # audit_control file
   dir:/var/audit
   flags:lo,as
   minfree:20
   naflags:lo
   ```

   Pour des instructions détaillées, reportez-vous à la section “Modification du fichier `audit_control` ” à la page 621.

▼ Procédure de 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`. Étant 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 des périphériques (liste des tâches)

La liste des tâches suivante présente les procédures permettant d'activer et de configurer 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 (liste des tâches) ” à la page 93.

Tâche	Description	Voir
Procédure pour rendre un périphérique allouable	Permet d'allouer un périphérique à un utilisateur à la fois.	“Procédure permettant de rendre un périphérique allouable” à la page 88
Autorisation des utilisateurs à allouer un périphérique.	Attribue des autorisations d'allocation de périphériques aux utilisateurs.	“Procédure d'autorisation des utilisateurs à allouer un périphérique ” à la page 89
Affichage des périphériques allouables sur votre système	Dresse la liste des périphériques allouables et de leur état.	“Procédure d'affichage d'informations d'allocation sur un périphérique ” à la page 90
Allocation forcée d'un périphérique	Alloue un périphérique à un utilisateur ayant un besoin immédiat.	“Allocation forcée d'un périphérique” à la page 90
Libération forcée d'un périphérique	Libère un périphérique actuellement alloué à un utilisateur.	“Forcez la libération d'un périphérique” à la page 91
Modification des propriétés d'allocation d'un périphérique	Modifie les conditions requises pour allouer un périphérique.	“Procédure de modification des périphériques pouvant être alloués” à la page 91

Tâche	Description	Voir
Création d'un script de nettoyage de périphériques	Purge les données d'un périphérique physique.	"Écriture de nouveaux scripts de nettoyage de périphériques" à la page 105
Désactivation de l'allocation de périphériques	Supprime des restrictions d'allocation de tous les périphériques.	"Désactivation du service d'audit " à la page 640
Audit de l'allocation de périphériques	Enregistre l'allocation de périphériques dans la piste d'audit.	"Procédure d'audit de l'allocation de périphériques" à la page 93

Gestion de l'allocation de périphériques

L'allocation des périphériques restreint ou empêche l'accès aux périphériques. Les restrictions sont appliquées lors de l'allocation des utilisateurs. Par défaut, les utilisateurs doivent avoir l'autorisation d'accéder aux périphériques allouables.

▼ Procédure permettant de rendre un périphérique allouable

Si vous avez déjà exécuté la commande `bsmconv` pour activer l'audit, l'allocation de périphériques est déjà activée sur votre système. Pour plus d'informations, reportez-vous à la page de manuel `bsmconv(1M)`.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits Audit Control.

Le rôle d'administrateur principal inclut le profil de droits Audit Control (Contrôle d'audit). Vous pouvez créer un rôle et lui attribuer le profil de droits Audit Control. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à l'Exemple 9–3.

2 Activation de l'allocation de périphériques

```
# bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: move aside /etc/rc3.d/S81volmgt.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation files.

The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

Remarque – Le démon de gestion du volume (`/etc/rc3.d/S81volmgt`) est désactivé par cette commande.

▼ Procédure d'autorisation des utilisateurs à allouer un périphérique

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

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

   Généralement, vous créez un profil de droits qui inclut l'autorisation `solaris.device.allocate`. Suivez les instructions fournies à la section "Procédure de création ou de modification d'un profil de droits" à la page 232. 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 attributs de sécurité : `mount` avec le privilège `sys_mount` et `umount` avec le privilège `sys_mount`

3. **Créez un rôle pour le profil de droits.**

   Suivez les instructions fournies à la section "Procédure de création et d'attribution d'un rôle à l'aide de l'interface graphique" à la page 211. 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 s'afficher en haut de la liste des profils inclus dans le rôle.

4. **Affectez le rôle à tous les utilisateurs autorisés à allouer un périphérique.**

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

   Pour consulter des exemples d'allocation de support amovible, reportez-vous à la section "Procédure d'allocation des périphériques" à la page 94.

Étant donné que le démon de gestion du volume (`vold`) n'est pas en cours d'exécution, les supports amovibles ne sont pas montés automatiquement. Pour consulter des exemples de montage d'un périphérique alloué, reportez-vous à la section “Procédure de montage d'un périphérique alloué ” à la page 95.

▼ Procédure d'affichage d'informations d'allocation sur un périphérique

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 “Procédure permettant de rendre un périphérique allouable” à la page 88.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits Device Security.

Le rôle d'administrateur principal inclut le profil de droits Device Security (Sécurité des périphériques). Vous pouvez créer un rôle et lui attribuer le profil de droits Device Security. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à l'Exemple 9–3.

2 Affichez des informations sur les périphériques allouables sur votre système.

```
# list_devices device-name
```

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

- `audio`[*n*] : microphone et haut-parleur.
- `fd`[*n*] : unité de disquette.
- `sr`[*n*] : unité de CD-ROM.
- `st`[*n*] : lecteur de bande.

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 L'utilisateur ou le rôle doit bénéficier de l'autorisation `solaris.device.revoke`.

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, le lecteur de bande est alloué de force à l'utilisateur `jdoe`.

```
$ allocate -U jdoe
```

▼ Forcez la libération 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 L'utilisateur ou le rôle doit bénéficier de l'autorisation `solaris.device.revoke`.

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, la libération de l'imprimante est forcée. L'imprimante est désormais disponible pour l'allocation par un autre utilisateur.

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

▼ Procédure de modification des périphériques pouvant être alloués

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits Device Security.**

   Le rôle d'administrateur principal inclut le profil de droits Device Security (Sécurité des périphériques). Vous pouvez créer un rôle et lui attribuer le profil de droits Device Security. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à l'Exemple 9–3.

2. **Spécifiez si l'autorisation est requise ou indiquez l'autorisation `solaris.device.allocate`.**

   Modifiez le cinquième champ dans l'entrée de périphérique du fichier `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 4–4 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 (`@`).

```
$ whoami
devicesec
$ vi /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 4–5 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 (`*`).

```
$ whoami
devicesec
$ vi /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 4–6 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 (`*`).

```
$ whoami
devicesec
$ vi /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
...
```

▼ Procédure d'audit de l'allocation de périphériques

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

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Présélectionnez la classe `ot` pour l'audit.**

   Ajoutez la classe `ot` à la ligne `flags` du fichier `audit_control`. Le fichier ressemble à ce qui suit :

   ```
   # audit_control file
   dir:/var/audit
   flags:lo,ot
   minfree:20
   naflags:lo
   ```

   Pour des instructions détaillées, reportez-vous à la section "Modification du fichier `audit_control` " à la page 621.

Allocation de périphériques (liste des tâches)

La liste des tâches suivante présente les procédures indiquant aux utilisateurs comment allouer des périphériques.

Tâche	Description	Voir
Allocation d'un périphérique	Permet à un utilisateur d'utiliser un périphérique tout en interdisant son utilisation par tout autre utilisateur.	"Procédure d'allocation des périphériques" à la page 94
Montage d'un périphérique alloué	Permet à un utilisateur d'afficher un périphérique à monter, tel qu'un CD-ROM ou une disquette.	"Procédure de montage d'un périphérique alloué " à la page 95
Libération d'un périphérique	Rend un périphérique allouable disponible pour l'utilisation par un autre utilisateur.	"Procédure de libération des périphériques" à la page 97

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.

▼ Procédure d'allocation des périphériques

Avant de commencer L'allocation de périphériques doit être activée, comme décrit dans la section "Procédure permettant de rendre un périphérique allouable" à la page 88. 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.

Exécutez la même commande.

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

Exemple 4–7 Allocation d'un microphone

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

```
% whoami
jdoe
% allocate audio
```

Exemple 4–8 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 "Forcez la libération d'un périphérique" à la page 91.

Exemple 4–9 Allocation d'un lecteur de bande

Dans cet exemple, l'utilisateur `jdoe` alloue un lecteur de bande, `st0`.

```
% whoami
jdoe
% allocate st0
```

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)`.

▼ Procédure de montage d'un périphérique alloué

Avant de commencer L'utilisateur ou le rôle a alloué le périphérique. Pour monter un périphérique, l'utilisateur ou le rôle doit disposer des privilèges requis correspondants. Pour accorder les privilèges requis, reportez-vous à la "Procédure d'autorisation des utilisateurs à allouer un périphérique " à la page 89.

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 personnel 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
```

où

`-o ro`	Indique que le périphérique doit être monté en lecture seule. Utilisez `-o rw` pour indiquer que vous devez être en mesure d'écrire sur le périphérique.
`-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 4–10 Allocation d'une unité de disquette

Dans cet exemple, un utilisateur prend un rôle pouvant allouer et monter une unité de disquette, `fd0`. La disquette est formatée avec un système de fichiers PCFS.

```
% roles
devicealloc
% su - devicealloc
Password:      <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: fd0 type: fd files: /dev/diskette /dev/rdiskette /dev/fd0a
...
$ allocate fd0
$ mount -o ro -F pcfs /dev/diskette /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
List of the contents of diskette
```

Exemple 4–11 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, un message d'erreur s'affiche : `mount: insufficient privileges`. Vérifiez les points suivants :

- Assurez-vous 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. Les commandes `pfsh`, `pfksh` et `pfcsh` permettent de créer un shell de profil.
- Assurez-vous 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.

▼ Procédure de 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.

1 Si le périphérique est monté, démontez-le.

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

2 Libérez le périphérique.

```
$ deallocate device-name
```

Exemple 4–12 Libération d'un microphone

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

```
% whoami
jdoe
% deallocate audio
```

Exemple 4–13 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. Les périphériques peuvent être protégés par le biais de l'allocation de périphériques. La stratégie de périphériques est mise en application par le noyau. 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. Seul le superutilisateur ou un rôle disposant de capacités équivalentes peut gérer des périphériques.

Le tableau suivant répertorie les commandes de gestion des périphériques.

TABLEAU 4–1 Commandes de gestion des périphériques

Commande	Objectif	Page de manuel
`devfsadm`	Administre des périphériques et des pilotes de périphériques sur un système en cours d'exécution. Charge également la stratégie de périphériques. 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.	`devfsadm`(1M)
`getdevpolicy`	Affiche la stratégie associée à un ou plusieurs périphériques. Cette commande peut être exécutée par n'importe quel utilisateur.	`getdevpolicy`(1M)
`add_drv`	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.	`add_drv`(1M)

TABLEAU 4–1 Commandes de gestion des périphériques *(Suite)*

Commande	Objectif	Page de manuel
`update_drv`	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.	`update_drv(1M)`
`rem_drv`	Supprime un périphérique ou un pilote de périphérique.	`rem_drv(1M)`

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. Les périphériques ne sont pas allouables tant que le script `bsmconv` n'est pas exécuté. 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 :

- 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 100.
- Les scripts de nettoyage de périphériques pour chaque périphérique allouable.

Ces commandes et scripts utilisent les fichiers locaux suivants pour mettre en œuvre 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.

Remarque – Le répertoire `/etc/security/dev` peut ne pas être pris en charge dans les versions futures d'Oracle Solaris.

Commandes d'allocation de périphériques

Avec les options 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 4–2 Commandes d'allocation de périphériques

Commande	Objectif	Page de manuel
`bsmconv`	Crée des bases de données pour gérer l'allocation de périphériques. Active également le service d'audit. Vous devez être connecté en tant que superutilisateur ou prendre un rôle d'administrateur principal. `devalloc_adm:` rend des périphériques allouables afin que des utilisateurs individuels puissent affecter un périphérique pour un usage privé. Empêche l'utilisation de périphériques sur un système en empêchant l'allocation de périphériques. Supprime des périphériques de la liste des périphériques allouables. Si vous ne souhaitez pas utiliser l'audit, vous pouvez utiliser la commande `devalloc_adm` pour activer l'allocation de périphériques.	`bsmconv(1M)`
`dminfo`	Recherche un périphérique allouable par type, nom et nom du chemin d'accès complet.	`dminfo(1M)`
`list_devices`	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`.	`list_devices(1)`
`list_devices -U`	Répertorie les périphériques allouables ou alloués à l'ID utilisateur spécifié. Cette option vous permet de vérifier les périphériques allouables ou alloués à un autre utilisateur. Vous devez avoir l'autorisation `solaris.device.revoke`.	
`allocate`	Réserve un périphérique allouable pour une utilisation par un autre utilisateur. Par défaut, un utilisateur doit avoir 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.	`allocate(1)`
`deallocate`	Supprime la réserve d'allocation d'un autre périphérique.	`deallocate(1)`

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 “Procédure d'autorisation des utilisateurs à allouer un périphérique ” à la page 89.

Les administrateurs doivent avoir 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 nécessitant des autorisations” à la page 256.

État 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 le superutilisateur ou un rôle bénéficiant du profil de droits Device Management ou Device Security 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`

Des cartes de périphériques sont créées lorsque vous paramétrez l'allocation de périphériques. Un fichier `/etc/security/device_maps` par défaut est créé par la commande `bsmconv` lorsque le service d'audit est activé. Ce fichier `device_maps` initial peut être personnalisé pour votre site. Le fichier `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 d'une ligne au format suivant :

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

EXEMPLE 4–14 Exemple d'entrée `device_maps`

Ce qui suit est un exemple d'entrée dans un fichier `device_maps` pour une unité de disquette, `fd0` :

```
fd0:\
        fd:\
        /dev/diskette /dev/rdiskette /dev/fd0a /dev/rfd0a \
/dev/fd0b /dev/rfd0b /dev/fd0c /dev/fd0 /dev/rfd0c /dev/rfd0:\
```

Les lignes dans le fichier `device_maps` peuvent se terminer par un backslash (\) pour indiquer que l'entrée se poursuit à 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 “Procédure d'affichage d'informations d'allocation sur un périphérique ” à la page 90.

device-type Spécifie le type de périphérique générique. Le nom générique est le nom de la classe de périphériques, tels que `st`, `fd` 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`

Un fichier `/etc/security/device_allocate` initial est créé par la commande `bsmconv` lorsque le service d'audit est activé. Ce fichier `device_allocate` initial peut être utilisé comme point de départ. Vous pouvez modifier le fichier `/etc/security/device_allocate` pour rendre des périphériques allouables non allouables ou pour ajouter de nouveaux périphériques. Un exemple de fichier `device_allocate` est indiqué ci-après.

```
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
```

Une entrée dans le fichier `device_allocate` ne signifie pas que le périphérique est allouable, sauf si l'entrée stipule spécifiquement que le périphérique est allouable. Dans l'exemple de fichier `device_allocate`, notez l'astérisque (*) dans le cinquième champ de l'entrée de périphérique audio. Un astérisque dans le cinquième champ indique au système que le

périphérique n'est pas allouable. Par conséquent, le périphérique ne peut pas être utilisé. D'autres valeurs ou aucune valeur dans ce champ indiquent que le périphérique peut être utilisé.

Dans le fichier `device_allocate`, chaque périphérique est représenté par une entrée d'une ligne au format suivant :

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

Les lignes dans le fichier `device_allocate` peuvent se terminer par un backslash (`\`) pour indiquer que l'entrée se poursuit à 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 "Procédure d'affichage d'informations d'allocation sur un périphérique " à la page 90.

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`.

`reserved` Sun se réserve les deux champs qui sont marqués `reserved` pour une utilisation ultérieure.

auths Indique si le périphérique est allouable. 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 avec l'autorisation `solaris.device.allocate` :

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

Vous pouvez décider d'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 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 modems, des terminaux, des tablettes graphiques et d'autres périphériques allouables. Le script doit remplir des exigences en matière de réutilisation des objets pour ce type de périphérique.

Scripts de nettoyage de périphériques

L'allocation de périphériques satisfait en partie l'exigence 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. Oracle Solaris fournit ces scripts. 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, le script interroge le périphérique pour déterminer si le périphérique 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 supports 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 support. La libération est reportée jusqu'à ce que le support 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 :

- **script`fd_clean`** : script de nettoyage de périphériques pour disquettes.
- **script `sr_clean`** : script de nettoyage de périphériques pour unités de CD-ROM.

Les scripts utilisent la commande `eject` pour supprimer les supports 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.

Écriture 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 une valeur égale à "`0`" en cas d'exécution correcte et supérieure à "`0`" en cas d'échec. Les options `-I`, `-f` et `-S` déterminent le mode d'exécution du script :

`-I` Requis 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 support 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` Pour le nettoyage standard. L'option est interactive et suppose que l'utilisateur est disponible pour répondre aux invites.

◆ ◆ ◆ CHAPITRE 5

Utilisation de l'outil de génération de rapports d'audit de base (tâches)

Ce chapitre décrit la création d'un manifeste des fichiers sur un système et son utilisation pour vérifier l'intégrité du système. 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 système dans le temps au niveau des fichiers.

Vous trouverez ci-après une liste des informations citées dans ce chapitre :

Outil de génération de rapports d'audit de base (présentation)

BART est un outil de suivi de fichiers fonctionnant entièrement au niveau du système de fichiers. L'utilisation de BART vous permet de collecter rapidement, facilement et de manière fiable des informations sur les composants de la pile logicielle installée sur les systèmes déployés. L'utilisation de BART peut réduire considérablement les coûts d'administration d'un réseau de systèmes en simplifiant des tâches d'administration fastidieuses.

BART vous permet de déterminer les modifications survenues au niveau des fichiers sur un système, par rapport à une ligne de base connue. Utilisez BART pour créer une ligne de base ou un manifeste de *contrôle* à partir d'un système entièrement installé et configuré. Vous pouvez comparer cette ligne de base à un instantané du système à un moment ultérieur, générant ainsi un rapport qui répertorie les modifications au niveau des fichiers survenues sur le système depuis son installation.

La commande `bart` est une commande UNIX standard. Vous pouvez rediriger la sortie de la commande `bart` vers un fichier en vue d'un traitement ultérieur.

Fonctionnalités BART

BART a été conçu en mettant l'accent sur une syntaxe simple, à la fois puissante et flexible. L'outil vous permet de générer des manifestes d'un système donné au fil du temps. Ensuite, lorsque les fichiers du système doivent être validés, vous pouvez générer un rapport en comparant les anciens et nouveaux manifestes. Un autre moyen d'utiliser BART consiste à générer des manifestes de plusieurs systèmes similaires et à exécuter des comparaisons de système à système. La principale différence entre BART et les outils d'audit existants est que BART est flexible, à la fois en termes d'informations suivies et d'informations signalées.

Les utilisations et avantages supplémentaires de BART sont les suivants :

- Méthode efficace et facile pour classifier un système exécutant le logiciel Oracle Solaris au niveau des fichiers.
- Possibilité de déterminer les fichiers à surveiller et de modifier les profils lorsque cela s'avère nécessaire. Cette flexibilité vous permet de surveiller les personnalisations locales et de reconfigurer le logiciel de manière simple et efficace.
- Garantie que les systèmes exécutent un logiciel fiable.
- Possibilité de surveiller les modifications au niveau des fichiers d'un système dans le temps, ce qui peut vous aider à localiser des fichiers corrompus ou inhabituels.
- Aide pour la résolution des problèmes de performances du système.

Composants BART

BART comporte deux composants principaux et un composant facultatif :

- Manifeste BART
- Rapport BART
- Fichier de règles BART

Manifeste BART

Vous utilisez la commande `bart create` pour prendre un instantané au niveau des fichiers d'un système à un moment donné. La sortie est un catalogue de fichiers et d'attributs de fichiers appelé *manifeste*. Le manifeste répertorie des informations sur tous les fichiers ou sur des fichiers spécifiques sur un système. Il contient des informations sur les attributs de fichiers, pouvant inclure des informations d'identification uniques, comme par exemple une somme de contrôle MD5. Pour plus d'informations sur la somme de contrôle MD5, reportez-vous à la page de manuel `md5(3EXT)`. Un manifeste peut être stocké et transféré entre des systèmes client et serveur.

Remarque – BART *ne franchit pas* les limites du système de fichiers, à l'exception des systèmes de fichiers du même type. Cette contrainte rend la sortie de la commande `bart create` plus prévisible. Par exemple, la commande `bart create` exécutée sans arguments répertorie tous les systèmes de fichiers sous le répertoire racine (`/`). Cependant, aucun système de fichiers NFS ou TMPFS ou CD-ROM monté n'est classifié. Lors de la création d'un manifeste, ne tentez pas d'auditer des systèmes de fichier sur un réseau. Notez que l'utilisation de BART pour surveiller des systèmes de fichiers en réseau peut consommer d'importantes ressources pour générer des manifestes de faible valeur.

Pour plus d'informations sur les manifestes BART, reportez-vous à la section "Format de fichier manifeste BART " à la page 125.

Rapport BART

L'outil de génération de rapports comporte trois entrées : les deux manifestes à comparer et éventuellement un fichier de règles fourni par l'utilisateur et indiquant les écarts à marquer.

Vous utilisez la commande `bart compare` pour comparer deux manifestes, un *manifeste de contrôle* et un *manifeste de test*. Ces manifestes doivent être préparés avec les mêmes systèmes de fichiers, options et fichier de règles que vous utilisez avec la commande `bart create`.

La sortie de la commande `bart compare` est un rapport qui répertorie les écarts par fichier entre les deux manifestes. Un *écart* est un changement apporté à n'importe quel attribut d'un fichier classifié pour les deux manifestes. Les ajouts ou suppressions d'entrées de fichiers entre les deux manifestes sont également considérés comme des écarts.

Il existe deux niveaux de contrôle lors du reporting des écarts :

- Lors de la génération d'un manifeste
- Lors de la production de rapports

Ces niveaux de contrôle sont intentionnels, étant donné que la génération d'un manifeste est plus coûteuse que l'établissement d'un rapport sur les écarts entre deux manifestes. Une fois que vous avez créé des manifestes, vous avez la possibilité de les comparer à partir de différentes perspectives en exécutant la commande `bart compare` avec différents fichiers de règles.

Pour plus d'informations sur les rapports BART, reportez-vous à la section "Génération de rapports BART" à la page 128.

Fichier de règles BART

Le *fichier de règles* est un fichier texte que vous pouvez éventuellement utiliser comme entrée pour la commande `bart`. Ce fichier utilise des règles d'inclusion et d'exclusion. Un fichier de règles est utilisé pour créer des manifestes et des rapports personnalisés. Un fichier de règles vous permet d'exprimer dans une syntaxe abrégée les ensembles de fichiers que vous souhaitez

classifier, ainsi que les attributs à surveiller pour tout ensemble de fichiers donné. Lorsque vous comparez des manifestes, le fichier de règles facilite le marquage des écarts entre les manifestes. L'utilisation d'un fichier de règles constitue un moyen efficace de collecter des informations spécifiques sur les fichiers d'un système.

Les fichiers de règles sont créés à l'aide d'un éditeur de texte. Avec un fichier de règles, vous pouvez effectuer les tâches suivantes :

- Utilisez la commande `bart create` pour créer un manifeste qui répertorie des informations sur tous les fichiers ou sur des fichiers spécifiques d'un système.
- Utilisez la commande `bart compare` pour générer un rapport qui surveille des attributs spécifiques d'un système de fichiers.

Remarque – Vous pouvez créer plusieurs fichiers de règles à des fins différentes. Toutefois, si vous créez un manifeste en utilisant un fichier de règles, vous devez utiliser le même fichier de règles lorsque vous comparez les manifestes. Si vous n'utilisez pas le même fichier de règles pour comparer des manifestes créés avec un même fichier de règles, la sortie de la commande `bart compare` répertorie de nombreux écarts non valides.

Un fichier de règles peut également contenir des erreurs de syntaxe et d'autres informations ambigües en raison d'une erreur de l'utilisateur. Si un fichier de règles contient des informations erronées, ces erreurs de l'utilisateur sont également signalées.

L'utilisation d'un fichier de règles pour surveiller des fichiers spécifiques et des attributs de fichiers sur un système requiert une planification. Avant de créer un fichier de règles, déterminez les fichiers et attributs de fichiers du système que vous souhaitez surveiller. En fonction de vos objectifs, vous pouvez utiliser un fichier de règles pour créer des manifestes, comparer des manifestes, ou à d'autres fins.

Pour plus d'informations sur le fichier de règles BART, reportez-vous à la section "Format de fichier de règles BART" à la page 126 et à la page de manuel `bart_rules(4)`.

Utilisation de BART (liste des tâches)

Tâche	Description	Voir
Création d'un manifeste BART.	Génère une liste d'informations sur chaque fichier installé sur un système.	"Création d'un manifeste" à la page 112

Tâche	Description	Voir
Création d'un manifeste BART personnalisé.	Génère une liste d'informations sur des fichiers spécifiques qui sont installés sur un système de l'une des façons suivantes : ■ En spécifiant une sous-arborescence ■ En spécifiant un nom de fichier ■ En utilisant un fichier de règles	"Personnalisation d'un manifeste" à la page 114 Exemple 5–2 Exemple 5–3 Exemple 5–4
Comparaison de manifestes BART.	Génère un rapport qui compare les modifications apportées à un système dans le temps. Ou génère un rapport qui compare un ou plusieurs systèmes pour contrôler le système.	"Procédure de comparaison des manifestes pour le même système dans le temps" à la page 117 "Comparaison de manifestes de différents systèmes " à la page 120
(Facultatif) Personnalisation d'un rapport BART.	Génère un rapport BART personnalisé de l'une des manières suivantes : ■ En spécifiant des attributs ■ En utilisant un fichier de règles	"Personnalisation d'un rapport BART en spécifiant des attributs de fichiers " à la page 122 "Personnalisation d'un rapport BART en utilisant un fichier de règles " à la page 123

Utilisation de BART (tâches)

Vous pouvez exécuter la commande `bart` en tant qu'utilisateur standard, superutilisateur ou utilisateur ayant pris le rôle d'administrateur principal. Si vous exécutez la commande `bart` en tant qu'utilisateur standard, vous pouvez uniquement classifier et surveiller des fichiers pour lesquels vous disposez d'une autorisation d'accès, tels que des fichiers dans votre répertoire personnel. L'avantage de vous connecter en tant que superutilisateur lorsque vous exécutez la commande `bart` est que les manifestes que vous créez contiennent des informations sur les fichiers cachés et privés que vous souhaitez peut-être surveiller. Si vous avez besoin de classifier des informations sur des fichiers disposant d'autorisations restreintes, par exemple, le fichier `/etc/passwd` ou `/etc/shadow`, exécutez la commande `bart` en tant que superutilisateur. Pour plus d'informations sur l'utilisation du contrôle d'accès basé sur le rôle, reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186.

Considérations de sécurité BART

L'exécution de la commande `bart` en tant que superutilisateur rend la sortie lisible par tout utilisateur. Cette sortie peut contenir des noms de fichiers destinés à être privés. Si vous vous connectez en tant que superutilisateur lorsque vous exécutez la commande `bart`, prenez les mesures appropriées pour protéger la sortie. Par exemple, utilisez les options générant des fichiers de sortie avec des autorisations restreintes.

Remarque – Les procédures et exemples de ce chapitre illustrent la commande `bart` exécutée par le superutilisateur. Sauf indication contraire, l'exécution de la commande `bart` en tant que superutilisateur est facultative.

▼ Création d'un manifeste

Vous pouvez créer un manifeste d'un système immédiatement après une première installation du logiciel Oracle Solaris. Ce type de manifeste vous fournit une ligne de base pour comparer des changements sur le même système dans le temps. Vous pouvez aussi l'utiliser pour effectuer des comparaisons avec des manifestes d'autres systèmes. Par exemple, si vous prenez un instantané de chaque système de votre réseau, puis comparez chaque manifeste de test au manifeste de contrôle, vous pouvez rapidement déterminer ce que vous devez faire pour synchroniser le système de test avec la configuration de référence.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle et redirigez la sortie vers un fichier.

```
# bart create options > control-manifest
```

`-R` Spécifie le répertoire root pour le manifeste. Tous les chemins d'accès spécifiés par les règles sont interprétés par rapport à ce répertoire. Tous les chemins d'accès signalés dans le manifeste sont relatifs à ce répertoire.

`-I` Accepte une liste de fichiers individuels à classifier, soit sur la ligne de commande soit à lire dans l'entrée standard.

`-r` Nom du fichier de règles pour ce manifeste. Notez que –, lorsqu'il est utilisé avec l'option `-r`, lit le fichier de règles dans l'entrée standard.

`-n` Désactive les signatures de contenu de tous les fichiers standard dans la liste de fichiers. Cette option peut être utilisée pour améliorer les performances. Ou bien vous pouvez l'utiliser s'il est prévu que le contenu de la liste de fichiers change, comme dans le cas des fichiers journaux du système.

3 Examinez le contenu du manifeste.

4 **Enregistrez le manifeste pour une utilisation ultérieure.**

Choisissez un nom explicite pour le manifeste. Par exemple, utilisez le nom du système et la date de création du manifeste.

Exemple 5–1 Création d'un manifeste répertoriant des informations sur chaque fichier d'un système

Si vous exécutez la commande `bart create` sans aucune option, des informations relatives à tous les fichiers installés sur le système sont répertoriées. Utilisez ce type de manifeste comme ligne de base de base lorsque vous installez de nombreux systèmes à partir d'une image centrale. Vous pouvez également utiliser ce type de manifeste pour effectuer des comparaisons lorsque vous souhaitez vous assurer que les installations sont identiques.

Par exemple :

```
# bart create
! Version 1.0
! Thursday, December 04, 2003 (16:17:39)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 1024 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea47 0 0
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f8dc04d 0 10
/.java/.userPrefs D 512 40700 user::rwx,group::---,mask:---
other:--- 3f8dc06b 010
/.java/.userPrefs/.user.lock.root F 0 100600 user::rw-
group::---,mask:---,other:--- 3f8dc06b 0 10 -
/.java/.userPrefs/.userRootModFile.root F 0 100600 user::rw-,
group::---,mask:---,other:--- 3f8dc0a1 0 10 -
.
.
.
/var/sadm/pkg/SUNWdtmad/install/depend F 932 100644 user::rw-,
group::r--,mask:r--,other:r-- 3c23a19e 0 0 -
/var/sadm/pkg/SUNWdtmad/pkginfo F 594 100644 user::rw-
group::r--,mask:r--,other:r-- 3f81e416 0 0 -
/var/sadm/pkg/SUNWdtmad/save D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e416 0 0
/var/sadm/pkg/SUNWdtmaz D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e41b 0 0
/var/sadm/pkg/TSIpgxw/save D 512 40755 user::rwx
group::r-x,mask:r-x,other:r-x 3f81e892 0 0
.
.
.
```

Chaque manifeste se compose d'un en-tête et d'entrées. Chaque entrée de fichier manifeste constitue une seule ligne, selon le type de fichier. Par exemple, pour chaque entrée de manifeste dans la sortie ci-dessus, le type `F` indique un fichier et le type `D` un répertoire. Sont également répertoriées des informations sur la taille, le contenu, l'ID utilisateur, l'ID de groupe et les autorisations. Les entrées de fichier dans la sortie sont triées par versions codées des noms de fichier de sorte à traiter correctement les caractères spéciaux. Toutes les entrées sont stockées dans l'ordre croissant par nom de fichier. Pour tous les noms de fichiers non standard, tels que ceux contenant des caractères de retour à la ligne ou de tabulation, les caractères non standard sont mis entre guillemets avant que les noms de fichiers ne soient triés.

Les lignes commençant par `!` fournissent des métadonnées sur le manifeste. La ligne de version du manifeste indique la version de spécification du manifeste. La ligne de date indique la date de création du manifeste. Reportez-vous à la page de manuel `date(1)`. Certaines lignes sont ignorées par l'outil de comparaison de manifestes. Les lignes ignorées incluent des lignes vides, des lignes composées uniquement d'espaces blancs et des commentaires commençant par #.

▼ Personnalisation d'un manifeste

Vous pouvez personnaliser un manifeste de l'une des façons suivantes :

- En spécifiant une sous-arborescence

  La création d'un manifeste pour une sous-arborescence sur un système est un moyen efficace de surveiller les modifications apportées à des fichiers spécifiques, au lieu de contrôler l'intégralité du contenu d'un vaste répertoire. Vous pouvez créer un manifeste de ligne de base pour une sous-arborescence spécifique sur votre système, puis créer périodiquement des manifestes de test de la même sous-arborescence. Utilisez la sous-commande `bart compare` pour comparer le manifeste de contrôle à celui de test. En utilisant cette option, vous pouvez surveiller efficacement les systèmes de fichiers importants pour déterminer si des fichiers ont été compromis par un intrus.

- En spécifiant un nom de fichier

  Étant donné que la création d'un manifeste classifiant l'ensemble du système requiert plus de temps et d'espace et est plus coûteuse, vous pouvez choisir d'utiliser cette option de la commande `bart` lorsque vous souhaitez uniquement répertorier des informations relatives à un ou plusieurs fichiers spécifiques sur un système.

- En utilisant un fichier de règles

  Vous utilisez un fichier de règles pour créer des manifestes personnalisés qui répertorient des informations sur des fichiers spécifiques et des sous-arborescences spécifiques sur un système donné. Vous pouvez également utiliser un fichier de règles pour contrôler des attributs de fichiers spécifiques. L'utilisation d'un fichier de règles pour créer et comparer des manifestes vous donne la possibilité de spécifier des attributs multiples pour plusieurs fichiers ou sous-arborescences. En revanche, à partir de la ligne de commande, vous ne

pouvez indiquer qu'une définition d'attribut globale qui s'applique à tous les fichiers pour chaque manifeste que vous créez ou chaque rapport que vous générez.

1. **Déterminez les fichiers que vous souhaitez classifier et surveiller.**

2. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

3. **Après l'installation du logiciel Oracle Solaris, créez un manifeste personnalisé à l'aide de l'une des options suivantes :**

   - En spécifiant une sous-arborescence :

     ```
     # bart create -R root-directory
     ```

   - En spécifiant un ou des noms de fichiers :

     ```
     # bart create -I filename...
     ```

     Par exemple :

     ```
     # bart create -I /etc/system /etc/passwd /etc/shadow
     ```

   - En utilisant un fichier de règles :

     ```
     # bart create -r rules-file
     ```

4. **Examinez le contenu du manifeste.**

5. **Enregistrez le manifeste pour une utilisation ultérieure.**

Exemple 5–2 Création d'un manifeste en spécifiant une sous-arborescence

Cet exemple montre la création d'un manifeste contenant des informations sur les fichiers de la sous-arborescence `/etc/ssh` uniquement.

```
# bart create -R /etc/ssh
! Version 1.0
! Saturday, November 29, 2003 (14:05:36)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81eab9 0 3
```

```
/ssh_config F 861 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81e504 0 3 422453ca0e2348cd9981820935600395
/ssh_host_dsa_key F 668 100600 user::rw-,group::---,mask:---,
other:--- 3f81eab9 0 0 5cc28cdc97e833069fd41ef89e4d9834
/ssh_host_dsa_key.pub F 602 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eab9 0 0 16118c736995a4e4754f5ab4f28cf917
/ssh_host_rsa_key F 883 100600 user::rw-,group::---,mask:---,
other:--- 3f81eaa2 0 0 6ff17aa968ecb20321c448c89a8840a9
/ssh_host_rsa_key.pub F 222 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eaa2 0 0 9ea27617efc76058cb97aa2caa6dd65a
.
.
.
```

Exemple 5–3 Personnalisation d'un manifeste en spécifiant un nom de fichier

Cet exemple montre la création d'un manifeste répertoriant uniquement des informations sur les fichiers `/etc/passwd` et `/etc/shadow` d'un système.

```
# bart create -I /etc/passwd /etc/shadow
! Version 1.0
! Monday, December 15, 2003 (16:28:55)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/passwd F 542 100444 user::r--,group::r--,mask:r--,
other:r-- 3fcfd45b 0 3 d6
84554f85d1de06219d80543174ad1a
/etc/shadow F 294 100400 user::r--,group::---,mask:---,
other:--- 3f8dc5a0 0 3 fd
c3931c1ae5ee40341f3567b7cf15e2
```

Par comparaison, ce qui suit est la sortie standard de la commande `ls -al` pour les fichiers `/etc/passwd` et `/etc/shadow` sur le même système.

```
# ls -al /etc/passwd
-r--r--r--   1 root     sys          542 Dec  4 17:42 /etc/passwd

# ls -al /etc/shadow
-r--------   1 root     sys          294 Oct 15 16:09 /etc/shadow
```

Exemple 5–4 Personnalisation d'un manifeste en utilisant un fichier de règles

Cet exemple montre la création d'un manifeste à l'aide d'un fichier de règles pour classifier uniquement les fichiers dans le répertoire `/etc`. Le même fichier de règles comprend les directives à suivre par la commande `bart compare` pour la surveillance des modifications apportées à l'attribut `acl` du fichier `/etc/système`.

- Utilisez un éditeur de texte pour créer un fichier de règles classifiant uniquement les fichiers du répertoire `/etc`.

```
# List information about all the files in the /etc directory.

CHECK all
/etc

# Check only acl changes in the /etc/system file

IGNORE all
CHECK acl
/etc/system
```

  Pour plus d'informations sur la création d'un fichier de règles, reportez-vous à la section "Fichier de règles BART" à la page 109.

- Créez un manifeste de contrôle en utilisant le fichier de règles que vous avez créé.

```
# bart create -r etc.rules-file > etc.system.control-manifest
! Version 1.0
! Thursday, December 11, 2003 (21:51:32)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/system F 1883 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81db61 0 3
```

- Créez un manifeste de test chaque fois que vous voulez surveiller les modifications du système. Préparez le manifeste de test exactement de la même façon que le manifeste de contrôle, à l'aide des mêmes options `bart` et du même fichier de règles.
- Comparez les manifestes en utilisant le même fichier de règles.

▼ Procédure de comparaison des manifestes pour le même système dans le temps

Utilisez cette procédure lorsque vous voulez surveiller les modifications au niveau des fichiers pour le même système dans le temps. Ce type de manifeste vous aide à localiser les fichiers corrompus ou inhabituels, détecter des violations de sécurité, ou résoudre des problèmes de performance sur un système.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Après l'installation du logiciel Oracle Solaris créez un manifeste de contrôle des fichiers que vous voulez surveiller sur le système.**

   ```
   # bart create -R /etc > control-manifest
   ```

3. **Créez un manifeste de test préparé exactement de la même façon que le manifeste de contrôle chaque fois que vous voulez surveiller les modifications apportées au système.**

   ```
   # bart create -R /etc > test-manifest
   ```

4. **Comparez le manifeste de contrôle à celui de test.**

   ```
   # bart compare options control-manifest test-manifest > bart-report
   ```

`-r`	Nom du fichier de règles pour cette comparaison. L'utilisation de l'option `-r` avec – signifie que les directives sont lues à partir de l'entrée standard.
`-i`	Permet à l'utilisateur de définir des directives `IGNORE` globales à partir de la ligne de commande.
`-p`	Mode de programmation qui génère des sorties standard non localisées pour l'analyse programmatique.
control-manifest	Sortie de la commande `bart create` pour le système de contrôle.
test-manifest	Sortie de la commande `bart create` du système de test.

5. **Recherchez les singularités dans le rapport BART**

Exemple 5–5 Comparaison des manifestes pour le même système dans le temps

Cet exemple montre la surveillance des modifications qui ont eu lieu dans le répertoire `/etc` entre deux points dans le temps. Ce type de comparaison vous permet de déterminer rapidement si des fichiers importants sur le système ont été compromis.

- Créez un manifeste de contrôle.

```
# bart create -R /etc > system1.control.121203
! Version 1.0
! Friday, December 12, 2003 (08:34:51)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
```

```
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:--- 3f81f14d
0 1 d41
d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb7
.
.
.
```

- Créez un manifeste de test lorsque vous voulez surveiller les modifications apportées au répertoire `/etc`.

```
# bart create -R /etc > system1.test.121503
Version 1.0
! Monday, December 15, 2003 (08:35:28)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:---
3f81f14d 0 1 d41d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb70 2
/.java/.systemPrefs/.system.lock F 0 100644 user::rw-,group::r--
,mask:r--,other:
r-- 3f81dcb5 0 2 d41d8cd98f00b204e9800998ecf8427e
/.java/.systemPrefs/.systemRootModFile F 0 100644 user::rw-,
group::r--,mask:r--,
other:r-- 3f81dd0b 0 2 d41d8cd98f00b204e9800998ecf8427e
.
.
.
```

- Comparez le manifeste de contrôle à celui de test.

```
# bart compare system1.control.121203 system1.test.121503
/vfstab:
  mode  control:100644  test:100777
  acl  control:user::rw-,group::r--,mask:r--,other:r--  test:user::rwx,
group::rwx,mask:rwx,other:rwx
```

La sortie ci-dessus indique les autorisations sur le fichier `vfstab` qui ont changé depuis la création du manifeste de contrôle. Ce rapport peut être utilisé pour déterminer si la propriété, la date, le contenu ou tout autre attribut de fichier a été modifié. Le fait que ce type d'informations soit disponible facilement peut vous aider à repérer l'utilisateur susceptible d'avoir altéré le fichier et le moment auquel la modification a pu survenir.

▼ Comparaison de manifestes de différents systèmes

Vous pouvez effectuer des comparaisons d'un système à l'autre, ce qui vous permet de déterminer rapidement s'il existe des différences au niveau des fichiers entre un système de référence et les autres systèmes. Par exemple, si vous avez installé une version spécifique du logiciel Oracle Solaris sur un système de référence, et que vous voulez savoir si des packages identiques sont installés sur d'autres systèmes, vous pouvez créer des manifestes pour ces systèmes, puis comparer les manifestes de test avec le manifeste de contrôle. Ce type de comparaison répertorie les écarts dans les contenus du fichier pour chaque système de test que vous comparez avec le système de contrôle.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle.**

   `# bart create` *options* `>` *control-manifest*

3. **Enregistrez le manifeste de contrôle.**

4. **Sur le système test, utilisez les mêmes options `bart` pour créer un manifeste et redirigez la sortie vers un fichier.**

   `# bart create` *options* `>` *test1-manifest*

   Choisissez un nom distinct et significatif pour le manifeste de test.

5. **Enregistrez le manifeste de test à un emplacement central sur le système jusqu'à ce que vous soyez prêt à comparer les manifestes.**

6. **Lorsque vous voulez comparer les manifestes, copiez le manifeste de contrôle à l'emplacement du manifeste de test. Ou copiez le manifeste de test sur le système de contrôle.**

   Par exemple :

   # **cp** *control-manifest /net/test-server/bart/manifests*

Si le système de test n'est pas un système monté via NFS, utilisez FTP ou un autre moyen fiable pour copier le manifeste de contrôle sur le système de test.

7 Comparez le manifeste de contrôle avec celui de test et redirigez la sortie vers un fichier.

```
# bart compare control-manifest test1-manifest > test1.report
```

8 Recherchez les singularités dans le rapport BART

9 Répétez les étapes 4 à 9 pour chaque manifeste de test que vous voulez comparer avec le manifeste de contrôle.

Utilisez les mêmes options `bart` pour chaque système de test.

Exemple 5–6 Comparaison de manifestes de différents systèmes avec le manifeste d'un système de contrôle

Cet exemple décrit la surveillance des modifications apportées au contenu du répertoire `/usr/bin` en comparant un manifeste de contrôle avec un manifeste de test d'un autre système.

- Créez un manifeste de contrôle.

```
# bart create -R /usr/bin > control-manifest.121203
!Version 1.0
! Friday, December 12, 2003 (09:19:00)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9e925 0 2
/.s F 14200 104711 user::rwx,group::--x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dcdc 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
/activation-client F 9172 100755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f5cb907 0 1 b3836ad1a656324a6e1bd01edcba28f0
/adb F 9712 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5736 0 2 5e026413175f65fb239ee628a8870eda
/addbib F 11080 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5803 0 2 a350836c36049febf185f78350f27510
.
.
.
```

- Créez un manifeste de test pour chaque système que vous souhaitez comparer avec le système de contrôle.

```
# bart create -R /usr/bin > system2-manifest.121503
! Version 1.0
! Friday, December 15, 2003 (13:30:58)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea9c 0 2
/.s F 14200 104711 user::rwx,group::---x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dcdc 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:
r-x 3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
.
.
.
```

- Lorsque vous voulez comparer des manifestes, copiez les manifestes dans le même emplacement.

  ```
  # cp control-manifest /net/system2.central/bart/manifests
  ```

- Comparez le manifeste de contrôle à celui de test.

  ```
  # bart compare control-manifest  system2.test > system2.report
  /su:
    gid  control:3  test:1
  /ypcat:
    mtime  control:3fd72511  test:3fd9eb23
  ```

La sortie précédente indique que l'ID de groupe du fichier `su` dans le répertoire `/usr/bin` n'est pas le même que celui du système de contrôle. Cette information peut être utile pour déterminer si une version différente du logiciel a été installée sur le système de test ou si quelqu'un a éventuellement manipulé ce fichier.

▼ Personnalisation d'un rapport BART en spécifiant des attributs de fichiers

Cette procédure est facultative et explique comment personnaliser un rapport BART en spécifiant des attributs de fichiers à partir de la ligne de commande. Si vous créez un manifeste de ligne de base qui répertorie des informations sur tous les fichiers ou sur des fichiers spécifiques de votre système, vous pouvez exécuter la commande `bart compare` en définissant des attributs différents, chaque fois que vous avez besoin de surveiller les modifications apportées à un répertoire, un sous-répertoire, un ou des fichiers en particulier. Vous pouvez exécuter différents types de comparaison pour les mêmes manifestes en spécifiant différents attributs de fichiers à partir de la ligne de commande.

1. **Déterminez les attributs de fichier que vous voulez surveiller.**

2. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

3. **Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle.**

4. **Créez un manifeste de test lorsque vous voulez surveiller les modifications.**

   Préparez le manifeste de test exactement de la même façon que le manifeste de contrôle.

5. **Comparez les manifestes.**

   Par exemple :

   ```
   # bart compare -i dirmtime,lnmtime,mtime control-manifest.121503 \
   test-manifest.010504 > bart.report.010504
   ```

   Notez qu'une virgule sépare chaque attribut que vous indiquez dans la syntaxe de la ligne de commande.

6. **Recherchez les singularités dans le rapport BART**

▼ Personnalisation d'un rapport BART en utilisant un fichier de règles

Cette procédure est également facultative et explique comment personnaliser un rapport BART à l'aide d'un fichier de règles comme entrée de la commande `bart compare`. En utilisant un fichier de règles, vous pouvez personnaliser un rapport BART, ce qui offre la flexibilité de spécifier plusieurs attributs pour plusieurs fichiers ou sous-arborescences. Vous pouvez exécuter différentes comparaisons pour les mêmes manifestes en utilisant différents fichiers de règles.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Déterminez les fichiers et attributs de fichier que vous voulez surveiller.**

3. **Utilisez un éditeur de texte pour créer un fichier de règles avec les directives appropriées.**

4 Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle à l'aide du fichier de règles que vous avez créé.

```
# bart create -r rules-file > control-manifest
```

5 Créez un manifeste de test préparé exactement de la même façon que le manifeste de contrôle.

```
# bart create -r rules-file > test-manifest
```

6 Comparez le manifeste de contrôle avec celui de test en utilisant le même fichier de règles.

```
# bart compare -r rules-file control-manifest test-manifest > bart.report
```

7 Recherchez les singularités dans le rapport BART

Exemple 5–7 Personnalisation d'un rapport BART en utilisant un fichier de règles

Le fichier de règles ci-après inclut les directives pour les commandes `bart create` et `bart compare`. Le fichier de règles indique à la commande `bart create` de répertorier des informations sur le contenu du répertoire `/usr/bin`. En outre, le fichier de règles indique à la commande `bart compare` de suivre uniquement les modifications de taille et de contenu dans le même répertoire.

```
# Check size and content changes in the /usr/bin directory.
# This rules file only checks size and content changes.
# See rules file example.

IGNORE all
CHECK size contents
/usr/bin
```

- Créez un manifeste de contrôle en utilisant le fichier de règles que vous avez créé.

  ```
  # bart create -r bartrules.txt > usr_bin.control-manifest.121003
  ```

- Créez un manifeste de test chaque fois que vous voulez surveiller les modifications apportées au répertoire `/usr/bin`.

  ```
  # bart create -r bartrules.txt > usr_bin.test-manifest.121103
  ```

- Comparez les manifestes en utilisant le même fichier de règles.

  ```
  # bart compare -r bartrules.txt usr_bin.control-manifest \
  usr_bin.test-manifest
  ```

- Examinez la sortie de la commande `bart compare`.

  ```
   /usr/bin/gunzip:  add
  /usr/bin/ypcat:
    delete
  ```

Dans la sortie ci-dessus, la commande `bart compare` rapporte un écart dans le répertoire `/usr/bin`. Cette sortie indique que le fichier `/usr/bin/ypcat` a été supprimé, et le fichier `/usr/bin/gunzip` ajouté.

Manifestes BART, fichiers de règles et rapports (référence)

Cette section comprend les informations de référence suivantes :

Cette section décrit le format des fichiers utilisés et créés par BART.

Format de fichier manifeste BART

Chaque entrée de fichier manifeste constitue une seule ligne, selon le type de fichier. Chaque entrée commence par *fname*, qui est le nom du fichier. Pour éviter les problèmes d'analyse provoqués par des caractères spéciaux incorporés dans les noms de fichiers, les noms de fichier sont codés. Pour plus d'informations, reportez-vous à la section "Format de fichier de règles BART" à la page 126.

Les champs ci-dessous représentent les attributs de fichier suivants :

type Type de fichier avec les valeurs possibles suivantes :

- B pour un nœud de périphérique en mode bloc
- C pour un nœud de périphérique en mode caractère
- D pour un répertoire
- F pour un fichier
- L pour un lien symbolique
- P pour un tuyau
- S pour un socket

size Taille de fichier en octets.

mode Nombre octal représentant les autorisations du fichier.

acl Attributs ACL du fichier. Pour un fichier avec des attributs ACL, contient la sortie de `acltotext()`.

uid ID utilisateur numérique du propriétaire de cette entrée.

gid L'ID de groupe numérique du propriétaire de cette entrée.

dirmtime Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les répertoires.

lnmtime Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les liens.

mtime Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les fichiers.

contents Valeur de somme de contrôle du fichier. Cet attribut n'est défini que pour des fichiers standard. Si vous désactivez la vérification du contexte ou si les sommes de contrôle ne peuvent pas être calculées, la valeur de ce champ est –.

dest Destination d'un lien symbolique.

devnode Valeur du nœud de périphérique. Cet attribut est réservé aux fichiers de périphérique en mode caractère et aux fichiers de périphériques en mode bloc.

Pour plus d'informations sur les manifestes BART, reportez-vous à la page de manuel `bart_manifest(4)`.

Format de fichier de règles BART

Les fichiers d'entrée de la commande `bart` sont des fichiers texte. Ces fichiers sont composés de lignes qui spécifient les fichiers à inclure dans le manifeste et les attributs de fichier à inclure dans le rapport. Le même fichier d'entrée peut être utilisé dans les deux parties de la fonctionnalité BART. Les lignes commençant par #, les lignes vides et les lignes qui contiennent des espaces ne sont pas prises en compte par l'outil.

Les fichiers d'entrée ont trois types de directives :

- Directive de sous-arborescence, avec modificateurs de concordance avec un modèle en option
- Directive `CHECK`
- Directive `IGNORE`

EXEMPLE 5–8 Format de fichier de règles

```
<Global CHECK/IGNORE Directives>
<subtree1> [pattern1..]
<IGNORE/CHECK Directives for subtree1>

<subtree2> [pattern2..]
<subtree3> [pattern3..]
<subtree4> [pattern4..]
<IGNORE/CHECK Directives for subtree2, subtree3, subtree4>
```

Remarque – Toutes les directives sont lues dans l'ordre. Les directives lues ultérieurement remplacent éventuellement les directives antérieures.

Il y a une directive de sous-arborescence par ligne. La directive *doit* commencer par un chemin d'accès absolu, suivi d'un zéro ou de plusieurs instructions de concordance avec un modèle.

Attributs du fichier de règles

La commande `bart` utilise les instructions `CHECK` et `IGNORE` pour définir les attributs à suivre ou à ignorer. Chaque attribut est associé à un mot-clé.

Les *mots-clés* d'attribut sont les suivants :

- `acl;`
- `all`
- `contents`
- `dest`
- `devnode`
- `dirmtime`
- `gid`
- `lnmtime`
- `mode`
- `mtime`
- `size`
- `type`
- `uid`

Le mot-clé `all` fait référence à tous les attributs d'un fichier.

Syntaxe de citation

Le langage de spécification du fichier de règles utilisé par BART est la syntaxe de citation UNIX standard pour la représentation des noms de fichier non-standard. Les caractères spéciaux, tabulations, nouvelle ligne, espace intégrés sont codés dans leurs formes octales pour activer l'outil permettant de lire des noms de fichier. Cette syntaxe de citation non uniforme empêche certains noms de fichiers, tels que ceux contenant un retour chariot intégré, d'être traités correctement dans un pipeline de commandes. Le langage de spécification des règles autorise l'expression de critères complexes de filtrage de noms de fichier, qui seraient difficiles à décrire à l'aide uniquement de la syntaxe shell.

Pour plus d'informations sur le fichier de règles BART ou la syntaxe de citation, reportez-vous à la page de manuel `bart_rules(4)`.

Génération de rapports BART

En mode par défaut, la commande `bart compare`, comme indiqué dans l'exemple suivant, vérifie tous les fichiers installés sur le système, à l'exception des horodatages de répertoire modifiés (`dirmtime`) :

```
CHECK all
IGNORE    dirmtime
```

Si vous fournissez un fichier de règles, les directives globales `CHECK all` et `IGNORE dirmtime`, dans cet ordre, sont automatiquement ajoutées au fichier de règles.

Sortie BART

Les valeurs de sortie renvoyées sont les suivantes :

0 Succès

1 Erreur non fatale lors du traitement de fichiers, telle que des problèmes d'autorisation

>1 Erreur fatale, telle qu'une option de ligne de commande non valide

Le mécanisme de génération de rapports fournit deux types de sortie : détaillée et programmatiques :

- La sortie détaillée est la sortie par défaut et est localisée et présentée sur plusieurs lignes. La sortie détaillée est internationalisée et lisible par l'homme. Lorsque la commande `bart compare` compare deux manifestes de système, une liste des différences de fichiers est générée.

  Par exemple :

  filename attribute control:xxxx test:yyyy

  filename Nom du fichier qui diffère entre le manifeste de contrôle et celui de test.

  attribute Nom de l'attribut de fichier qui diffère entre les manifestes comparés. *xxxx* est la valeur d'attribut du manifeste de contrôle et *yyyy* la valeur d'attribut de celui de test. Lorsque des écarts de plusieurs attributs se produisent dans le même fichier, chaque différence est indiquée sur une ligne distincte.

  Voici un exemple de sortie par défaut de la commande `bart compare`. Les différences d'attribut concernent le fichier `/etc/passwd`. La sortie indique que les attributs `size`, `mtime` et `contenu` ont été modifiés.

  ```
  /etc/passwd:
  size    control:74    test:81
  mtime control:3c165879    test:3c165979
  contents    control:daca28ae0de97afd7a6b91fde8d57afa
  test:84b2b32c4165887355317207b48a6ec7
  ```

- Une sortie programmatique est générée si vous utilisez l'option `-p` lorsque vous exécutez la commande `bart compare`. Cette sortie est générée dans une forme adaptée à la manipulation de programmation. Une sortie programmatique peut être facilement analysée par d'autres programmes et est conçu pour être utilisé comme entrée pour d'autres outils.

  Par exemple :

  filename attribute control-val test-val [*attribute control-val test-val*]*

filename	Identique à l'attribut *filename* dans le format par défaut
Attribut control-val test-val	Description des attributs de fichier qui diffèrent entre les manifestes de contrôle et de test pour chaque fichier.

Pour obtenir une liste des attributs pris en charge par la commande `bart`, reportez-vous à la section "Attributs du fichier de règles" à la page 127.

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

◆ ◆ ◆ CHAPITRE 6

Contrôle de l'accès aux fichiers (tâches)

Ce chapitre explique comment protéger les fichiers dans Oracle Solaris. En outre, ce chapitre explique comment protéger le système de fichiers dont les autorisations pourraient compromettre le système.

Remarque – Pour protéger les fichiers ZFS avec des ACL (listes de contrôle d'accès), reportez-vous au Chapitre 8, "Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS" du *Guide d'administration Oracle Solaris ZFS*.

Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Utilisation des autorisations UNIX pour protéger les fichiers

Les fichiers peuvent être sécurisés à l'aide des autorisations de fichiers UNIX et par l'intermédiaire des ACL. Les fichiers avec sticky bit et les fichiers exécutables nécessitent des mesures de sécurité spéciales.

Commandes d'affichage et de sécurisation des fichiers

Ce tableau décrit les commandes pour la surveillance et la sécurisation des fichiers et répertoires.

TABLEAU 6–1 Commandes de sécurisation des fichiers et répertoires

Commande	Description	Page de manuel
`ls`	Affiche la liste des fichiers dans un répertoire et des informations sur les fichiers.	`ls(1)`
`chown`	Modifie la propriété d'un fichier.	`chown(1)`
`chgrp`	Modifie le groupe propriétaire d'un fichier.	`chgrp(1)`
`chmod`	Modifie les autorisations de fichier. Vous pouvez utiliser le mode symbolique, qui utilise des lettres et des symboles, ou le mode absolu, qui utilise les octaux, pour modifier les autorisations d'un fichier.	`chmod(1)`

Propriété des fichiers et des répertoires

Les autorisations de fichiers UNIX classiques peuvent attribuer la propriété à trois catégories d'utilisateurs :

- **user –** : le propriétaire du fichier ou du répertoire, qui est généralement l'utilisateur qui a créé le fichier. Le propriétaire d'un fichier peut décider qui a le droit de lire le fichier, d'écrire dans le fichier (pour y effectuer des modifications) ou, si le fichier est une commande, d'exécuter le fichier.
- **group –** : les membres d'un groupe d'utilisateurs.
- **others –** : tous les autres utilisateurs qui ne sont ni le propriétaire du fichier, ni membres du groupe.

Le propriétaire du fichier peut généralement affecter ou modifier les autorisations de fichier. En outre, les utilisateurs ou les rôles avec des capacités d'administration, par exemple le superutilisateur ou le rôle d'administrateur principal, peuvent modifier la propriété d'un fichier. Pour remplacer la stratégie du système, reportez-vous à l'Exemple 6–2.

Il existe sept types de fichier. Chaque type est indiqué par un symbole :

- (signe moins)	Texte ou programme
b	Fichier spécial en mode bloc
c	Fichier spécial en mode caractère
d	Répertoire
l	Lien symbolique
s	Socket
D	Porte
P	Tube nommé (FIFO)

Autorisations des fichiers UNIX

Le tableau ci-dessous répertorie et décrit les autorisations que vous pouvez attribuer à chaque classe d'utilisateur pour un fichier ou un répertoire.

TABLEAU 6–2 Autorisations des fichiers et répertoires

Symbole	Autorisation	Objet	Description
`r`	Lecture	Fichier	Les utilisateurs autorisés peuvent ouvrir et lire le contenu d'un fichier.
		Répertoire	Les utilisateurs autorisés peuvent afficher la liste des fichiers dans le répertoire.
`w`	Écriture	Fichier	Les utilisateurs autorisés peuvent modifier le contenu du fichier ou le supprimer.
		Répertoire	Les utilisateurs autorisés peuvent ajouter des fichiers ou des liens dans le répertoire. Ils peuvent également supprimer des fichiers ou des liens dans le répertoire.
`x`	Exécution	Fichier	Les utilisateurs autorisés peuvent exécuter le fichier, s'il s'agit d'un programme ou d'un script shell. Ils peuvent également exécuter le programme avec l'un des appels système `exec(2)`.
		Répertoire	Les utilisateurs autorisés peuvent ouvrir les fichiers ou exécuter des fichiers dans le répertoire. Ils peuvent également définir le répertoire et les répertoires inférieurs comme étant actuels.
-	Refusé	Fichier et répertoire	Les utilisateurs désignés ne peuvent pas lire, écrire ni exécuter le fichier.

Les autorisations des fichiers s'appliquent aux fichiers classiques et aux fichiers spéciaux tels que les périphériques, les sockets et les tubes nommés (FIFO).

Pour un lien symbolique, les autorisations qui s'appliquent sont celles du fichier vers lesquels pointe le lien.

Vous pouvez protéger les fichiers dans un répertoire et ses sous-répertoires en définissant des autorisations de fichiers restrictives sur ce répertoire. Notez, cependant, que le superutilisateur a accès à tous les fichiers et répertoires sur le système.

Autorisations de fichiers spéciales (`setuid`, `setgid` et sticky bit)

Il existe trois types d'autorisations pour les fichiers exécutables et les répertoires publics : `setuid`, `setgid` et sticky bit. Lorsqu'elles sont définies, n'importe quel utilisateur qui exécute ce fichier exécutable prend l'ID du propriétaire (ou du groupe) du fichier exécutable.

Vous devez être très prudent lorsque vous définissez des autorisations spéciales, car elles constituent un risque de sécurité. Par exemple, un utilisateur peut obtenir des capacités de superutilisateur en exécutant un programme qui définit l'ID utilisateur (UID) sur `0`, qui est l'UID de `root`. En outre, tous les utilisateurs peuvent définir des autorisations spéciales pour les fichiers qu'ils détiennent, ce qui constitue un autre problème de sécurité.

Il est recommandé de surveiller votre système pour toute utilisation non autorisée des autorisations `setuid` et `setgid` pour obtenir les capacités de superutilisateur. Une autorisation suspecte accorde la propriété d'un programme d'administration à un utilisateur plutôt qu'à `root` ou `bin`. Pour rechercher et afficher la liste de tous les fichiers qui utilisent ces autorisations spéciales, reportez-vous à la section "Recherche de fichiers avec des autorisations de fichier spéciales" à la page 154.

Autorisation `setuid`

Quand l'autorisation `setuid` est définie sur un fichier exécutable, un processus qui exécute ce fichier se voit accorder l'accès sur la base du propriétaire du fichier. L'accès n'est *pas* basé sur l'utilisateur qui exécute le fichier exécutable. Ces autorisations spéciales permettent à un utilisateur d'accéder aux fichiers et répertoires qui sont normalement disponibles uniquement pour le propriétaire.

Par exemple, les autorisations `setuid` sur la commande `passwd` permettent aux utilisateurs de modifier les mots de passe. Une commande `passwd` avec une autorisation `setuid` doit ressembler à ceci :

```
-r-sr-sr-x   3 root     sys       28144 Jun 17 12:02 /usr/bin/passwd
```

Ces autorisations spéciales présentent un risque de sécurité. Certains utilisateurs déterminés peuvent trouver un moyen de conserver les autorisations qui sont leur sont accordées par le processus `setuid` même lorsque le processus a terminé de s'exécuter.

Remarque – L'utilisation des autorisations `setuid` avec des UID réservés (de 0 à 100) à partir d'un programme risque d'entraîner une définition incorrecte de l'ID d'utilisateur réel. Utilisez d'un script shell ou évitez d'utiliser les UID réservés avec les autorisations `setuid`.

Autorisation `setgid`

Les autorisations `setgid` sont similaires aux autorisations `setuid`. L'ID de groupe (GID) effectif du processus est remplacé par le groupe qui est propriétaire du fichier, et un utilisateur se voit accorder les autorisations qui sont accordées au groupe. La commande `/usr/bin/mail` dispose des autorisations `setgid` :

```
-r-x--s--x   1 root   mail     67504 Jun 17 12:01 /usr/bin/mail
```

Lorsque les autorisations `setgid` sont appliquées à un répertoire, les fichiers qui ont été créés dans ce répertoire appartiennent au groupe auquel appartient le répertoire. Les fichiers

n'appartiennent pas au groupe auquel le processus de création appartient. Tout utilisateur qui dispose d'autorisations d'écriture et d'exécution dans le répertoire peut y créer un fichier. Toutefois, le fichier appartient au groupe qui est propriétaire du répertoire, et non au groupe auquel appartient l'utilisateur.

Vous devez surveiller votre système pour toute utilisation non autorisée des autorisations `setgid` pour obtenir des capacités de superutilisateur. Des autorisations suspectes accordent l'accès de groupe à un tel programme à un groupe inhabituel plutôt qu'à `root` ou `bin`. Pour rechercher et afficher la liste de tous les fichiers qui utilisent ces autorisations, reportez-vous à la section "Recherche de fichiers avec des autorisations de fichier spéciales" à la page 154.

Sticky Bit

Le *sticky bit* est un bit d'autorisation qui protège les fichiers d'un répertoire. Si le sticky bit est défini pour le répertoire, un fichier peut être supprimé uniquement par le propriétaire du fichier, le propriétaire du répertoire ou par un utilisateur privilégié. L'utilisateur `root` et le rôle d'administrateur principal sont des exemples d'utilisateurs privilégiés. Le sticky bit empêche un utilisateur de supprimer les fichiers d'autres utilisateurs dans des répertoires publics tels que `/tmp` :

```
drwxrwxrwt 7  root  sys   400 Sep  3 13:37 tmp
```

Veillez à définir le sticky bit manuellement lorsque vous définissez un répertoire public directory dans un système de fichiers TMPFS. Pour plus d'instructions, reportez-vous à l'Exemple 6–5.

Valeur `umask` par défaut

Lorsque vous créez un fichier ou un répertoire, vous devez le créer avec un jeu d'autorisations par défaut. Les valeurs par défaut du système sont ouvertes. Un fichier texte dispose de `666` autorisations, et accorde des autorisations de lecture et d'écriture à tout le monde. Un répertoire et un fichier exécutable disposent de `777` autorisations, et accordent des autorisations de lecture, d'écriture et d'exécution à tout le monde. En règle générale, les utilisateurs remplacent les valeurs par défaut du système dans leur fichier `/etc/profile`, `.cshrc` ou `.login`.

La valeur affectée par la commande `umask` est soustraite de la valeur par défaut. Ce processus a pour effet de refuser les autorisations de la même manière que la commande `chmod` les accorde. Par exemple, la commande `chmod 022` permet d'accorder l'autorisation d'écriture au groupe et aux autres. La commande `umask 022` refuse l'accès en écriture au groupe et aux autres.

Le tableau suivant présente quelques exemples courants de paramètres `umask` et leur effet sur un fichier exécutable.

TABLEAU 6–3 Paramètres `umask` pour différents niveaux de sécurité

Niveau de sécurité	Paramètre `umask`	Autorisations refusés
Permissif (`744`)	`022`	`w` pour le groupe et les autres
Modéré (`740`)	`027`	`w` pour le groupe, `rwx` pour les autres utilisateurs
Modéré (`741`)	`026`	`w` pour le groupe, `rw` pour les autres utilisateurs
Grave (`700`)	`077`	`rwx` pour le groupe et les autres

Pour plus d'informations sur la définition de la valeur `umask`, reportez-vous à la page de manuel `umask(1)`.

Modes d'autorisation de fichier

La commande `chmod` vous permet de modifier les autorisations d'un fichier. Vous devez être le superutilisateur ou le propriétaire d'un fichier ou d'un répertoire pour modifier ses autorisations.

Vous pouvez utiliser la commande `chmod` pour définir les autorisations dans l'un des deux modes suivants :

- **Mode absolu –** : utilise les numéros pour représenter les autorisations de fichier. Lorsque vous modifiez les autorisations l'aide du mode absolu, vous représentez les autorisations pour chaque triplet par un numéro de mode octal. Le mode absolu est la méthode la plus couramment utilisée pour définir les autorisations.
- **Mode symbolique –** : utilise des combinaisons de lettres et de symboles pour ajouter ou supprimer des autorisations.

Le tableau suivant répertorie les valeurs octales pour la définition des autorisations en mode absolu. Ces numéros s'utilisent en ensembles de trois pour définir les autorisations pour le propriétaire, le groupe et les autres, dans cet ordre. Par exemple, la valeur `644` définit les autorisations de lecture et d'écriture pour le propriétaire, et les autorisations de lecture seule pour le groupe et les autres.

TABLEAU 6–4 Définition des autorisations de fichiers en mode absolu

Valeur octale	Ensemble d'autorisations de fichier	Description des autorisations
`0`	`---`	Aucune autorisation
`1`	`--x`	Autorisation d'exécution uniquement
`2`	`-w-`	Autorisation d'écriture uniquement

TABLEAU 6–4 Définition des autorisations de fichiers en mode absolu *(Suite)*

Valeur octale	Ensemble d'autorisations de fichier	Description des autorisations
3	`-wx`	Autorisations d'exécution et d'écriture
4	`r--`	Autorisation de lecture seule
5	`r-x`	Autorisations de lecture et d'exécution
6	`rw-`	Autorisations de lecture et d'écriture
7	`rwx`	Autorisations de lecture, d'écriture et d'exécution

Le tableau suivant répertorie les symboles pour la définition des autorisations de fichiers en mode symbolique. Les symboles peuvent spécifier pour qui les autorisations doivent être définies ou modifiées, l'opération à effectuer et les autorisations à affecter ou modifier.

TABLEAU 6–5 Définition des autorisations de fichiers en mode symbolique

Symbole	Fonction	Description
`u`	*who*	Utilisateur (propriétaire)
`g`	*who*	Groupe
`o`	*who*	Autres
`a`	*who*	Tous
`=`	*operator*	Assigner
`+`	*operator*	Ajouter
`-`	*operator*	Supprimer
`r`	*permissions*	Lecture
`w`	*permissions*	Écriture
`x`	*permissions*	Exécution
`l`	*permissions*	Verrouillage obligatoire, bit `setgid` activé, bit d'exécution du groupe désactivé
`s`	*permissions*	Bit `setuid` ou `setgid` activé
`t`	*permissions*	Sticky bit activé, bit d'exécution pour les autres activé

Les désignations des *who operator permissions* dans la colonne des fonctions spécifient les symboles qui modifient les autorisations du fichier ou du répertoire.

who Spécifie pour qui les autorisations doivent être modifiées.

operator Indique l'opération à effectuer.

permissions Spécifie les autorisations à modifier.

Vous pouvez définir des autorisations spéciales pour un fichier en mode absolu ou en mode symbolique. Cependant, vous devez utiliser le mode symbolique pour définir ou supprimer les autorisations `setuid` sur un répertoire. En mode absolu, vous définissez les autorisations spéciales en ajoutant une nouvelle valeur octale à la gauche du triplé d'autorisation. Le tableau suivant répertorie les valeurs octales pour la définition des autorisations spéciales d'un fichier.

TABLEAU 6–6 Définition des autorisations de fichiers spéciales en mode absolu

Valeur octale	Autorisations de fichiers spéciales
1	Sticky bit
2	`setgid`
4	`setuid`

Utilisation des ACL pour protéger les fichiers UFS

Les protections de fichier UNIX conventionnelles fournissent des autorisations de lecture, d'écriture et d'exécution pour les trois classes d'utilisateur : propriétaire de fichier, groupe de fichier et autre. Dans un système de fichiers UFS, une liste de contrôle d'accès (ACL) offre une meilleure sécurité des fichiers en permettant d'effectuer les opérations suivantes :

- définir les autorisations de fichier pour le propriétaire du fichier, le groupe, les autres, ainsi que des utilisateurs et des groupes spécifiques ;
- définir les autorisations par défaut pour chacune des catégories précédentes.

Remarque – Pour les ACL dans le système de fichiers ZFS et les ACL sur les fichiers NFSv4, reportez-vous au Chapitre 8, “Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS” du *Guide d'administration Oracle Solaris ZFS*.

Par exemple, si vous souhaitez que tous les membres d'un groupe soient en mesure de lire un fichier, vous pouvez simplement accorder des autorisations de lecture de groupe sur ce fichier. Maintenant, supposons que vous souhaitez que seule une personne dans le groupe soit en mesure d'écrire dans ce fichier. UNIX standard ne fournit pas ce niveau de sécurité des fichiers. Toutefois, une ACL fournit ce niveau de sécurité.

Sur un système de fichiers UFS, les entrées d'ACL sont définies dans un fichier par le biais de la commande `setfacl`. Les entrées d'ACL UFS se composent des champs suivants séparés par le signe deux-points :

entry-type:[*uid*|*gid*]:*perms*

entry-type Type d'entrée d'ACL sur laquelle définir les autorisations de fichiers. Par exemple, *entry-type* peut être `user` (le propriétaire d'un fichier) ou `mask` (le masque ACL). Pour obtenir la liste des entrées d'ACL, reportez-vous au Tableau 6–7 et au Tableau 6–8.

uid Nom d'utilisateur ou ID d'utilisateur (UID).

gid Nom du groupe ou ID de groupe (GID).

perms Représente les autorisations définies sur *entry-type*. *perms* peut être indiqué par les caractères symboliques `rwx` ou un nombre octal. Il s'agit des mêmes nombres que ceux utilisés avec la commande `chmod`.

Dans l'exemple suivant, une entrée d'ACL définit les autorisations de lecture et d'écriture pour l'utilisateur `stacey`.

```
user:stacey:rw-
```

Attention – Les attributs de système de fichiers UFS tels que les ACL sont pris en charge dans les systèmes de fichiers UFS uniquement. Par conséquent, si vous restaurez ou copiez des fichiers avec des entrées d'ACL dans le répertoire `/tmp`, qui est généralement monté en tant que système de fichiers TMPFS, les entrées d'ACL seront perdues. Utilisez le répertoire `/var/tmp` pour le stockage temporaire des fichiers UFS.

Entrées d'ACL pour les fichiers UFS

Le tableau suivant répertorie les entrées d'ACL valides que vous pouvez être amené à utiliser lors de la définition d'ACL sur des fichiers. Les trois premières entrées d'ACL assurent la protection de fichiers UNIX de base.

TABLEAU 6–7 Entrées d'ACL pour les fichiers UFS

Entrée d'ACL	Description
`u[ser]::`*perms*	Autorisations du propriétaire du fichier.
`g[roup]::`*perms*	Autorisations du groupe de fichiers.
`o[ther]:`*perms*	Autorisations pour les utilisateurs autres que le propriétaire du fichier ou des membres du groupe de fichiers.

TABLEAU 6–7 Entrées d'ACL pour les fichiers UFS *(Suite)*

Entrée d'ACL	Description
`m[ask]:`*perms*	Masque d'ACL. L'entrée de masque indique les autorisations maximales accordées aux utilisateurs (autres que le propriétaire) et aux groupes. Le masque est un moyen rapide de changer les autorisations pour tous les utilisateurs et groupes. Par exemple, l'entrée de masque `mask:r--` indique que les utilisateurs et groupes ne peuvent pas avoir plus que l'autorisation de lecture, même si leurs comptes indiquent qu'ils disposent d'autorisations d'écriture et d'exécution.
`u[ser]:`*uid:perms*	Autorisations pour un utilisateur spécifique. Pour *uid*, vous pouvez spécifier un nom d'utilisateur ou un ID d'utilisateur (UID) numérique.
`g[roup]:`*gid:perms*	Autorisations pour un groupe spécifique. Pour *gid*, vous pouvez spécifier un nom de groupe ou un ID de groupe (GID) numérique.

Entrées d'ACL pour les répertoires UFS

Outre les entrées d'ACL décrites dans le Tableau 6–7, vous pouvez définir les entrées d'ACL par défaut dans un répertoire. Les fichiers ou répertoires créés dans un répertoire doté d'entrées d'ACL par défaut auront les mêmes entrées d'ACL que les entrées d'ACL par défaut. Le Tableau 6–8 répertorie les entrées d'ACL par défaut pour les répertoires.

Lorsque vous définissez pour la première fois les entrées d'ACL par défaut pour des utilisateurs et des groupes spécifiques sur un répertoire, vous devez également définir les valeurs par défaut des entrées d'ACL pour le propriétaire du fichier, le groupe de fichiers, les autres et le masque d'ACL. Ces entrées sont obligatoires. Ils s'agit des quatre premières entrées d'ACL par défaut dans le tableau ci-dessous.

TABLEAU 6–8 Entrées d'ACL par défaut pour les répertoires UFS

Entrée d'ACL par défaut	Description
`d[efault]:u[ser]::`*perms*	Autorisations du propriétaire du fichier par défaut.
`d[efault]:g[roup]::`*perms*	Autorisations du groupe de fichiers par défaut.
`d[efault]:o[ther]:`*perms*	Autorisations par défaut pour les utilisateurs autres que le propriétaire du fichier ou les membres du groupe de fichiers.
`d[efault]:m[ask]:`*perms*	Masque par défaut de l'ACL.
`d[efault]:u[ser]:`*uid:perms*	Autorisations par défaut pour un utilisateur spécifique. Pour *uid*, vous pouvez spécifier un nom d'utilisateur ou un ID d'utilisateur (UID) numérique.
`d[efault]:g[roup]:`*gid:perms*	Autorisations par défaut pour un groupe spécifique. Pour *gid*, vous pouvez spécifier un nom de groupe ou un ID de groupe (GID) numérique.

Commandes pour l'administration des ACL d'UFS

Les commandes ci-dessous administrent les ACL sur les fichiers ou les répertoires UFS.

Commande `setfacl`	Définit, ajoute, modifie et supprime les entrées d'ACL. Pour plus d'informations, reportez-vous à la page de manuel `setfacl(1)`.
Commande `getfacl`	Affiche les entrées d'ACL. Pour plus d'informations, reportez-vous à la page de manuel `getfacl(1)`.

Prévention des problèmes de sécurité causés par les fichiers exécutables

Un certain nombre de bogues de sécurité sont liés aux piles exécutables par défaut lorsque leurs autorisations sont définies sur lecture, écriture et exécution. Alors que les piles avec autorisations d'exécution sont autorisées, la plupart des programmes peuvent fonctionner correctement sans utiliser de piles exécutables.

La variable `noexec_user_stack` vous permet de spécifier si les mappages de pile sont exécutables. La variable est disponible à partir de la version Solaris 2.6. Par défaut, cette variable est définie sur zéro, à l'exception des applications 64 bits, et fournit le comportement conforme ABI. Si la variable est définie sur une valeur non nulle, le système marque la pile de chaque processus dans le système comme étant accessible en lecture et en écriture, mais non exécutable.

Une fois que cette variable est définie, un signal `SIGSEGV` est envoyé aux programmes qui tentent d'exécuter du code sur leur pile. Ce signal résulte généralement en un arrêt du programme à l'aide d'un core dump. Ces programmes génèrent également un message d'avertissement qui inclut le nom du programme concerné, l'ID de processus, et l'UID réel de l'utilisateur à l'origine de l'exécution du programme. Par exemple :

```
a.out[347] attempt to execute code on stack by uid 555
```

Le message est consigné par le démon `syslog` lorsque la fonctionnalité `syslog kern` est définie sur le niveau `notice`. Cet enregistrement est défini par défaut dans le fichier `syslog.conf`, ce qui signifie que le message est envoyé à la console et au fichier `/var/adm/messages`. Pour plus d'informations, reportez-vous aux pages de manuel `syslogd(1M)` et `syslog.conf(4)`.

Le message `syslog` est utile pour l'observation de problèmes de sécurité potentiels. Le message identifie également les programmes valides qui dépendent des piles exécutable dont le bon fonctionnement est empêché par la définition de cette variable. Si vous ne voulez pas que les messages soient consignés, définissez la variable `noexec_user_stack_log` sur zéro dans le fichier `/etc/system`. Bien que les messages ne soient pas consignés, le signal SIGSEGV peut continuer d'entraîner l'arrêt du programme d'exécution à l'aide d'un core dump.

Vous pouvez utiliser la fonction `mprotect()` si vous souhaitez que les programmes marquent explicitement leur pile comme exécutable. Pour plus d'informations, reportez-vous à la page de manuel `mprotect(2)`.

En raison de limitations matérielles, la capacité de détection et de signalement des problèmes de pile exécutable n'est pas disponible sur la plupart les systèmes x86. Les systèmes de la famille de produits AMD64 peuvent détecter et signaler les problèmes de pile exécutable.

Protection des fichiers (liste des tâches)

La liste des tâches suivante présente des ensembles de procédures de protection de fichiers.

Tâche	Description	Voir
Utilisation des autorisations UNIX pour protéger les fichiers	Affiche les autorisations UNIX sur les fichiers. Protège les fichiers à l'aide d'autorisations UNIX.	"Protection des fichiers avec des autorisations UNIX (liste des tâches)" à la page 142
Utilisation des ACL pour protéger les fichiers	Ajoute des ACL pour protéger les fichiers à un niveau plus précis que les autorisations UNIX.	"Protection de fichiers UFS à l'aide des ACL (liste des tâches)" à la page 148
Protection du système contre les fichiers qui présentent un risque de sécurité	Détecte les fichiers exécutables dont le propriétaire est suspect. Désactive les fichiers qui peuvent endommager le système.	"Protection contre les programmes présentant des risques de sécurité (liste des tâches)" à la page 154

Protection des fichiers avec des autorisations UNIX (liste des tâches)

La liste des tâches suivante présente les procédures permettant de répertorier les autorisations de fichiers, des les modifier et de protéger les fichiers avec les autorisations de fichiers spéciales.

Tâche	Voir
Affichage des informations de fichier	"Affichage des informations de fichier" à la page 143
Modification des propriétaires des fichiers	"Modification du propriétaire d'un fichier local" à la page 144 "Modification de la propriété de groupe d'un fichier" à la page 145
Modification des autorisations de fichier	"Modification des autorisations de fichier en mode symbolique" à la page 145 "Modification des autorisations de fichier en mode absolu" à la page 146 "Modification des autorisations de fichier spéciales en mode absolu" à la page 147

▼ Affichage des informations de fichier

Affichez les informations sur tous les fichiers d'un répertoire en utilisant la commande `ls`.

- **Tapez la commande suivante pour afficher une longue liste de tous les fichiers dans le répertoire en cours.**

```
% ls -la
```

`-l` Affiche le format long qui inclut la propriété d'utilisateur, la propriété de groupe et les autorisations du fichier.

`-a` Affiche tous les fichiers, y compris les fichiers cachés qui commencent par un point (`.`).

Exemple 6–1 Affichage des informations de fichier

Dans l'exemple suivant, une liste partielle de fichiers dans le répertoire `/sbin` s'affiche.

```
% cd /sbin
% ls -la
total 13456
drwxr-xr-x   2 root     sys          512 Sep  1 14:11 .
drwxr-xr-x  29 root     root        1024 Sep  1 15:40 ..
-r-xr-xr-x   1 root     bin       218188 Aug 18 15:17 autopush
lrwxrwxrwx   1 root     root          21 Sep  1 14:11 bpgetfile -> ...
-r-xr-xr-x   1 root     bin       505556 Aug 20 13:24 dhcpagent
-r-xr-xr-x   1 root     bin       456064 Aug 20 13:25 dhcpinfo
-r-xr-xr-x   1 root     bin       272360 Aug 18 15:19 fdisk
-r-xr-xr-x   1 root     bin       824728 Aug 20 13:29 hostconfig
-r-xr-xr-x   1 root     bin       603528 Aug 20 13:21 ifconfig
-r-xr-xr-x   1 root     sys       556008 Aug 20 13:21 init
-r-xr-xr-x   2 root     root      274020 Aug 18 15:28 jsh
-r-xr-xr-x   1 root     bin       238736 Aug 21 19:46 mount
-r-xr-xr-x   1 root     sys         7696 Aug 18 15:20 mountall
   .
   .
   .
```

Chaque ligne affiche des informations sur un fichier dans l'ordre suivant :

- Type de fichier : par exemple, `d`. Pour obtenir la liste des types de fichiers, reportez-vous à la section "Propriété des fichiers et des répertoires" à la page 132.
- Autorisations : par exemple, `r-xr-xr-x`. Pour obtenir une description, reportez-vous à la section "Propriété des fichiers et des répertoires" à la page 132.
- Nombre de liens fixes : par exemple, `2`.
- Propriétaire du fichier : par exemple, `root`.
- Groupe du fichier : par exemple, `bin`.
- Taille du fichier, en octets : par exemple, `7696`.
- Date à laquelle le fichier créé ou modifié pour la dernière fois : par exemple, `Aug 18 15:20`.

- Nom du fichier : par exemple, `mountall`.

▼ Modification du propriétaire d'un fichier local

L'administrateur principal ou le rôle de superutilisateur peut modifier le propriétaire de n'importe quel fichier.

1 Affichez les autorisations d'un fichier.

```
% ls -l example-file
-rw-r--r--   1 janedoe   staff   112640 May 24 10:49 example-file
```

2 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

3 Modifiez le propriétaire du fichier.

```
# chown stacey example-file
```

4 Vérifiez que le propriétaire du fichier a bien été modifié.

```
# ls -l example-file
-rw-r--r--   1 stacey   staff   112640 May 26 08:50 example-file
```

Exemple 6–2 Modification par les utilisateurs de la propriété de leurs propres fichiers

Considération de sécurité : vous devez avoir une bonne raison de modifier la valeur de la variable `rstchown` à zéro. Ce paramètre permet à un utilisateur de modifier la propriété de ses fichiers en un autre nom d'utilisateur.

Dans cet exemple, la valeur de la variable `rstchown` est définie sur zéro dans le fichier `/etc/system`. Ce paramètre permet au propriétaire d'un fichier d'utiliser la commande `chown` pour modifier la propriété du fichier à un autre utilisateur. Ce paramètre permet également au propriétaire d'utiliser la commande `chgrp` pour définir le groupe propriétaire d'un fichier sur un groupe auquel dont le propriétaire n'appartient pas. Le changement entre en vigueur lors du redémarrage du système.

```
set rstchown = 0
```

Pour plus d'informations, reportez-vous aux pages de manuel `chown(1)` et `chgrp(1)`.

Par ailleurs, n'oubliez pas que les systèmes de fichiers montés sur NFS ont des restrictions supplémentaires en ce qui concerne la modification de la propriété et des groupes. Pour plus

d'informations sur la restriction de l'accès aux systèmes montés sur NFS, reportez-vous au Chapitre 6, "Accès aux systèmes de fichiers réseau (référence) " du *Guide d'administration système : Services réseau*.

▼ Modification de la propriété de groupe d'un fichier

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Modifiez la propriété de groupe d'un fichier.**

```
$ chgrp scifi example-file
```

Pour plus d'informations sur la définition des groupes, reportez-vous au Chapitre 4, "Gestion des comptes utilisateur et des groupes (présentation) " du *Guide d'administration système : administration de base*.

3 **Vérifiez que la propriété de groupe du fichier a changé.**

```
$ ls -l example-file
 -rw-r--r--   1 stacey   scifi   112640 June 20 08:55  example-file
```

Reportez-vous également à l'Exemple 6–2.

▼ Modification des autorisations de fichier en mode symbolique

1 **Si vous n'êtes pas le propriétaire du fichier ou du répertoire, connectez-vous en tant que superutilisateur ou équivalent.**

Seul le propriétaire actuel ou le superutilisateur peut utiliser la commande `chmod` pour modifier les autorisations d'un fichier ou d'un répertoire.

2 **Modifiez les autorisations en mode symbolique.**

`% chmod` *who operator permissions filename*

who	Spécifie pour qui les autorisations doivent être modifiées.
operator	Indique l'opération à effectuer.
permissions	Spécifie les autorisations à modifier. Pour obtenir la liste des symboles valides, reportez-vous au Tableau 6–5.

filename Spécifie le fichier ou répertoire.

3 Vérifiez que les autorisations du fichier ont changé.

```
% ls -l filename
```

Exemple 6–3 Modification des autorisations en mode symbolique

Dans l'exemple ci-dessous, l'autorisation de lecture est retirée aux autres.

```
% chmod o-r example-file1
```

Dans l'exemple suivant, les autorisations de lecture et d'exécution sont ajoutées pour l'utilisateur, le groupe et les autres.

```
$ chmod a+rx example-file2
```

Dans l'exemple suivant, les autorisations de lecture, d'écriture et d'exécution sont attribuées au groupe.

```
$ chmod g=rwx example-file3
```

▼ Modification des autorisations de fichier en mode absolu

1 Si vous n'êtes pas le propriétaire du fichier ou du répertoire, connectez-vous en tant que superutilisateur ou équivalent.

Seul le propriétaire actuel ou le superutilisateur peut utiliser la commande `chmod` pour modifier les autorisations d'un fichier ou d'un répertoire.

2 Modifiez les autorisations en mode absolu.

```
% chmod nnn filename
```

nnn Spécifie les valeurs octales qui représentent les autorisations du propriétaire du fichier, du groupe de fichiers et autres, dans cet ordre. Pour obtenir la liste des valeurs octales, reportez-vous au Tableau 6–4.

filename Spécifie le fichier ou répertoire.

Remarque – Lorsque vous utilisez la commande `chmod` pour modifier les autorisations de groupe sur un fichier avec des entrées d'ACL, les autorisations de groupe de fichiers et le masque d'ACL sont modifiés et reflètent les nouvelles autorisations. N'oubliez pas que les nouvelles autorisations du masque d'ACL peuvent modifier les autorisations d'autres utilisateurs et de groupes qui disposent d'entrées d'ACL sur le fichier. Utilisez la commande `getfacl` pour vous assurer que les autorisations appropriées sont définies pour toutes les entrées d'ACL. Pour plus d'informations, reportez-vous à la page de manuel `getfacl(1)`.

3 **Vérifiez que les autorisations du fichier ont changé.**

```
% ls -l filename
```

Exemple 6–4 Modification des autorisations en mode absolu

Dans l'exemple ci-dessous, les autorisations d'un répertoire public sont modifiées de `744` (lecture, écriture, exécution ; lecture seule ; et lecture seule) en `755` (lecture, écriture, exécution ; lecture et exécution ; et lecture et exécution).

```
# ls -ld public_dir
drwxr--r--  1 jdoe   staff    6023 Aug  5 12:06 public_dir
# chmod 755 public_dir
# ls -ld public_dir
drwxr-xr-x  1 jdoe   staff    6023 Aug  5 12:06 public_dir
```

Dans l'exemple suivant, les autorisations d'un script de shell exécutable sont modifiées de lecture et écriture en lecture, écriture et exécution.

```
% ls -l my_script
-rw------- 1 jdoe   staff    6023 Aug  5 12:06 my_script
% chmod 700 my_script
% ls -l my_script
-rwx------ 1 jdoe   staff    6023 Aug  5 12:06 my_script
```

▼ Modification des autorisations de fichier spéciales en mode absolu

1 **Si vous n'êtes pas le propriétaire du fichier ou du répertoire, connectez-vous en tant que superutilisateur ou équivalent.**

Seul le propriétaire actuel ou un utilisateur avec des capacités de superutilisateur peut utiliser la commande `chmod` pour modifier les autorisations d'un fichier ou d'un répertoire.

2 **Modifiez les autorisations spéciales en mode absolu.**

```
% chmod nnnn filename
```

nnnn Spécifie les valeurs octales qui modifient les autorisations du fichier ou du répertoire. La valeur octale le plus à gauche définit les autorisations spéciales du fichier. Pour obtenir la liste de valeurs octales valides pour les autorisations spéciales, reportez-vous au Tableau 6–6.

filename Spécifie le fichier ou répertoire.

Remarque – Lorsque vous utilisez la commande `chmod` pour modifier les autorisations de groupe sur un fichier avec des entrées d'ACL, les autorisations de groupe de fichiers et le masque d'ACL sont modifiés et reflètent les nouvelles autorisations. N'oubliez pas que les nouvelles autorisations du masque d'ACL peuvent modifier les autorisations d'autres utilisateurs et de groupes qui disposent d'entrées d'ACL sur le fichier. Utilisez la commande `getfacl` pour vous assurer que les autorisations appropriées sont définies pour toutes les entrées d'ACL. Pour plus d'informations, reportez-vous à la page de manuel `getfacl(1)`.

---

3 Vérifiez que les autorisations du fichier ont changé.

```
% ls -l filename
```

Exemple 6–5 Définition des autorisations de fichiers spéciales en mode absolu

Dans l'exemple suivant, l'autorisation `setuid` est définie sur le fichier `dbprog`.

```
# chmod 4555 dbprog
# ls -l dbprog
-r-sr-xr-x   1 db     staff        12095 May  6 09:29 dbprog
```

Dans l'exemple suivant, l'autorisation `setgid` est définie sur le fichier `dbprog2`.

```
# chmod 2551 dbprog2
# ls -l dbprog2
-r-xr-s--x   1 db     staff       24576 May  6 09:30 dbprog2
```

Dans l'exemple suivant, l'autorisation Sticky bit est définie dans le répertoire `public_dir`.

```
# chmod 1777 public_dir
# ls -ld public_dir
drwxrwxrwt   2 jdoe   staff          512 May 15 15:27 public_dir
```

Protection de fichiers UFS à l'aide des ACL (liste des tâches)

La liste des tâches suivante présente les procédures qui répertorient les ACL sur un système de fichiers UFS, modifient les ACL et copient les ACL dans un autre fichier.

Tâche	Voir
Vérification de la présence d'une ACL dans un fichier	"Vérification de la présence d'une ACL dans un fichier" à la page 149
Ajout d'une ACL à un fichier	"Ajout d'entrées d'ACL à un fichier" à la page 149
Copie d'une ACL	"Copie d'une ACL" à la page 151
Modification d'une ACL	"Modification d'entrées d'ACL sur un fichier" à la page 151
Suppression des ACL d'un fichier	"Suppression d'entrées d'ACL sur un fichier" à la page 152
Affichage des ACL dans un fichier	"Affichage des entrées d'ACL d'un fichier" à la page 153

▼ Vérification de la présence d'une ACL dans un fichier

- **Vérifiez si un fichier dispose d'une ACL.**

  `% ls -l` *filename*

  Où *filename* spécifie le fichier ou répertoire.

  Dans la sortie, un signe plus (+) à la droite du champ mode indique que le fichier possède une ACL.

  Remarque – Sauf si vous avez ajouté des entrées d'ACL qui étendent les autorisations de fichier UNIX, un fichier est considéré comme ayant une ACL dite triviale et le signe plus (+) ne s'affiche pas.

Exemple 6–6 Vérification de la présence d'une ACL dans un fichier

Dans l'exemple suivant, le fichier `ch1.sgm` dispose d'une ACL. L'ACL est indiquée par le signe plus (+) à la droite du champ mode.

```
% ls -l ch1.sgm
-rwxr-----+  1 stacey   techpubs      167 Nov 11 11:13 ch1.sgm
```

▼ Ajout d'entrées d'ACL à un fichier

1. **Définissez une ACL dans un fichier en utilisant la commande `setfacl`.**

   `% setfacl -s user::`*perms*`,group::`*perms*`,other:`*perms*`,mask:`*perms*`,`*acl-entry-list* *filename* ...

   `-s` Définit une ACL sur le fichier. Si un fichier possède déjà une ACL, elle est remplacé. Cette option nécessite au moins les entrées `user::`, `group::` et `other::`.

   `user::`*perms* Spécifie les autorisations du propriétaire du fichier.

`group::`*perms*	Spécifie les autorisations de propriété de groupe.
`other:`*perms*	Spécifie les autorisations pour les utilisateurs autres que le propriétaire du fichier ou les membres du groupe.
`mask:`*perms*	Spécifie les autorisations pour le masque d'ACL. Le masque indique les autorisations maximales accordées aux utilisateurs (autres que le propriétaire) et aux groupes.
acl-entry-list	Spécifie la liste d'une ou plusieurs entrées d'ACL à définir pour des utilisateurs et groupes spécifiques sur le fichier ou le répertoire. Vous pouvez également définir des entrées d'ACL par défaut sur un répertoire. Les entrées d'ACL valides sont répertoriées dans le Tableau 6–7 et le Tableau 6–8.
filename ...	Spécifie un ou plusieurs fichiers ou répertoires sur lesquels définir l'ACL. S'il y a plusieurs *filename*, ils sont séparés par des espaces.

Attention – Si une ACL existe déjà sur le fichier, l'option `-s` remplace l'intégralité de l'ACL par la nouvelle ACL.

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

2 Vérifiez que les entrées d'ACL ont été définies dans le fichier.

```
% getfacl filename
```

Pour plus d'informations, reportez-vous à la section "Vérification de la présence d'une ACL dans un fichier" à la page 149.

Exemple 6–7 Définition d'une ACL sur un fichier

Dans l'exemple suivant, les autorisations du propriétaire du fichier sont définies sur lecture et écriture, celles du groupe de fichiers sont définies sur lecture seule et celles des autres sont définies sur aucun pour le fichier `ch1.sgm`. En outre, l'utilisateur `anusha` dispose d'autorisations de lecture et d'écriture sur le fichier. Les autorisations du masque d'ACL sont définies sur lecture et écriture, ce qui signifie qu'aucun utilisateur ni groupe ne dispose d'autorisation d'exécution.

```
% setfacl -s user::rw-,group::r--,other:---,mask:rw-,user:anusha:rw- ch1.sgm
% ls -l
total 124
-rw-r-----+  1 stacey  techpubs   34816 Nov 11 14:16 ch1.sgm
-rw-r--r--   1 stacey  techpubs   20167 Nov 11 14:16 ch2.sgm
-rw-r--r--   1 stacey  techpubs    8192 Nov 11 14:16 notes
% getfacl ch1.sgm
# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:rw-    #effective:rw-
group::r--         #effective:r--
```

```
mask:rw-
other:---
```

Dans l'exemple suivant, le propriétaire du fichier définit les autorisations de lecture, d'écriture et d'exécution, les autorisations du groupe de fichiers sont définies sur lecture seule et celles des autres sont définies sur la valeur aucun. En outre, les autorisations du masque d'ACL sont définies en lecture sur le fichier `ch2.sgm`. Enfin, l'utilisateur `anusha` dispose d'autorisations de lecture et d'écriture. Cependant, en raison du masque d'ACL, les autorisations pour `anusha` sont de lecture seule.

```
% setfacl -s u::7,g::4,o:0,m:4,u:anusha:7 ch2.sgm
% getfacl ch2.sgm
# file: ch2.sgm
# owner: stacey
# group: techpubs
user::rwx
user:anusha:rwx         #effective:r--
group::r--              #effective:r--
mask:r--
other:---
```

▼ Copie d'une ACL

- **Copiez l'ACL d'un fichier sur un autre fichier en redirigeant la sortie `getfacl`.**

  `% getfacl` *filename1* `| setfacl -f -` *filename2*

  filename1 Spécifie le fichier à partir duquel vous souhaitez copier l'ACL.

  filename2 Spécifie le fichier sur lequel vous voulez définir l'ACL copiée.

Exemple 6–8 Copie d'une ACL

Dans l'exemple suivant, l'ACL sur `ch2.sgm` est copiée sur `ch3.sgm`.

```
% getfacl ch2.sgm | setfacl -f - ch3.sgm
```

▼ Modification d'entrées d'ACL sur un fichier

1. **Modifiez les entrées d'ACL sur un fichier à l'aide de la commande `setfacl`.**

   `% setfacl -m` *acl-entry-list filename ...*

   `-m` Modifie l'entrée d'ACL existante.

acl-entry-list Spécifie la liste d'une ou plusieurs entrées d'ACL à modifier dans le fichier ou le répertoire. Vous pouvez également modifier les entrées d'ACL par défaut dans un répertoire. Les entrées d'ACL valides sont répertoriées dans le Tableau 6–7 et le Tableau 6–8.

filename ... Spécifie un ou plusieurs fichiers ou répertoires, séparés par un espace.

2 Vérifiez que les entrées d'ACL ont été modifiées sur le fichier.

```
% getfacl filename
```

Exemple 6–9 Modification d'entrées d'ACL sur un fichier

Dans l'exemple ci-dessous, les autorisations de l'utilisateur `anusha` sont modifiées sur lecture et écriture.

```
% setfacl -m user:anusha:6 ch3.sgm
% getfacl ch3.sgm
# file: ch3.sgm
# owner: stacey
# group: techpubs
user::rw-
user::anusha:rw-        #effective:r--
group::r-               #effective:r--
mask:r--
other:r-
```

Dans l'exemple suivant, les autorisations par défaut pour le groupe `staff` sont modifiées en lecture sur le répertoire `book`. En outre, les autorisations du masque d'ACL par défaut sont modifiées en lecture et écriture.

```
% setfacl -m default:group:staff:4,default:mask:6 book
```

▼ Suppression d'entrées d'ACL sur un fichier

1 Supprimez les entrées d'ACL dans un fichier.

```
% setfacl -d acl-entry-list filename ...
```

`-d` Supprime les entrées d'ACL spécifiées.

acl-entry-list Spécifie la liste des entrées d'ACL (sans spécifier les autorisations) à supprimer dans le fichier ou répertoire. Vous pouvez supprimer les entrées d'ACL et les entrées d'ACL par défaut pour des utilisateurs et des groupes spécifiques. Les entrées d'ACL valides sont répertoriées dans le Tableau 6–7 et le Tableau 6–8.

filename ... Spécifie un ou plusieurs fichiers ou répertoires, séparés par un espace.

Vous pouvez également utiliser la commande `setfacl -s` pour supprimer toutes les entrées d'ACL sur un fichier et les remplacer par les nouvelles entrées d'ACL spécifiées.

2 Vérifiez que les entrées d'ACL ont été supprimée du fichier.

```
% getfacl filename
```

Exemple 6–10 Suppression d'entrées d'ACL sur un fichier

Dans l'exemple ci-dessous, l'utilisateur `anusha` est supprimé du fichier `ch4.sgm`.

```
% setfacl -d user:anusha ch4.sgm
```

▼ Affichage des entrées d'ACL d'un fichier

- **Affichez les entrées d'ACL dans un fichier en utilisant la commande `getfacl`.**

  ```
  % getfacl [-a | -d] filename ...
  ```

  `-a` Affiche le nom du fichier, son propriétaire, le groupe de fichiers, et les entrées d'ACL pour le fichier ou le répertoire spécifié.

  `-d` Affiche le nom du fichier, son propriétaire, le groupe de fichiers, et les entrées d'ACL par défaut, si elles existent, pour le répertoire spécifié.

  filename ... Spécifie un ou plusieurs fichiers ou répertoires, séparés par un espace.

  Si vous spécifiez plusieurs noms de fichier sur la ligne de commande, les entrées d'ACL sont affichées avec une ligne vide entre chaque entrée.

Exemple 6–11 Affichage des entrées d'ACL d'un fichier

Dans l'exemple ci-dessous, toutes les entrées d'ACL pour le fichier `ch1.sgm` s'affichent. La note `#effective:` en regard des entrées d'utilisateur et de groupe indique quels sont les autorisations après modification par le masque d'ACL.

```
% getfacl ch1.sgm

# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:r-        #effective:r--
group::rw-            #effective:rw-
mask:rw-
other:---
```

Dans l'exemple suivant, les entrées d'ACL par défaut pour le répertoire `book` s'affichent.

```
% getfacl -d book

# file: book
# owner: stacey
# group: techpubs
user::rwx
user:anusha:r-x       #effective:r-x
group::rwx            #effective:rwx
mask:rwx
other:---
default:user::rw-
default:user:anusha:r--
default:group::rw-
default:mask:rw-
default:other:---
```

Protection contre les programmes présentant des risques de sécurité (liste des tâches)

La liste des tâches suivante présente les procédures permettant trouver les exécutables à risque dans le système, et qui empêchent les programmes d'exploiter une pile exécutable.

Tâche	Description	Voir
Recherche de fichiers avec des autorisations spéciales	Localise les fichiers avec l'ensemble de bits `setuid`, mais non détenus par l'utilisateur `root`.	"Recherche de fichiers avec des autorisations de fichier spéciales" à la page 154
Empêchement du débordement de pile exécutable	Empêche les programmes d'exploiter une pile exécutable.	"Désactivation de l'utilisation de piles exécutables par les programmes" à la page 156
Empêchement de la journalisation des messages de pile exécutable	Désactive la journalisation des messages de pile exécutable.	Exemple 6–13

▼ Recherche de fichiers avec des autorisations de fichier spéciales

Il est conseillé de surveiller votre système pour vérifier les autorisations `setuid` et `setgid` sur les programmes. Les autorisations `setuid` et `setgid` permettent aux utilisateurs standard d'obtenir les capacités de superutilisateur. Un fichier exécutable suspect accorde la propriété à un utilisateur plutôt qu'à `root` ou `bin`.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Recherchez les fichiers avec des autorisations `setuid` en utilisant la commande `find`.**

   ```
   # find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/filename
   ```

`find` *répertoire*	Vérifie tous les chemins montés en commençant par le *répertoire* spécifié, qui peut être root (`/`), `sys`, `bin`, ou `mail`.
`-user root`	Affiche les fichiers appartenant uniquement à `root`.
`-perm -4000`	Affiche les fichiers uniquement avec les autorisations définies sur `4000`.
`-exec ls -ldb`	Affiche le résultat de la commande `find` au format `ls -ldb`.
`/tmp/`*filename*	Il s'agit du fichier qui contient les résultats de la commande `find`.

3. **Affichez les résultats dans `/tmp/`*filename*.**

   ```
   # more /tmp/filename
   ```

   Pour plus d'informations d'ordre général sur les autorisations `setuid`, reportez-vous à la section “Autorisation `setuid`” à la page 134.

Exemple 6–12 Recherche de fichiers avec des autorisations `setuid`

La sortie de l'exemple suivant indique qu'un utilisateur d'un groupe appelé `rar` a effectué une copie personnelle de `/usr/bin/sh` et a défini les autorisations `setuid` sur `root`. Par conséquent, le programme `/usr/rar/bin/sh` s'exécute avec les autorisations `root`.

Ce résultat a été enregistré pour référence ultérieure en déplaçant le répertoire `/var/tmp/chkprm` dans le répertoire `/export/sysreports/ckprm`.

```
# find / -user root -perm -4000 -exec ls -ldb {} \; > /var/tmp/ckprm
# cat /var/tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
# mv /var/tmp/ckprm /export/sysreports/ckprm
```

▼ Désactivation de l'utilisation de piles exécutables par les programmes

Pour obtenir une description des risques de sécurité liés aux piles exécutables, reportez-vous à la section "Prévention des problèmes de sécurité causés par les fichiers exécutables" à la page 141.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Modifiez le fichier `/etc/système` et ajoutez la ligne suivante :**

   ```
   set noexec_user_stack=1
   ```

3. **Redémarrez le système.**

   ```
   # init 6
   ```

Exemple 6–13 Désactivation de la journalisation des messages de pile exécutable

Dans cet exemple, la journalisation des messages de pile exécutable est désactivée et le système est ensuite redémarré.

```
# cat /etc/system
set noexec_user_stack=1
set noexec_user_stack_log=0
# init 6
```

◆ ◆ ◆ CHAPITRE 7

Utilisation d'Automated Security Enhancement Tool (Tâches)

Ce chapitre décrit l'utilisation de l'outil Automated Security Enhancement Tool (ASET) pour surveiller ou restreindre l'accès aux fichiers et répertoires du système.

Vous trouverez ci-après une liste des instructions relatives à chaque étape décrite dans ce chapitre.

Pour un outil plus complet qu'ASET, utilisez le logiciel Oracle Solaris Security Toolkit. Oracle Solaris Security Toolkit fournit une structure pour la sécurisation et la réduction d'un système Oracle Solaris. Cette boîte à outils comprend un outil de profilage, un outil de génération de rapports et une fonction d'annulation. Pour plus d'informations, reportez-vous à la section "Utilisation de la Oracle Solaris Security Toolkit " à la page 53.

Automated Security Enhancement Tool (ASET)

L'outil Automated Security Enhancement Tool (ASET) est inclus dans le SE Oracle Solaris. ASET vous aide à contrôler la sécurité du système en effectuant automatiquement des tâches que vous feriez autrement manuellement.

Le package de sécurité ASET fournit des outils d'administration automatisés permettant de contrôler et surveiller la sécurité de votre système. Vous devez spécifier un niveau de sécurité pour l'exécution d'ASET. Les niveaux de sécurité disponibles sont faible, moyen et élevé. À chaque niveau supérieur, les fonctions de contrôle de fichiers d'ASET augmentent afin de réduire l'accès aux fichiers et de renforcer la sécurité de votre système.

ASET exécute sept tâches. Chacune d'entre elle effectue des vérifications spécifiques et apporte des modifications aux fichiers système. Les tâches ASET renforcent les autorisations des fichiers, vérifient le contenu des fichiers système critiques afin d'y détecter d'éventuelles

défaillances de sécurité et contrôlent des zones cruciales. ASET peut également protéger un réseau en appliquant les exigences de base d'un système pare-feu à un système servant de passerelle. Reportez-vous à la section “Configuration du pare-feu” à la page 161.

ASET utilise des fichiers maîtres pour la configuration. Les fichiers maîtres, rapports et autres fichiers ASET se trouvent dans le répertoire `/usr/aset`. Ces fichiers peuvent être modifiés afin de les adapter aux besoins particuliers de votre site.

Chaque tâche génère un rapport. Les rapports signalent les défaillances de sécurité détectées et les modifications apportées aux fichiers système au cours de la tâche. Lorsque l'outil ASET est exécuté au niveau de sécurité le plus élevé, il tente de modifier toutes les défaillances de sécurité du système. Si ASET ne peut pas corriger un problème de sécurité potentiel, il signale l'existence de ce problème dans un rapport.

Vous pouvez lancer une session ASET en utilisant la commande `/usr/aset/aset` de manière interactive. Vous pouvez également configurer ASET pour qu'il s'exécute périodiquement en plaçant une entrée dans le fichier `crontab`.

Les tâches ASET entraînent une forte activité sur le disque. Elles peuvent interférer avec les activités ordinaires. Afin de minimiser l'impact sur les performances du système, programmez ASET pour qu'il s'exécute lorsque l'activité du système est au niveau le plus bas. Par exemple, exécutez ASET une fois toutes les 24 ou 48 heures à minuit.

Niveaux de sécurité ASET

ASET peut être configuré pour fonctionner sur l'un des trois niveaux de sécurité suivant : faible, moyen ou élevé À chaque niveau supérieur, les fonctions de contrôle de fichiers d'ASET augmentent afin de réduire l'accès aux fichiers et de relever la sécurité de votre système. Ces fonctions s'étendent du contrôle de la sécurité du système sans limiter l'accès aux fichiers par les utilisateurs au renforcement progressif des autorisations d'accès jusqu'à la sécurisation totale du système.

Le tableau suivant décrit ces trois niveaux de sécurité.

Niveau de sécurité	Description
Faible	Permet de s'assurer que les attributs des fichiers système sont définis sur des valeurs de version standard. ASET exécute plusieurs vérifications, puis génère un rapport sur les défaillances de sécurité potentielles. À ce niveau, ASET n'effectue aucune action, de sorte qu'il n'affecte pas les services système.
Moyen	Assure un contrôle de sécurité approprié pour la plupart des environnements. ASET modifie certains paramètres des fichiers système. ASET limite l'accès au système afin de réduire les risques d'attaque contre la sécurité. ASET signale les défaillances de sécurité et toute modification apportée par ASET visant à restreindre l'accès. À ce niveau, ASET n'affecte pas les services système.

Niveau de sécurité	Description
Élevé	Rend un système hautement sécurisé. ASET ajuste de nombreux fichiers système et paramètres pour accorder des autorisations minimales. La plupart des applications et commandes système continuent de fonctionner normalement. Cependant, à ce niveau, les considérations relatives à la sécurité sont prioritaires sur les autres comportements du système.

Remarque – ASET ne modifie pas les autorisations d'un fichier pour le rendre moins sécurisé, sauf si vous réduisez vous-même le niveau de sécurité. Vous pouvez également rétablir volontairement les paramètres du système tels qu'ils étaient avant l'exécution d'ASET.

Liste des tâches ASET

Cette section présente les tâches effectuées par ASET. Vous devez comprendre chacune de ces tâches. La connaissance des objectifs d'ASET, des opérations qu'il réalisé et des composants système qu'il affecte vous permet d'interpréter et d'exploiter les rapports efficacement.

Les fichiers de rapport ASET contiennent des messages décrivant le plus précisément possible les problèmes détectés par chaque tâche ASET. Ces messages peuvent vous aider à diagnostiquer et résoudre ces problèmes. Cependant, l'utilisation appropriée d'ASET suppose que vous avez une compréhension générale de l'administration système et des composants du système. Si vous êtes un administrateur novice, vous pouvez vous reporter à d'autres documentations relatives à l'administration du système Oracle Solaris. Vous pouvez également lire des pages de manuel connexes pour vous préparer à l'administration ASET.

L'utilitaire `taskstat` identifie les tâches qui ont été exécutées. L'utilitaire identifie également les tâches encore en cours d'exécution. Chaque tâche exécutée génère un fichier de rapport. Pour obtenir une description complète de l'utilitaire `taskstat`, reportez-vous à la page de manuel `taskstat(1M)`.

Réglage des autorisations de fichier

Cette tâche définit les autorisations des fichiers système sur le niveau de sécurité désigné. Cette tâche est exécutée lorsque le système est installé. Si vous décidez par la suite de modifier les niveaux établis précédemment, réexécutez cette tâche. Au niveau de sécurité faible, les autorisations sont définies sur des valeurs appropriées pour un environnement ouvert de partage d'informations. Au niveau de sécurité moyen, les autorisations sont renforcées pour assurer une sécurité adaptée à la plupart des environnements. Au niveau de sécurité élevé, les autorisations sont renforcées afin de restreindre considérablement les accès.

Les modifications apportées par cette tâche aux autorisations des fichiers système et aux paramètres sont signalées dans le fichier `tune.rpt`. Pour obtenir un exemple des fichiers consultés par ASET lorsqu'il définit des autorisations, reportez-vous à la section "Exemples de fichiers de réglages" à la page 174.

Vérification des fichiers système

Cette tâche examine les fichiers système et compare chaque fichier à la description correspondante dans un fichier maître. Le fichier maître est créé lors de la première exécution de cette tâche par ASET. Il contient les paramètres des fichiers système mis en œuvre par `checklist` pour le niveau de sécurité spécifié.

Une liste de répertoires contenant des fichiers à vérifier est définie pour chaque niveau de sécurité. Vous pouvez utiliser la liste par défaut ou modifier la liste en indiquant des répertoires différents pour chaque niveau.

Pour chaque fichier, les critères suivants sont vérifiés :

- Propriétaire et groupe
- Bits d'autorisation
- Taille et somme de contrôle
- Nombre de liens
- Heure de la dernière modification

Toute différence détectée par ASET est signalée dans le fichier `cklist.rpt` . Ce fichier contient les résultats de la comparaison des tailles de fichiers système, des autorisations et des valeurs de la somme de contrôle par rapport au fichier maître.

Vérifications des utilisateurs et des groupes

Cette tâche contrôle la cohérence et l'intégrité des comptes utilisateur et des groupes. La tâche utilise les définitions dans les fichiers `passwd` et `group` . Cette tâche vérifie les fichiers de mots de passe locaux et NIS ou NIS+. Les problèmes liés au fichier de mots de passe pour NIS+ sont signalés mais pas corrigés.

Cette tâche recherche les violations suivantes :

- Noms ou ID en double
- Entrées au format incorrect
- Comptes sans mot de passe
- Répertoires de connexion non valides
- Compte `nobody`
- Mot de passe de groupe null
- Présence d'un signe plus (+) dans le fichier `/etc/passwd` sur un serveur NIS ou NIS+

Les différences sont signalées dans le fichier `usrgrp.rpt`.

Vérification des fichiers de configuration système

Au cours de cette tâche, ASET vérifie différentes tables système, dont la plupart se trouvent dans le répertoire `/etc`.

Ces fichiers sont les suivants :

- `/etc/default/login`
- `/etc/hosts.equiv`
- `/etc/inetd.conf`
- `/etc/aliases`
- `/var/adm/utmpx n`
- `/.rhosts`
- `/etc/vfstab`
- `/etc/dfs/dfstab`
- `/etc/ftpd/ftpusers`

ASET effectue diverses vérifications et modifications sur ces fichiers. Les problèmes détectés sont signalés dans le fichier `sysconf.rpt`.

Vérification des variables d'environnement

Cette tâche vérifie la définition des variables d'environnement `PATH` et `UMASK` pour l'utilisateur root et les autres utilisateurs. La tâche vérifie les fichiers `/.profile` , `/.login`, et `/.cshrc`.

Les résultats du contrôle de sécurité de l'environnement sont indiqués dans le fichier `env.rpt`.

Vérification `eeprom`

Cette tâche vérifie la valeur du paramètre de sécurité `eeprom` afin de garantir que le paramètre est défini sur le niveau de sécurité approprié. Vous pouvez définir le paramètre de sécurité `eeprom` sur `none`, `command` ou `full`.

ASET ne modifie pas ce paramètre, mais rapporte ses recommandations dans le fichier `eeprom.rpt`.

Configuration du pare-feu

Cette tâche permet de s'assurer que le système peut être utilisé comme relais réseau en toute sécurité. Cette tâche protège un réseau interne des réseaux publics externes en configurant un système dédié en tant que pare-feu. Reportez-vous à la description à la section “Systèmes pare-feu” à la page 60. Le système pare-feu sépare deux réseaux. Dans ce cas, chaque réseau considère l'autre réseau comme non autorisé. La tâche de configuration du pare-feu désactive la transmission de paquets IP (Internet Protocol). Le pare-feu permet également de masquer les informations de routage au réseau externe.

La tâche du pare-feu s'exécute à tous les niveaux de sécurité, mais prend des mesures uniquement au niveau le plus élevé. Si vous voulez exécuter ASET à un niveau de sécurité élevé, mais que votre système ne nécessite pas la protection par pare-feu, vous pouvez supprimer la tâche du pare-feu. Vous pouvez supprimer cette tâche en modifiant le fichier `asetenv`.

Toute modification apportée est signalée dans le fichier `firewall.rpt`.

Journal d'exécution ASET

ASET génère un journal d'exécution si ASET s'exécute de manière interactive ou en arrière-plan. Par défaut, ASET génère le fichier journal sur la sortie standard. Le journal d'exécution confirme qu'ASET s'est exécuté à l'heure prévue et contient également les éventuels messages d'erreur d'exécution. La commande `aset -n` indique que le journal doit être transmis par courrier électronique à un utilisateur désigné. Pour obtenir la liste complète des options ASET, reportez-vous à la page de manuel `aset(1M)`.

Exemple d'un fichier journal d'exécution ASET

```
ASET running at security level low

Machine=example; Current time = 0325_08:00


aset: Using /usr/aset as working directory

Executing task list...
        firewall
        env
        sysconfig
        usrgrp
        tune
        cklist
        eeprom
All tasks executed. Some background tasks may still be running.

Run /usr/aset/util/taskstat to check their status:
     $/usr/aset/util/taskstat     aset_dir
Where aset_dir is ASET's operating directory, currently=/usr/aset

When the tasks complete, the reports can be found in:
     /usr/aset/reports/latest/*.rpt
You can view them by:
more /usr/aset/reports/latest/*.rpt
```

Le journal d'exécution affiche d'abord le système et l'heure d'exécution d'ASET. Il répertorie ensuite chaque tâche lorsque celle-ci est lancée.

ASET appelle un processus d'arrière-plan pour chacune de ces tâches, qui sont décrites dans la section "Liste des tâches ASET" à la page 159. La tâche est répertoriée dans le journal d'exécution lors de son lancement. Cette liste n'indique pas si la tâche s'est terminée. Pour vérifier le statut des tâches d'arrière-plan, utilisez la commande `taskstat`.

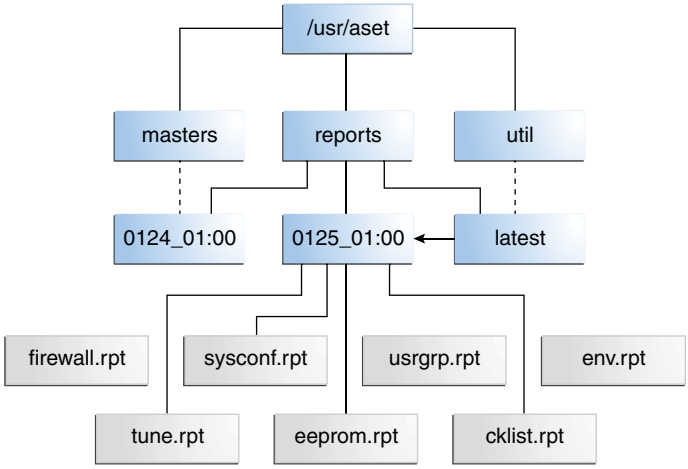
Rapports ASET

Tous les fichiers de rapport générés à partir de tâches ASET sont stockés dans des sous-répertoires du répertoire `/usr/aset/reports`. Cette section décrit la structure du répertoire `/usr/aset/reports` et fournit des instructions sur la gestion des fichiers de rapport.

ASET place les fichiers de rapport dans des sous-répertoires nommés de sorte à refléter la date et l'heure de génération des rapports. Cette convention vous permet de garder une trace des enregistrements relatifs à l'état du système étant donné que celui-ci varie d'une exécution ASET à l'autre. Vous pouvez contrôler et comparer ces rapports afin de déterminer la solidité de la sécurité de votre système.

La figure suivante montre un exemple de la structure du répertoire `reports`.

FIGURE 7–1 Structure du répertoire `reports` d'ASET



Cet exemple montre deux sous-répertoires de rapports.

- `0124_01:00`
- `0125_01:00`

Les noms des sous-répertoires indiquent la date et l'heure de création des rapports. Le format du nom des sous-répertoires de rapports est le suivant :

monthdate_hour:minute

Le *mois*, le *jour*, l'*heure* et les *minutes* sont indiqués par des nombres à deux chiffres. Par exemple, `0125_01:00` correspond au 25 janvier à 1 heure.

Chacun des deux sous-répertoires de rapports contient un ensemble de rapports générés à partir d'une seule exécution d'ASET.

Le répertoire `latest` est un lien symbolique qui pointe vers le sous-répertoire contenant les derniers rapports. Par conséquent, pour consulter les derniers rapports générés par ASET, vous pouvez accéder au répertoire `/usr/aset/reports/latest`. Il contient un fichier de rapport pour chaque tâche effectuée par ASET lors de sa dernière exécution.

Format des fichiers de rapport ASET

Les fichiers de rapports sont nommés en fonction de la tâche générant le rapport. Le tableau suivant répertorie des tâches et leurs rapports.

TABLEAU 7–1 Tâches ASET et rapports obtenus

Tâches	Rapport
Réglage des autorisations de fichiers système (`tune`)	`tune.rpt`
Vérification des fichiers système (`cklist`)	`cklist.rpt`
Vérification des utilisateurs et des groupes (`usrgrp`)	`usrgrp.rpt`
Vérification des fichiers de configuration système (`sysconf`)	`sysconf.rpt`
Vérification des variables d'environnement (`env`)	`env.rpt`
Vérification `eeprom` (`eeprom`)	`eeprom.rpt`
Configuration du pare-feu (`firewall`)	`firewall.rpt`

Au sein de chaque fichier de rapport, les messages sont encadrés par une ligne de début et de fin. Il arrive parfois qu'une tâche se termine prématurément. Cela peut par exemple se produire lorsqu'un composant d'ASET est accidentellement supprimé ou endommagé. Dans ce cas, le fichier de rapport contient généralement un message vers la fin indiquant la raison de l'interruption prématurée.

L'exemple suivant illustre un fichier de rapport `usrgrp.rpt`.

```
*** Begin User and Group Checking ***

Checking /etc/passwd ...
Warning! Password file, line 10, no passwd
:sync::1:1::/:/bin/sync
..end user check; starting group check ...
Checking /etc/group...
*** End User And group Checking ***
```

Examen des fichiers de rapport ASET

Une fois que vous avez initialement exécuté ou reconfiguré ASET, vous devez examiner de près les fichiers de rapport. La reconfiguration inclut la modification du fichier `asetenv` ou des fichiers maîtres dans le sous-répertoire `masters`, ou le changement de niveau de sécurité auquel ASET s'exécute.

Les rapports enregistrent les erreurs qui ont été introduites lorsque vous avez reconfiguré ASET. En regardant les rapports de près, vous pouvez réagir aux problèmes et les résoudre dès qu'ils surviennent.

Comparaison des fichiers de rapport ASET

Après avoir contrôlé les fichiers de rapport durant une période pendant laquelle il n'y a pas eu de modification de configuration ni de mise à jour système, vous constaterez peut-être que le contenu des rapports commence à se stabiliser. Dès lors que les rapports contiennent peu d'informations inattendues, vous pouvez utiliser l'utilitaire `diff` pour les comparer.

Fichiers maîtres ASET

Les fichiers maîtres d'ASET, `tune.high`, `tune.low`, `tune.med` et `uid_aliases` se trouvent dans le répertoire `/usr/aset/masters`. ASET utilise les fichiers maîtres pour définir les niveaux de sécurité. Pour plus d'informations, reportez-vous à la page de manuel `asetmasters(4)`.

Fichiers de réglages

Les fichiers maîtres `tune.low`, `tune.med` et `tune.high` définissent les niveaux de sécurité ASET disponibles. Ces fichiers spécifient les attributs de fichiers système à chaque niveau et sont utilisés à des fins de comparaison et de référence

Fichier `uid_aliases`

Le fichier `uid_aliases` contient une liste de plusieurs comptes utilisateur partageant le même ID utilisateur (UID). Normalement, ASET met en garde contre l'utilisation de comptes d'utilisateurs multiples car cette pratique réduit la responsabilité. Vous pouvez autoriser des exceptions à cette règle en les répertoriant dans le fichier `uid_aliases`. ASET ne signale pas les entrées dans le fichier `passwd` avec des UID en double si ces entrées sont spécifiées dans le fichier `uid_aliases`.

Évitez d'avoir des comptes d'utilisateurs multiples partageant le même UID. Vous devez prendre en compte d'autres méthodes pour atteindre votre objectif. Par exemple, si vous avez l'intention de permettre à plusieurs utilisateurs de partager un jeu d'autorisations, vous pouvez créer un compte de groupe. Vous pouvez également créer un rôle. Le partage d'UID doit être le dernier recours, utilisé uniquement lorsque d'autres méthodes ne vous permettent pas d'atteindre vos objectifs.

Vous pouvez utiliser la variable d'environnement `UID_ALIASES` pour spécifier un autre fichier d'alias. Le fichier par défaut est `/usr/aset/masters/uid_aliases`.

Fichiers de liste de contrôle

Les fichiers maîtres utilisés par les vérifications des fichiers système sont générés lors de la première exécution d'ASET. Les fichiers maîtres sont également générés lorsque vous exécutez ASET après modification du niveau de sécurité.

Les variables d'environnement suivantes définissent les fichiers vérifiés par cette tâche.

- `CKLISTPATH_LOW`
- `CKLISTPATH_MED`
- `CKLISTPATH_HIGH`

Fichier d'environnement ASET (`asetenv`)

Le fichier d'environnement `asetenv` contient une liste des variables d'environnement affectant les tâches ASET. Certaines de ces variables peuvent être ajustées pour modifier le fonctionnement d'ASET. Pour plus d'informations sur le fichier `asetenv`, reportez-vous à `asetenv(4)`.

Configuration d'ASET

Cette section présente la configuration d'ASET. Elle traite également de l'environnement dans lequel ASET fonctionne.

ASET nécessite une administration et une configuration minimales. Dans la plupart des cas, vous pouvez exécuter ASET avec les valeurs par défaut. Cependant, vous pouvez aussi ajuster certains paramètres affectant le fonctionnement et le comportement d'ASET pour optimiser son utilisation. Avant de modifier les valeurs par défaut, vous devez comprendre comment ASET fonctionne et comment il affecte les composants de votre système.

ASET repose sur quatre fichiers de configuration pour contrôler le comportement de ses tâches :

- `/usr/aset/asetenv`
- `/usr/aset/masters/tune.low`
- `/usr/aset/masters/tune.med`
- `/usr/aset/masters/tune.high`

Modification du fichier d'environnement (`asetenv`)

Le fichier `/usr/aset/asetenv` comporte deux sections principales :

- Une section de variables d'environnement non configurables par l'utilisateur
- Une section de variables d'environnement internes

Vous pouvez modifier les valeurs figurant dans la section des paramètres configurables par l'utilisateur. Les paramètres de la section de variables d'environnement internes sont destinés à une utilisation interne uniquement. Ils ne doivent pas être modifiés.

Les entrées figurant dans la section configurable par l'utilisateur permettent d'effectuer les tâches suivantes :

- Sélection des tâches à exécuter
- Spécification des répertoires pour la tâche de vérification des fichiers système
- Planification de l'exécution d'ASET
- Spécification d'un fichier d'alias d'UID
- Extension des vérifications aux tables NIS+

Sélection des tâches à exécuter : `TASKS`

Chaque tâche effectuée par ASET surveille un domaine spécifique de la sécurité du système. Dans la plupart des environnements système, toutes les tâches sont nécessaires pour assurer une couverture de sécurité équilibrée. Cependant, vous pouvez choisir de supprimer une ou plusieurs tâches.

Par exemple, la tâche du pare-feu s'exécute à tous les niveaux de sécurité, mais elle ne prend des mesures qu'au niveau de sécurité élevé. Vous souhaitez peut-être exécuter ASET au niveau de sécurité élevé, mais vous n'avez pas besoin de la protection par pare-feu.

Dans ce cas, vous pouvez configurer ASET pour qu'il s'exécute au niveau de sécurité élevé sans la fonction de pare-feu. Pour ce faire, modifiez la liste `TASKS` des variables d'environnement dans le fichier `asetenv`. Par défaut, la liste `TASKS` contient toutes les tâches ASET. Pour supprimer une tâche, retirez la variable d'environnement liée à cette tâche dans le fichier. Dans ce cas, supprimez la variable d'environnement `firewall` de la liste. Lors de la prochaine exécution d'ASET, la tâche exclue ne sera pas effectuée.

L'exemple suivant montre la liste `TASKS` incluant toutes les tâches ASET.

```
TASKS=”env sysconfig usrgrp tune cklist eeprom firewall”
```

Spécification des répertoires pour la tâche de vérification des fichiers système : CKLISTPATH

La vérification des fichiers système contrôle les attributs des fichiers dans les répertoires système sélectionnés. Vous définissez les répertoires à vérifier à l'aide des variables d'environnement suivantes :

La variable `CKLISTPATH_LOW` définit les répertoires à vérifier au niveau de sécurité faible. Les variables d'environnement `CKLISTPATH_MED` et `CKLISTPATH_HIGH` fonctionnent de la même manière pour les niveaux de sécurité moyen et élevé.

La liste de répertoires définie par une variable d'environnement à un niveau de sécurité faible doit être un sous-ensemble de la liste de répertoires définie au niveau supérieur suivant. Par exemple, tous les répertoires spécifiés pour `CKLISTPATH_LOW` doivent être inclus dans `CKLISTPATH_MED`. De même, tous les répertoires spécifiés pour `CKLISTPATH_MED` doivent être inclus dans `CKLISTPATH_HIGH`.

Les vérifications effectuées dans ces répertoires ne sont pas récursives. ASET vérifie uniquement les répertoires qui sont explicitement énumérés dans la variable d'environnement. ASET ne vérifie pas leurs sous-répertoires.

Vous pouvez modifier ces définitions de variables d'environnement pour ajouter ou supprimer des répertoires dont vous souhaitez qu'ils soient contrôlés par ASET. Notez que ces listes de contrôle ne sont utiles que pour les fichiers système ne subissant normalement pas de modifications quotidiennes. Le répertoire personnel d'un utilisateur, par exemple, est généralement trop dynamique pour faire l'objet d'une liste de contrôle.

Planification de l'exécution d'ASET : PERIODIC_SCHEDULE

Vous pouvez démarrer ASET de manière interactive, ou vous pouvez utiliser l'option `-p` pour planifier l'exécution d'ASET à une heure prévue. Vous pouvez exécuter ASET périodiquement, à une heure où la demande système est faible. Par exemple, ASET consulte `PERIODIC_SCHEDULE` afin de déterminer la fréquence et l'heure d'exécution des tâches ASET. Pour obtenir des instructions détaillées sur la configuration d'ASET pour qu'il s'exécute périodiquement, reportez-vous à la section “Exécution périodique d'ASET” à la page 177.

Le format de `PERIODIC_SCHEDULE` suit le format des entrées `crontab`. Pour des informations complètes, reportez-vous à `crontab(1)`.

Spécification d'un fichier d'alias : UID_ALIASES

La variable `UID_ALIASES` indique un fichier d'alias qui répertorie les UID partagés. Le fichier par défaut est `/usr/aset/masters/uid_aliases`.

Extension des vérifications aux tables NIS+ : YPCHECK

La variable d'environnement YPCHECK spécifie si ASET doit également vérifier les tables du fichier de configuration système. YPCHECK est une variable booléenne. Vous ne pouvez spécifier que true ou false pour YPCHECK. La valeur par défaut est false, ce qui désactive le contrôle de la table NIS+.

Pour comprendre le fonctionnement de cette variable d'environnement, examinez ses effets sur le fichier passwd. Lorsque la variable est définie sur false, ASET vérifie le fichier passwd local. Lorsqu'elle est définie sur true, la tâche vérifie également la table passwd NIS+ pour le domaine du système.

Remarque – Bien qu'ASET répare automatiquement les fichiers locaux, il signale uniquement les problèmes potentiels dans les tables NIS+. ASET ne modifie pas les tables.

Modification des fichiers de réglage

ASET utilise les trois fichiers maîtres de réglage, tune.low, tune.med et tune.high, pour relâcher ou renforcer l'accès aux fichiers système critiques. Ces fichiers maîtres sont situés dans le répertoire /usr/aset/masters . Vous pouvez modifier les fichiers pour les adapter à votre environnement. Pour consulter des exemples, reportez-vous à la section “Exemples de fichiers de réglages” à la page 174.

Le fichier tune.low définit des autorisations sur des valeurs appropriées pour les paramètres système définis par défaut. Le fichier tune.med permet de restreindre davantage ces autorisations. Le fichier tune.med contient également des entrées qui ne sont pas présentes dans tune.low. Le fichier tune.high restreint encore davantage les autorisations.

Remarque – Modifiez les paramètres dans les fichiers de réglages en ajoutant ou supprimant des entrées de fichier. Vous ne pouvez définir efficacement une autorisation sur une valeur moins restrictive que le paramètre actuel. Les tâches ASET n'assouplissent pas les autorisations, à moins que vous réduisiez la sécurité de votre système à un niveau inférieur.

Restauration de fichiers système modifiés par ASET

Lorsqu'ASET est exécuté pour la première fois, il enregistre et archive les fichiers système d'origine. L'utilitaire aset.restore réintègre ces fichiers. Cet utilitaire permet également de déprogrammer ASET s'il est actuellement programmé pour une exécution périodique. La commande aset.restore se trouve dans /usr/aset , le répertoire d'exploitation d'ASET.

Les modifications apportées aux fichiers système sont perdues lorsque vous exécutez la commande aset.restore.

Vous devez utiliser la commande `aset.restore` dans les cas suivants :

- Lorsque vous souhaitez annuler des modifications apportées par ASET et restaurer le système d'origine.

  Si vous voulez désactiver ASET définitivement, vous pouvez le supprimer de la planification `cron` si la commande `aset` avait été précédemment ajoutée au fichier `crontab` de la racine. Pour obtenir des instructions sur l'utilisation de `cron` pour supprimer l'exécution automatique, reportez-vous à la section "Arrêt de l'exécution périodique d'ASET" à la page 178.
- Lorsque vous souhaitez restaurer le système d'origine après une brève période d'expérimentation d'ASET.
- Lorsque des fonctions majeures du système ne fonctionnent pas correctement, et vous avez des raisons de croire qu'ASET est à l'origine du problème.

Opération réseau avec le système NFS

Généralement, ASET est utilisé en mode autonome, même sur un système faisant partie d'un réseau. En tant qu'administrateur système de votre système autonome, vous êtes responsable de la sécurité du système. Par conséquent, vous êtes chargé de l'exécution et de la gestion d'ASET afin de protéger votre système.

Vous pouvez également utiliser ASET dans l'environnement distribué NFS. En tant qu'administrateur réseau, vous êtes responsable de l'installation, de l'exécution et de la gestion des différentes tâches d'administration pour tous vos clients. Pour faciliter la gestion d'ASET sur plusieurs systèmes client, vous pouvez apporter des modifications à la configuration qui sont appliquées de manière globale à tous les clients. En appliquant des modifications de manière globale, vous n'avez plus besoin de vous connecter à chaque système afin de répéter les modifications de configuration.

Lorsque vous déterminez la façon de configurer ASET sur vos systèmes en réseau, vous devez prendre en considération les utilisateurs auxquels vous souhaitez confier le contrôle de la sécurité. Vous pouvez faire en sorte que les utilisateurs contrôlent certains paramètres de sécurité de leurs propres systèmes. Ou vous pouvez souhaiter centraliser la responsabilité du contrôle de sécurité.

Définition d'une configuration globale pour chaque niveau de sécurité

Il se peut que vous souhaitiez configurer plusieurs configurations réseau. Par exemple, vous pouvez vouloir définir une configuration pour des clients désignés avec un niveau de sécurité faible. Vous pouvez être amené à définir une autre configuration pour les clients de niveau moyen et encore une autre configuration de niveau élevé.

Si vous avez besoin de créer une configuration réseau ASET distincte pour chaque niveau de sécurité, vous pouvez créer trois configurations ASET sur le serveur. Vous devez créer une

configuration pour chaque niveau. Vous devez exporter chaque configuration vers les clients avec le niveau de sécurité approprié. Certains composants ASET communs aux trois configurations peuvent être partagés à l'aide de liens.

Collecte de rapports ASET

Non seulement vous pouvez centraliser les composants ASET sur un serveur, mais vous pouvez également configurer un répertoire central sur un serveur afin de collecter tous les rapports ASET. Le serveur est accessible par des clients avec ou sans privilèges de superutilisateur. Pour obtenir des instructions sur la configuration d'un mécanisme de collecte, reportez-vous à la section "Collecte de rapports ASET sur un serveur " à la page 179.

Lorsque vous configurez la collecte des rapports sur un serveur, vous pouvez consulter les rapports de tous les clients à partir d'un seul emplacement. Vous pouvez utiliser cette méthode qu'un client possède ou non des privilèges de superutilisateur. Vous pouvez aussi laisser le répertoire reports sur le système local lorsque vous voulez que les utilisateurs surveillent leurs propres rapports ASET.

Variables d'environnement ASET

La liste suivante répertorie les variables d'environnement ASET et les valeurs spécifiées par ces variables.

`ASETDIR`	Spécifie le répertoire de travail ASET
`ASETSECLEVEL`	Spécifie le niveau de sécurité
`PERIODIC_SCHEDULE`	Spécifie le calendrier périodique
`TASKS`	Spécifie les tâches ASET à exécuter
`UID_ALIASES`	Spécifie un fichier d'alias
`YPCHECK`	Détermine si les vérifications doivent être étendues aux cartes NIS et aux tables NIS+
`CKLISTPATH_LOW`	Correspond à la liste des répertoires pour le niveau de sécurité faible
`CKLISTPATH_MED`	Correspond au répertoire pour le niveau de sécurité moyen
`CKLISTPATH_HIGH`	Correspond à la liste des répertoires pour le niveau de sécurité élevé

Les variables d'environnement répertoriées dans les sections suivantes sont disponibles dans le fichier `/usr/aset/asetenv`. Les variables `ASETDIR` et `ASETSECLEVEL` sont facultatives. Les variables peuvent être définies uniquement par le biais du shell à l'aide de la commande `/usr/aset/aset`. Les autres variables d'environnement peuvent être définies en modifiant le fichier.

Variable d'environnement ASETDIR

ASETDIR spécifie un répertoire de travail ASET.

Dans le shell C, entrez :

```
% setenv ASETDIR pathname
```

Dans le shell Bourne ou Korn, entrez :

```
$ ASETDIR=pathname
$ export ASETDIR
```

Remplacez *pathname* par le nom de chemin d'accès complet du répertoire de travail ASET.

Variable d'environnement ASETSECLEVEL

La variable ASETSECLEVEL indique le niveau de sécurité auquel les tâches ASET sont exécutées.

Dans le shell C, entrez :

```
% setenv ASETSECLEVEL level
```

Dans le shell Bourne ou Korn, entrez :

```
$ ASETSECLEVEL=level
$ export ASETSECLEVEL
```

Dans ces commandes, *level* peut être défini sur l'un des éléments suivants :

`low` Niveau de sécurité faible

`med` Niveau de sécurité moyen

`high` Niveau de sécurité élevé

Variable d'environnement PERIODIC_SCHEDULE

La valeur de PERIODIC_SCHEDULE suit le même format que le fichier `crontab`. Spécifiez la valeur de la variable sous la forme d'une chaîne de cinq champs entre guillemets doubles, avec chaque champ séparé par un espace :

"*minutes hours day-of-month month day-of-week*"

minutes hours Spécifie l'heure de début en minutes (0-59) après l'heure, suivies de l'heure (0-23).

day-of-month Spécifie le jour du mois où ASET doit être exécuté. Les valeurs sont comprises entre 1 et 31.

month Spécifie le mois de l'année ASET doit être exécuté. Les valeurs sont comprises entre 1 et 12.

day-of-week Spécifie le jour de la semaine où ASET doit être exécuté. Les valeurs sont comprises entre 0 et 6. Le dimanche est le jour 0.

Les règles suivantes s'appliquent lorsque vous créez un programme périodique pour ASET :

- Vous pouvez spécifier une liste de valeurs, délimitées par une virgule, pour n'importe quel champ.
- Vous pouvez spécifier une valeur sous la forme d'un nombre ou d'une plage. Une plage de valeurs est une paire de nombres reliés par un trait d'union. Une plage indique que les tâches ASET doivent être exécutées pendant toute la durée de la plage.
- Vous pouvez spécifier un astérisque (*) comme valeur pour n'importe quel champ. Un astérisque indique de manière inclusive toutes les valeurs possibles pour le champ.

L'entrée par défaut pour la variable `PERIODIC_SCHEDULE` entraîne l'exécution d'ASET à minuit tous les jours :

```
PERIODIC_SCHEDULE=”0 0 * * *”
```

Variable d'environnement `TASKS`

La variable `TASKS` répertorie les tâches effectuées par ASET. Par défaut, les sept tâches sont répertoriées :

```
TASKS=”env sysconfig usrgrp tune cklist eeprom firewall”
```

Variable d'environnement `UID_ALIASES`

La variable `UID_ALIASES` indique un fichier d'alias. Si la variable est spécifiée, ASET consulte le fichier correspondant pour obtenir la liste des alias multiples autorisés. Le format est `UID_ALIASES=`*pathname*, où *pathname* est le nom de chemin d'accès complet du fichier d'alias.

La valeur par défaut est la suivante :

```
UID_ALIASES=${ASETDIR}/masters/uid_aliases
```

Variable d'environnement `YPCHECK`

La variable `YPCHECK` étend la tâche de vérification des tables système aux tables NIS ou NIS+. La variable `YPCHECK` est une variable booléenne, qui peut être définie sur true ou false.

La valeur par défaut est false, ce qui limite la vérification aux tables système locales :

```
YPCHECK=false
```

Variables d'environnement `CKLISTPATH_`*level*

Les trois variables de chemin de liste de contrôle indiquent les répertoires qui doivent être contrôlés par la tâche de vérification des fichiers système. Les définitions suivantes des variables sont définies par défaut. Les définitions illustrent la relation entre les variables à différents niveaux :

```
CKLISTPATH_LOW=${ASETDIR}/tasks:${ASETDIR}/util:${ASETDIR}/masters:/etc
CKLISTPATH_MED=${CKLISTPATH_LOW}:/usr/bin:/usr/ucb
CKLISTPATH_HIGH=${CKLISTPATH_MED}:/usr/lib:/sbin:/usr/sbin:/usr/ucblib
```

Les valeurs pour les variables d'environnement de chemin d'accès à la liste de contrôle sont semblables aux valeurs des variables du chemin d'accès au shell. À l'instar des variables de chemin d'accès au shell, les variables d'environnement de chemin d'accès à la liste de contrôle sont des listes de noms de répertoire. Les noms de répertoire sont séparés par le signe deux-points. Utilisez un signe égale (=) pour relier le nom de variable à sa valeur.

Exemples de fichiers ASET

Cette section contient des exemples de fichiers ASET, y compris des fichiers de réglages et le fichier d'alias.

Exemples de fichiers de réglages

ASET gère trois fichiers de réglages. Chaque entrée d'un fichier de réglages occupe une ligne. Les champs d'une entrée sont indiqués dans l'ordre suivant :

pathname mode owner group type

pathname	Nom complet du chemin d'accès au fichier
mode	Nombre à cinq chiffres représentant le paramètre d'autorisation
owner	Propriétaire du fichier
group	Groupe propriétaire du fichier
type	Type de fichier

Les règles suivantes s'appliquent lorsque vous éditez les fichiers de réglages :

- Vous pouvez utiliser des caractères génériques de shell standard, tels que l'astérisque (`*`) et le point d'interrogation (`?`) dans le nom du chemin d'accès à des références multiples. Pour plus d'informations, reportez-vous à `sh(1)`.
- *mode* représente la valeur la moins restrictive. Si le paramètre actuel est déjà plus restrictif que la valeur spécifiée, ASET n'assouplit pas les paramètres d'autorisation. Par exemple, si la valeur spécifiée est `00777`, l'autorisation reste inchangée car `00777` est toujours moins restrictif que n'importe quel paramètre actif.

  Ce processus reflète la manière dont ASET gère les paramètres de mode. Le processus est différent si le niveau de sécurité est réduit ou si vous supprimez ASET. Lorsque vous abaissez le niveau de sécurité par rapport au niveau de l'exécution précédente, ou lorsque vous souhaitez restaurer les fichiers système à leur état précédant la première exécution d'ASET, ASET identifie vos actions en cours et diminue le niveau de protection.
- Vous devez utiliser des noms pour *owner* et *group* plutôt que des ID numériques.
- Vous pouvez utiliser un point d'interrogation (`?`) à la place de *owner*, *group* et *type* afin d'empêcher ASET de modifier les valeurs existantes de ces paramètres.
- *type* peut être un `symlink`, un répertoire ou un fichier. Un `symlink` est un lien symbolique.
- Les fichiers de réglages d'un niveau de sécurité supérieur réinitialisent les autorisations de fichier pour qu'ils soient au moins aussi restrictifs que ceux des niveaux inférieurs. En outre, à des niveaux de sécurité supérieurs, d'autres fichiers sont ajoutés à la liste.
- Un fichier peut correspondre à plusieurs entrées de fichier de réglages. Par exemple, `etc/passwd` correspond aux entrées `etc/pass*` et `/etc/*` .
- Lorsque deux entrées disposent d'autorisations différentes, l'autorisation du fichier est définie sur la valeur la plus restrictive. Dans l'exemple suivant, l'autorisation du fichier `/etc/passwd` est définie sur `00755` qui est la valeur la plus restrictive entre `00755` et `00770`.

  ```
  /etc/pass* 00755 ? ? file
  /etc/* 00770 ? ? file
  ```
- Si deux entrées disposent de différentes désignations *owner* ou *group*, la dernière entrée est prioritaire. Dans l'exemple suivant, le propriétaire de `/usr/sbin/chroot` est défini sur `root`.

  ```
  /usr/sbin/chroot 00555 bin bin file
  /usr/sbin/chroot 00555 root bin file
  ```

Exemples de fichiers d'alias

Le fichier d'alias contient une liste d'alias qui partagent le même ID utilisateur.

Chaque entrée se présente sous la forme suivante :

uid=alias1 =alias2=alias3 = . . .

uid UID partagé

aliasn Comptes utilisateur partageant un UID

Par exemple, l'entrée suivante répertorie l'UID `0`. L'UID est partagé par les comptes `sysadmin` et `root` :

```
0=root=sysadmin
```

Exécution d'ASET (liste des tâches)

Tâche	Description	Voir
Exécution d'ASET à partir de la ligne de commande	Protège le système au niveau ASET que vous spécifiez. Affiche le journal d'exécution pour voir les modifications.	"Exécution d'ASET de manière interactive" à la page 176
Exécution d'ASET en mode batch à intervalles réguliers	Définit une tâche cron pour garantir qu'ASET protège le système.	"Exécution périodique d'ASET" à la page 177
Arrêt de l'exécution d'ASET en mode batch	Supprime la tâche cron d'ASET.	"Arrêt de l'exécution périodique d'ASET" à la page 178
Stockage des rapports ASET sur un serveur	Collecte des rapports ASET de clients pour le contrôle à partir d'un emplacement central.	"Collecte de rapports ASET sur un serveur " à la page 179

Pour définir les variables dans ASET, reportez-vous à la section "Variables d'environnement ASET" à la page 171. Pour configurer ASET, reportez-vous à la section "Configuration d'ASET" à la page 166.

▼ Exécution d'ASET de manière interactive

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 Exécutez ASET de manière interactive à l'aide de la commande `aset`.

```
# /usr/aset/aset -l level -d pathname
```

level Spécifie le niveau de sécurité. Les valeurs valides sont `low`, `medium` et `high`. Le paramètre par défaut est `low`. Pour plus d'informations sur les niveaux de sécurité, reportez-vous à la section "Niveaux de sécurité ASET" à la page 158.

pathname Spécifie le répertoire de travail pour ASET. La valeur par défaut est `/usr/aset`.

3 **Vérifiez qu'ASET est en cours d'exécution en consultant le journal d'exécution d'ASET affiché à l'écran.**

Le message du journal d'exécution identifie les tâches en cours d'exécution.

Exemple 7–1 Exécution d'ASET de manière interactive

Dans l'exemple suivant, ASET est exécuté à un niveau de sécurité faible avec le répertoire de travail par défaut.

```
# /usr/aset/aset -l low
======= ASET Execution Log =======

ASET running at security level low

Machine = jupiter; Current time = 0111_09:26

aset: Using /usr/aset as working directory

Executing task list ...
    firewall
    env
    sysconf
    usrgrp
    tune
    cklist
    eeprom

All tasks executed. Some background tasks may still be running.

Run /usr/aset/util/taskstat to check their status:
 /usr/aset/util/taskstat [aset_dir]

where aset_dir is ASET's operating
directory,currently=/usr/aset.

When the tasks complete, the reports can be found in:
 /usr/aset/reports/latest/*.rpt

You can view them by:
 more /usr/aset/reports/latest/*.rpt
```

▼ Exécution périodique d'ASET

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2. **Si nécessaire, définissez l'heure à laquelle vous souhaitez qu'ASET s'exécute périodiquement.**

   Il est recommandé de programmer l'exécution d'ASET à une heure où la demande système est faible. La variable d'environnement `PERIODIC_SCHEDULE` dans le fichier `/usr/aset/asetenv` est utilisée pour configurer l'heure de l'exécution périodique d'ASET. Par défaut, l'heure est définie à minuit pour chaque jour.

   Si vous souhaitez configurer une autre heure, modifiez la variable `PERIODIC_SCHEDULE` dans le fichier `/usr/aset/asetenv` . Pour plus d'informations sur la définition de la variable `PERIODIC_SCHEDULE` , reportez-vous à la section "Variable d'environnement `PERIODIC_SCHEDULE` " à la page 172.

3. **Ajoutez une entrée dans le fichier `crontab` à l'aide de la commande `aset`.**

   ```
   # /usr/aset/aset -p
   ```

   L'option `-p` insère une ligne dans le fichier `crontab` qui démarre l'exécution d'ASET à l'heure déterminée par la variable d'environnement `PERIODIC_SCHEDULE` du fichier `/usr/aset/asetenv`.

4. **Affichez l'entrée `crontab` pour vérifier l'heure à laquelle l'exécution d'ASET est planifiée.**

   ```
   # crontab -l root
   ```

▼ Arrêt de l'exécution périodique d'ASET

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Éditez le fichier `crontab`.**

   ```
   # crontab -e root
   ```

3. **Supprimez l'entrée ASET.**

4. **Enregistrez les modifications et quittez.**

5. **Affichez l'entrée `crontab` pour vérifier que l'entrée ASET a bien été supprimée.**

   ```
   # crontab -l root
   ```

▼ Collecte de rapports ASET sur un serveur

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Configurez un répertoire sur le serveur :**

   a. **Accédez au répertoire `/usr/aset`.**

      ```
      mars# cd /usr/aset
      ```

   b. **Créez un répertoire *rptdir*.**

      ```
      mars# mkdir rptdir
      ```

   c. **Accédez au répertoire *rptdir* et créez un répertoire *client_rpt*.**

      Cette étape crée un sous-répertoire *client_rpt* pour un client. Répétez cette étape pour chaque client dont vous souhaitez collecter les rapports.

      ```
      mars# cd rptdir
      mars# mkdir client_rpt
      ```

      Dans l'exemple suivant, le répertoire `all_reports` et les sous-répertoires `pluto_rpt` et `neptune_rpt` sont créés.

      ```
      mars# cd /usr/aset
      mars# mkdir all_reports
      mars# cd all_reports
      mars# mkdir pluto_rpt
      mars# mkdir neptune_rpt
      ```

3. **Ajoutez les répertoires *client_rpt* au fichier `/etc/dfs/dfstab`.**

   Les répertoires doivent disposer d'options de lecture et écriture.

   Par exemple, les entrées suivantes dans le fichier `dfstab` sont partagées avec des autorisations de lecture et écriture.

   ```
   share -F nfs -o rw=pluto /usr/aset/all_reports/pluto_rpt
   share -F nfs -o rw=neptune /usr/aset/all_reports/neptune_rpt
   ```

4. **Rendez les ressources dans le fichier `dfstab` disponibles pour les clients.**

   ```
   # shareall
   ```

5. **Sur chaque client, montez le sous-répertoire client à partir du serveur au point de montage, `/usr/aset/masters/reports`.**

   ```
   # mount server:/usr/aset/client_rpt /usr/aset/masters/reports
   ```

6 **Éditez le fichier `/etc/vfstab` pour monter le répertoire automatiquement au moment de l'initialisation.**

L'exemple d'entrée suivant dans `/etc/vfstab` sur `neptune` répertorie le répertoire à monter à partir de `mars`, `/usr/aset/all_reports/neptune_rpt` et le point de montage sur `neptune`, `/usr/aset/reports`. Pendant l'initialisation, les répertoires qui sont répertoriés dans `vfstab` sont automatiquement montés.

```
mars:/usr/aset/all_reports/neptune.rpt /usr/aset/reports nfs - yes hard
```

Dépannage de problèmes liés à ASET

Cette section décrit les messages d'erreur générés par ASET.

Messages d'erreur ASET

`ASET failed: no mail program found.`
Origine : ASET doit envoyer le journal d'exécution à un utilisateur, mais aucun programme de messagerie n'a été détecté.

Solution : Installer un programme de messagerie.

`Usage: aset [-n user[@host]] in /bin/mail or /usr/ucb/mail.`

`Cannot decide current and previous security levels.`
Origine : ASET ne peut pas déterminer les niveaux de sécurité des appels actuel et précédent.

Solution : Assurez-vous que le niveau de sécurité actuel est défini par l'intermédiaire de la ligne de commande ou de la variable d'environnement `ASETSECLEVEL`. Assurez-vous également que la dernière ligne de `ASETDIR/archives` `asetseclevel.arch` reflète bien le niveau de sécurité précédent. Si ces valeurs ne sont pas définies, ou si elles sont incorrectes, entrez les valeurs appropriées.

`ASET working directory undefined.`

`To specify, set ASETDIR environment variable or use command line option -d.`

`ASET startup unsuccessful.`
Origine : Le répertoire de travail ASET n'est pas défini ou de manière incorrecte. Le répertoire de travail est le répertoire d'exploitation.

Solution : Utilisez la variable d'environnement `ASETDIR` ou l'option de ligne de commande `-d` pour corriger l'erreur, puis redémarrez ASET.

`ASET working directory $ASETDIR missing.`

`ASET startup unsuccessful.`

Origine : Le répertoire de travail ASET n'est pas défini ou de manière incorrecte. Le répertoire de travail est le répertoire d'exploitation. Ce problème peut être dû au fait que la variable `ASETDIR` correspond à un répertoire inexistant. Ou l'option de ligne de commande `-d` peut faire référence à un répertoire inexistant.

Solution : Assurez-vous que le répertoire approprié, c'est-à-dire le répertoire contenant la hiérarchie de répertoires ASET, est correctement référencé.

`Cannot expand $ASETDIR to full pathname.`

Origine : ASET ne peut pas développer le nom de répertoire indiqué par la variable `ASETDIR` ou l'option de ligne de commande `-d` en un nom de chemin d'accès complet.

Solution : Assurez-vous que le nom de répertoire est correct. Assurez-vous que le répertoire fait référence à un répertoire existant auquel l'utilisateur a accès.

`aset: invalid/undefined security level.`

`To specify, set ASETSECLEVEL environment variable or use command line option -l, with argument= low/med/high.`

Origine : Le niveau de sécurité n'est pas défini ou est incorrect. Seules les valeurs `low`, `med` et `high` sont acceptables.

Solution : Utilisez la variable `ASETSECLEVEL` ou l'option de ligne de commande `-l` pour spécifier l'une des trois valeurs.

`ASET environment file asetenv not found in $ASETDIR.`

`ASET startup unsuccessful.`

Origine : ASET ne peut pas localiser un fichier `asetenv` dans son répertoire de travail.

Solution : Assurez-vous qu'un fichier `asetenv` existe dans le répertoire de travail ASET. Pour plus d'informations sur ce fichier, reportez-vous à la page de manuel `asetenv(4)`.

`filename doesn’t exist or is not readable.`

Origine : Le fichier désigné par *filename* n'existe pas ou n'est pas lisible. Ce problème peut se produire lorsque vous utilisez l'option `-u`. Cette option vous permet de spécifier un fichier contenant une liste d'utilisateurs que vous souhaitez vérifier.

Solution : Assurez-vous que l'argument pour l'option `-u` existe et qu'il est lisible.

`ASET task list TASKLIST undefined.`

Origine : La liste de tâches ASET, qui doit être définie dans le fichier `asetenv`, n'est pas définie. Ce message peut signifier que votre fichier `asetenv` est défectueux.

Solution : Examinez votre fichier `asetenv`. Assurez-vous que la liste de tâches est définie dans la section `User Configurable`. Vérifiez également d'autres parties du fichier pour vous assurer qu'il est intact. Pour voir le contenu d'un fichier `asetenv` valide, reportez-vous à la page de manuel `asetenv(4)`.

`ASET task list $TASKLIST missing.`

`ASET startup unsuccessful.`

Origine : La liste de tâches ASET, qui doit être définie dans le fichier `asetenv`, n'est pas définie. Ce message peut signifier que votre fichier `asetenv` est défectueux.

Solution : Examinez votre fichier `asetenv`. Assurez-vous que la liste de tâches est définie dans la section `User Configurable`. Vérifiez également d'autres parties du fichier pour vous assurer qu'il est intact. Pour voir le contenu d'un fichier `asetenv` valide, reportez-vous à la page de manuel `asetenv(4)`.

`Schedule undefined for periodic invocation.`

`No tasks executed or scheduled. Vérifiez le fichier asetenv.`

Origine : La planification ASET est requise par le biais de l'option `-p` , mais la variable d'environnement `PERIODIC_SCHEDULE` n'est pas définie dans le fichier `asetenv`.

Solution : Vérifiez la section `User Configurable` du fichier `asetenv` afin de vous assurer que la variable est définie. Assurez-vous que la variable est au format approprié.

`Attention ! Duplicate ASET execution scheduled.`

`Check crontab file.`

Origine : ASET est programmé pour s'exécuter plusieurs fois. En d'autres termes, la planification d'ASET est requise alors qu'un programme est déjà en vigueur. Ce message n'indique pas nécessairement une erreur, si plusieurs programmes sont effectivement souhaités. Dans ce cas, les messages servent uniquement d'avertissement. Si vous souhaitez planifier plusieurs programmes, vous devez utiliser le format de planification approprié à l'aide de la commande `crontab`. Pour plus d'informations, reportez-vous à la page de manuel `crontab(1)`.

Solution : Vérifiez, par l'intermédiaire de la commande `crontab`, que le programme correct est en vigueur. Assurez-vous que le fichier ne contient aucune entrée `crontab` inutile pour ASET.

PARTIE III

Rôles, profils de droits et privilèges

Cette section couvre le contrôle d'accès basé sur les rôles (RBAC) et la gestion des droits de processus. Les composants RBAC incluent les rôles, les profils de droits et les autorisations. La gestion des droits de processus est mise en œuvre par le biais des privilèges. Les privilèges, aux côtés des composants RBAC, permettent d'offrir une alternative d'administration mieux sécurisée que l'administration d'un système par un superutilisateur.

◆ ◆ ◆ CHAPITRE 8

Utilisation des rôles et des privilèges (présentation)

Le contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control) et les privilèges Oracle Solaris offrent une solution plus sécurisée au superutilisateur. Ce chapitre contient des informations de présentation sur le RBAC et les privilèges.

Vous trouverez ci-après une liste des informations de présentation contenues dans ce chapitre.

Nouveautés RBAC

Solaris 10 8/07 : les contrôles de ressources `project.max-locked-memory` et `zone.max-locked-memory` ont été introduits à partir de cette version. Si le privilège `PRIV_PROC_LOCK_MEMORY` est affecté à un utilisateur ou à une zone non globale, ces contrôles de ressources peuvent être définis de manière à empêcher l'utilisateur ou la zone de verrouiller la totalité de la mémoire. Pour plus d'informations, reportez-vous à la section "Privilèges et ressources du système " à la page 201.

Solaris 10 10/08 : dans cette version, les autorisations `solaris.admin.usermgr` ont été réorganisées de manière à prendre en charge la *séparation des tâches*, une exigence de sécurité appliquée dans les installations haute sécurité. Pour satisfaire la séparation des tâches, deux comptes sont requis pour créer un compte utilisateur. Pour configurer le logiciel en fonction de cette exigence, reportez-vous à la section "Création de profils de droits permettant d'appliquer la séparation des tâches" du *Guide de configuration d'Oracle Solaris Trusted Extensions*. Concernant également cette version, ce guide décrit la manière de modifier le mot de passe d'un rôle dans la section "Procédure de modification du mot de passe d'un rôle" à la page 228.

Solaris 10 9/10 : dans cette version, le privilège `net_access` est ajouté au jeu de privilèges de base. Pour une description des privilèges, reportez-vous à la page de manuel `privileges(5)`.

Contrôle d'accès basé sur les rôles (présentation)

La fonction de sécurité RBAC (Role-based access control, contrôle d'accès basé sur les rôles) permet de contrôler l'accès utilisateur aux tâches qui incombent normalement au superutilisateur. En appliquant les attributs de sécurité aux processus et aux utilisateurs, RBAC peut répartir les capacités superutilisateur entre plusieurs administrateurs. La gestion des droits des processus est mise en œuvre par le biais des *privilèges*. La gestion des droits des utilisateurs est mise en œuvre par le biais de RBAC.

- Pour une description de la gestion des droits des processus, reportez-vous à la section "Privilèges (présentation)" à la page 197.
- Pour plus d'informations sur les tâches RBAC, reportez-vous au Chapitre 9, "Utilisation du contrôle d'accès basé sur les rôles (tâches)".
- Pour obtenir des informations de référence, reportez-vous au Chapitre 10, "Contrôle d'accès basé sur les rôles (référence)".

RBAC : la solution de substitution au modèle superutilisateur

Dans les systèmes UNIX classiques, l'utilisateur `root`, également appelé superutilisateur, dispose de tous les pouvoirs. Les programmes exécutés comme `root` ou `setuid` ont tous les pouvoirs. L'utilisateur `root` peut lire les fichiers et y écrire des données, exécuter tous les programmes et envoyer des signaux d'interruption aux processus. Concrètement, un superutilisateur peut changer le pare-feu d'un site, modifier la piste d'audit, consulter des informations confidentielles et arrêter l'ensemble du réseau. Un programme `setuid` piraté peut avoir la mainmise sur le système.

RBAC constitue la solution de substitution plus sécurisée au modèle du tout ou rien des superutilisateurs. Avec RBAC, vous pouvez appliquer des stratégies de sécurité à un niveau plus détaillé. RBAC met en œuvre le principe de sécurité du *moindre privilège*. En d'autres termes, un utilisateur dispose des privilèges exacts en termes de quantité nécessaires à l'exécution d'un travail. Les utilisateurs standard ont suffisamment de privilèges pour utiliser leurs applications, vérifier l'état de leurs tâches, imprimer des fichiers, créer des fichiers, et ainsi de suite. Les capacités qui dépassent celles de l'utilisateur ordinaire sont regroupées dans des profils de droits. Les utilisateurs devant effectuer des tâches pour lesquelles il est nécessaire de disposer de capacités de superutilisateur endossent un rôle incluant le profil de droits approprié.

RBAC regroupe les capacités de superutilisateur en *profils de droits*. Ces profils de droits sont affectés à des comptes utilisateur spéciaux, appelés *rôles*. Un utilisateur peut alors endosser un rôle pour effectuer une tâche qui requiert certaines capacités du superutilisateur. Des profils de droits prédéfinis sont fournis avec le logiciel Oracle Solaris. Vous créez les rôles et affectez les profils.

Les profils de droits peuvent fournir des capacités étendues. Par exemple, le profil de droits d'administrateur principal est l'équivalent du superutilisateur. Les profils de droits peuvent également être définis avec précision. Par exemple, le profil de droits de gestion cron gère les tâches `at` et `cron`. Lorsque vous créez des rôles, vous pouvez décider de créer des rôles aux capacités étendues et/ou des rôles aux capacités restreintes.

Dans le modèle RBAC, le superutilisateur crée un ou plusieurs rôles. Les rôles sont basés sur des profils de droits. Le superutilisateur attribue ensuite les rôles aux utilisateurs autorisés à effectuer les tâches que ce rôle implique. Les utilisateurs se connectent avec leur nom d'utilisateur. Une fois connectés, les utilisateurs endossent les rôles qui autorisent l'utilisation des commandes d'administration et des outils d'interface graphique d'accès limité.

La flexibilité qui caractérise la configuration des rôles permet de définir une vaste gamme de stratégies de sécurité. Bien que Oracle Solaris soit livré avec peu de rôles, trois rôles recommandés peuvent être configurés facilement. Les rôles sont basés sur des profils de droits du même nom :

- **Administrateur principal :** rôle puissant, équivalent de celui de l'utilisateur `root` ou du superutilisateur.
- **Root :** rôle puissant, équivalent de celui de l'utilisateur `root`. Cependant, le rôle `root` ne permet pas de se connecter. Un utilisateur standard doit se connecter, puis prendre le rôle `root` qui lui est affecté.
- **Administrateur système :** rôle moins puissant impliquant des tâches d'administration, mais pas de sécurité. Ce rôle peut gérer des systèmes de fichiers, la messagerie électronique et l'installation de logiciels. Cependant, ce rôle ne permet pas de définir des mots de passe.
- **Opérateur :** rôle d'administrateur débutant, permettant d'effectuer des opérations telles que la gestion d'imprimantes et de sauvegardes.

Remarque – Le profil de droits Media Backup (sauvegarde des supports) donne accès au système de fichiers root entier. Par conséquent, bien que les profils de droits Sauvegarde des supports et Opérateur soient conçus pour les administrateurs débutants, les utilisateurs auxquels vous les affectez doivent être dignes de confiance.

Il n'est pas nécessaire de mettre en œuvre ces trois rôles. Les rôles sont fonction des besoins de sécurité d'une organisation. Les rôles peuvent être configurés pour les administrateurs ayant un objectif précis dans des domaines tels que la sécurité, la mise en réseau ou l'administration d'un pare-feu. Une autre stratégie consiste à créer un seul rôle d'administrateur puissant conjointement avec un rôle d'utilisateur avancé. Le rôle d'utilisateur avancé est affecté aux utilisateurs autorisés à réparer des parties de leur propre système.

Le modèle superutilisateur et le modèle RBAC peuvent coexister. Le tableau suivant résume les différents degrés (du superutilisateur à l'utilisateur ordinaire limité) possibles dans le modèle

RBAC. Le tableau comprend les actions d'administration pouvant faire l'objet d'un suivi dans les deux modèles. Pour obtenir un récapitulatif de l'effet de chaque privilège sur un système, reportez-vous au Tableau 8–2.

TABLEAU 8–1 Modèle de superutilisateur par rapport au modèle RBAC avec privilèges

Capacités d'un utilisateur sur un système	Modèle superutilisateur	Modèle RBAC
Peut devenir superutilisateur avec la capacité correspondante complète	Oui	Oui
Peut se connecter en tant qu'utilisateur disposant des capacités utilisateur complètes	Oui	Oui
Peut devenir superutilisateur avec des capacités limitées	Non	Oui
Peut se connecter en tant qu'utilisateur et disposer des capacités de superutilisateur, sporadiquement	Oui, avec les programmes `setuid` uniquement	Oui, avec les programmes `setuid` et RBAC
Peut se connecter en tant qu'utilisateur disposant des capacités d'administration, mais sans la capacité superutilisateur complète	Non	Oui, avec RBAC, et avec les privilèges et les autorisations attribués directement
Peut se connecter en tant qu'utilisateur disposant de moins de capacités qu'un utilisateur ordinaire	Non	Oui, avec RBAC et avec les privilèges supprimés
Peut suivre les actions superutilisateur	Oui, par l'audit de la commande `su`	Oui, par l'audit des commandes shell de profil En outre, si l'utilisateur `root` est désactivé, le nom de l'utilisateur qui a endossé le rôle `root` se trouve dans la piste d'audit.

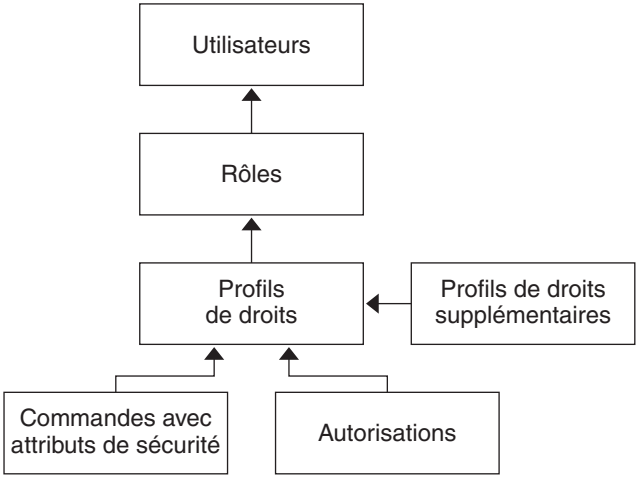
Éléments et concepts de base RBAC Oracle Solaris

Le modèle RBAC dans Oracle Solaris introduit les éléments suivants :

- **Autorisation :** autorisation permettant à un utilisateur ou rôle de réaliser une classe d'actions nécessitant des droits supplémentaires. Par exemple, la stratégie de sécurité lors de l'installation attribue aux utilisateurs standard l'autorisation `solaris.device.cdrw`. Cette autorisation offre aux utilisateurs les droits de lecture et d'écriture au niveau du périphérique de CD-ROM. Pour obtenir la liste des autorisations, reportez-vous au fichier `/etc/security/auth_attr`.
- **Privilège :** droit discret accordé à une commande, un utilisateur, un rôle ou un système. Les privilèges permettent la réussite d'un processus. Par exemple, le privilège `proc_exec` permet à un processus d'appeler `execve()`. Les utilisateurs standard disposent des privilèges de base. Pour connaître vos privilèges de base, exécutez la commande `ppriv -vl basic`.
- **Attribut de sécurité :** attribut autorisant un processus à effectuer une opération. Dans un environnement UNIX standard, un attribut de sécurité permet à un processus d'effectuer une opération qui serait autrement interdite aux utilisateurs standard. Par exemple, les programmes `setuid` et `setgid` ont des attributs de sécurité. Dans le modèle RBAC, les opérations effectuées par les utilisateurs standard peuvent nécessiter des attributs de sécurité. Outre les programmes `setuid` et `setgid`, les autorisations et les privilèges sont également des attributs de sécurité dans le modèle RBAC. Par exemple, un utilisateur avec l'autorisation `solaris.device.allocate` peut allouer un périphérique pour une utilisation exclusive. Un processus avec le privilège `sys_time` peut manipuler le temps système.
- **Application privilégiée :** application ou commande pouvant ignorer les contrôles système en recherchant les *attributs de sécurité*. Dans un environnement UNIX standard et dans le modèle RBAC, les programmes qui utilisent `setuid` et `setgid` sont des applications privilégiées. Dans le modèle RBAC, les programmes ayant besoin de privilèges ou d'autorisations pour s'exécuter correctement sont également des applications privilégiées. Pour plus d'informations, reportez-vous à la section “Applications privilégiées et RBAC ” à la page 193.
- **Profil de droits :** ensemble de capacités d'administration pouvant être affecté à un rôle ou un utilisateur. Un profil de droits peut se composer d'autorisations, de commandes avec des attributs de sécurité et d'autres profils de droits. Les profils de droits offre un moyen pratique de regrouper les attributs de sécurité.
- **Rôle :** identité spéciale permettant d'exécuter des applications privilégiées. L'identité spéciale peut être endossée par les utilisateurs assignés uniquement. Dans un système exécuté par les rôles, le superutilisateur n'est pas nécessaire. Les capacités de superutilisateur sont distribuées aux différents rôles. Par exemple, dans un système à deux rôles, les tâches de sécurité sont traitées par un rôle de sécurité. Le deuxième rôle traite des tâches d'administration système qui ne sont pas liées à la sécurité. Les rôles peuvent être définis de manière plus précise. Par exemple, un système peut inclure des rôles d'administration distincts pour la gestion de la structure cryptographique, des imprimantes, du temps système, des systèmes de fichiers et de l'audit.

La figure suivante illustre la collaboration entre les éléments RBAC.

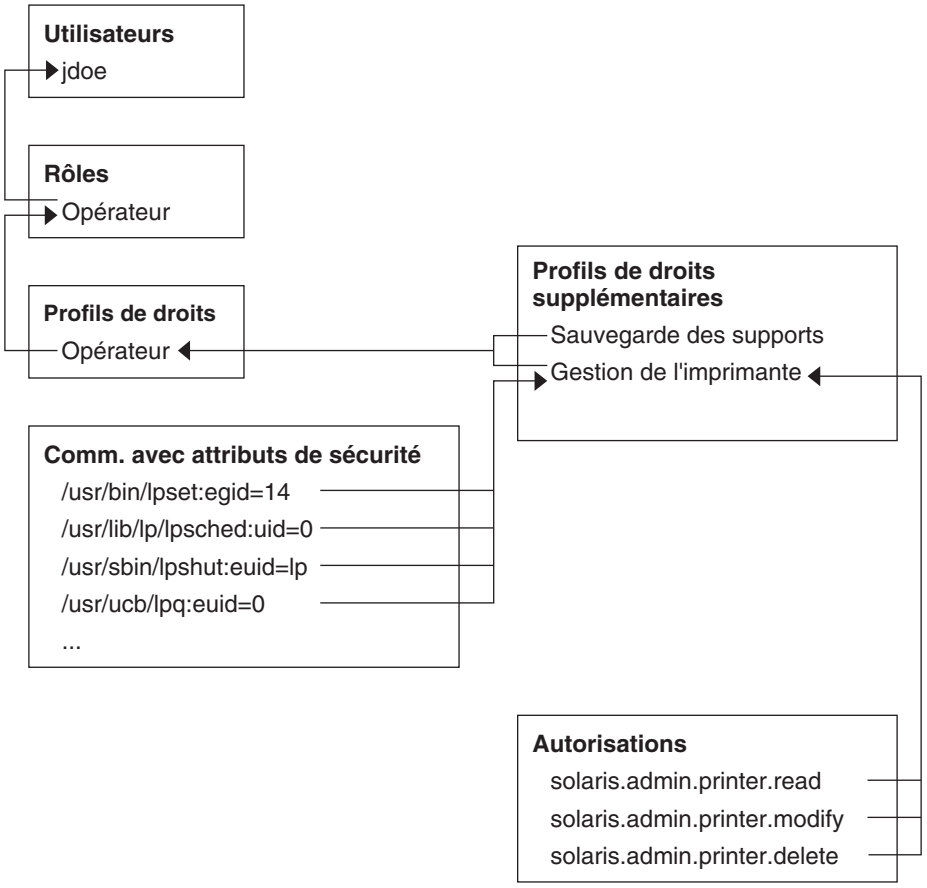
FIGURE 8–1 Relations entre les éléments RBAC Oracle Solaris



Dans RBAC, les rôles sont affectés à des utilisateurs. Lorsqu'un utilisateur endosse un rôle, les capacités de ce rôle sont disponibles. Les rôles reçoivent leurs capacités des profils de droits. Les profils de droits peuvent contenir des autorisations, des privilèges affectés directement, des commandes privilégiées et d'autres profils de droits. Les commandes privilégiées s'exécutent avec des attributs de sécurité.

La figure suivante utilise le rôle Sécurité réseau et le profil de droits Sécurité réseau pour illustrer les relations RBAC.

FIGURE 8–2 Exemple de relations entre éléments RBAC d'Oracle Solaris



Le rôle Sécurité réseau permet de gérer les liaisons réseau, IPsec et wifi. Ce rôle est assigné à l'utilisateur `jdoe`. Pour endosser le rôle, `jdoe` change de rôle, puis indique le mot de passe correspondant.

Le profil de droits Sécurité réseau a été affecté au rôle Sécurité réseau. Le profil de droits Sécurité réseau contient des profils supplémentaires qui sont évalués dans l'ordre Sécurité Wifi réseau, Sécurité Liaison réseau et Gestion IPsec réseau. Ces profils supplémentaires remplissent les tâches principales du rôle.

Le profil de droits Sécurité réseau comporte trois autorisations attribuées directement, aucun privilège affecté directement et deux commandes avec des attributs de sécurité. Les profils de droits supplémentaires ont des autorisations attribuées directement et deux d'entre eux ont des commandes avec des attributs de sécurité. Dans le rôle Sécurité réseau, `jdoe` possède toutes les autorisations attribuées dans ces profils et peut exécuter toutes les commandes avec les attributs de sécurité dans ces profils. `jdoe` peut administrer la sécurité du réseau.

Escalade des privilèges

Oracle Solaris offre aux administrateurs une grande flexibilité pour configurer la sécurité. Selon la configuration de l'installation, le logiciel n'autorise pas l'escalade des privilèges. L'escalade des privilèges se produit lorsqu'un utilisateur ou un processus obtient plus de droits d'administration qu'il n'était prévu de lui accorder. Dans ce sens, privilège signifie n'importe quel attribut de sécurité.

Le logiciel Oracle Solaris comprend les attributs de sécurité affectés à l'utilisateur `root` uniquement. Si d'autres systèmes de sécurité sont en place, l'administrateur peut affecter les attributs conçus pour les utilisateurs `root` à d'autres comptes, mais il doit procéder avec prudence.

Par exemple, le profil de droits Restauration des supports existe, mais il ne fait partie d'aucun autre profil de droits. Dans la mesure où `Media Restore` permet d'accéder à l'ensemble du système de fichiers racine, son utilisation est une escalade possible de privilège. Des fichiers délibérément modifiés ou des supports de substitution peuvent être restaurés. Par défaut, seul l'utilisateur `root` a ce profil de droits.

Pour connaître les escalades ayant une incidence sur l'attribut de sécurité, reportez-vous à la section “Prévention de l'escalade de privilèges ” à la page 278.

Autorisations RBAC

Une *autorisation* est un droit discret pouvant être accordé à un rôle ou à un utilisateur. Les autorisations permettent d'appliquer des stratégies au niveau de l'application utilisateur.

Tandis que les autorisations peuvent être attribuées directement à un rôle ou à un utilisateur, il est recommandé d'inclure les autorisations dans un profil de droits. Le profil de droits d'accès est alors ajouté à un rôle et le rôle est assigné à un utilisateur. La Figure 8–2 présente un exemple.

Les applications compatibles avec RBAC peuvent vérifier les autorisations de l'utilisateur avant de lui autoriser l'accès au niveau de l'application ou des opérations spécifiques au sein de l'application. Cette vérification remplace la vérification conventionnelle dans les applications UNIX pour `UID=0`. Pour plus d'informations sur les autorisations, reportez-vous aux sections suivantes :

- “Délégation et nommage des autorisations” à la page 246
- “Base de données `auth_attr`” à la page 250
- “Commandes nécessitant des autorisations” à la page 256

Autorisations et privilèges

Les privilèges appliquent la stratégie de sécurité dans le noyau. La différence entre les autorisations et les privilèges réside dans le niveau auquel la stratégie de sécurité est appliquée. Sans le privilège adéquat, un processus peut se voir empêcher d'exécuter des opérations privilégiées par le noyau. Sans les autorisations adéquates, un utilisateur peut se voir empêcher d'utiliser une application privilégiée ou d'exécuter des opérations liées à la sécurité au sein d'une application privilégiée. Pour en savoir plus sur les privilèges, reportez-vous à la section "Privilèges (présentation)" à la page 197.

Applications privilégiées et RBAC

Les applications et les commandes pouvant ignorer les contrôles système sont considérées comme des applications privilégiées. Les attributs de sécurité tels que `UID=0`, les privilèges et les autorisations rendent une application privilégiée.

Applications vérifiant les UID et GID

Les applications privilégiées vérifiant l'ID utilisateur `root` (`UID=0`) ou autres UID (ID utilisateur) ou GID (ID de groupe) existent depuis longtemps dans l'environnement UNIX. Le mécanisme de profil de droits vous permet d'isoler les commandes nécessitant un ID spécifique. Au lieu de modifier l'ID sur une commande accessible par tous, vous pouvez placer la commande avec les attributs de sécurité d'exécution dans un profil de droits. Un utilisateur ou un rôle avec ce profil de droits peut alors exécuter le programme sans avoir à devenir superutilisateur.

Les ID peuvent être spécifiés en tant qu'ID réels ou effectifs. On préférera une affectation d'ID effectifs à une affectation d'ID réels. Les ID effectifs correspondent à la fonction `setuid` dans les bits d'autorisation de fichier. Les ID effectifs permettent également d'identifier l'UID pour l'audit. Cependant, étant donné que certains programmes et scripts shell nécessitent un UID réel de `root`, il est également possible de définir des ID utilisateur réels. Par exemple, la commande `pkgadd` requiert un ID utilisateur réel plutôt qu'un ID utilisateur effectif. Si un ID effectif n'est pas suffisant pour exécuter une commande, vous devez le remplacer par un ID réel. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" à la page 232.

Applications vérifiant les privilèges

Les applications privilégiées peuvent vérifier l'utilisation des privilèges. Le mécanisme de profil de droits RBAC permet de spécifier les privilèges pour des commandes spécifiques. Au lieu de demander des capacités de superutilisateur pour utiliser une application ou une commande, vous pouvez isoler la commande avec des attributs de sécurité d'exécution dans un profil de droits. Un utilisateur ou un rôle doté de ce profil de droits peut ensuite exécuter la commande avec les privilèges nécessaires à la réussite de la commande.

Voici la liste des commandes vérifiant les privilèges :

- Commandes Kerberos, telles que `kadmin`, `kprop` et `kdb5_util`
- Commandes réseau, telles que `ifconfig`, `routeadm` et `snoop`
- Commandes de fichier et de système de fichiers, telles que `chmod`, `chgrp` et `monter`
- Commandes qui contrôlent les processus, telles que `kill`, `pcred` et `rcapadm`

Pour ajouter des commandes avec des privilèges à un profil de droits, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" à la page 232. Pour déterminer quelles commandes vérifient les privilèges dans un profil particulier, reportez-vous à la section "Détermination des privilèges qui vous sont attribués" à la page 268.

Applications vérifiant les autorisations

Oracle Solaris fournit également des commandes qui vérifient les autorisations. Par définition, les utilisateurs `root` possèdent toutes les autorisations. Par conséquent, l'utilisateur `root` peut exécuter n'importe quelle application. Voici la liste des applications qui vérifient les autorisations :

- Suite d'outils de la console de gestion Solaris
- Commandes d'administration d'audit, telles que `auditconfig` et `auditreduce`
- Commandes d'administration d'imprimante, telles que `lpadmin` et `Ipfilter`
- Commandes de tâche par lot, telles que `at`, `atq`, `batch` et `crontab`
- Commandes orientées périphérique, telles que `allocate`, `deallocate`, `list_devices` et `cdrw`.

Pour tester un script ou un programme dans le cadre des autorisations, reportez-vous à l'Exemple 9–24. Pour écrire un programme nécessitant des autorisations, reportez-vous à la rubrique "About Authorizations" du *Developer's Guide to Oracle Solaris Security*.

Profils de droits RBAC

Un *profil de droits* est un ensemble de remplacements système pouvant être affecté à un rôle ou à un utilisateur. Un profil de droits peut se composer d'autorisations, de commandes avec des attributs de sécurité affectés et d'autres profils de droits. Les informations de profil de droits sont divisées entre les bases de données `prof_attr` et `exec_attr`. Le nom du profil de droits et les autorisations résident dans la base de données `prof_attr`. Le nom du profil de droits et les commandes avec les attributs de sécurité affectés résident dans la base de données `exec_attr`.

Pour plus d'informations sur des profils de droits, reportez-vous aux sections suivantes :

- "Contenu des profils de droits" à la page 241
- "Base de données `prof_attr`" à la page 252

- "Base de données exec_attr" à la page 253

Rôles RBAC

Un *rôle* est un type spécial de compte utilisateur à partir duquel vous pouvez exécuter des applications privilégiées. Les rôles sont créés de la même manière que les comptes utilisateur. Les rôles ont un répertoire personnel, une affectation de groupe, un mot de passe, et ainsi de suite. Les profils de droits et les autorisations attribuent les capacités administratives des rôles. Les rôles ne peuvent pas hériter des capacités d'autres rôles ou d'autres utilisateurs. Les rôles discrets répartissent les capacités de superutilisateur et permettent ainsi des pratiques administratives plus sécurisées.

Lorsqu'un utilisateur endosse un rôle, les attributs du rôle remplacent tous les attributs de l'utilisateur. Les informations sur les rôles sont stockées dans les bases de données `passwd`, `shadow` et `user_attr`. Les informations sur les rôles peuvent être ajoutées à la base de données `audit_user`. Pour obtenir des informations détaillées sur la configuration des rôles, reportez-vous aux sections suivantes :

- "Procédure de planification de votre implémentation RBAC" à la page 209
- "Procédure de création d'un rôle à partir de la ligne de commande" à la page 214
- "Procédure de modification des propriétés d'un rôle" à la page 230

Un rôle peut être affecté à plusieurs utilisateurs. Tous les utilisateurs qui peuvent endosser le même rôle possèdent le même répertoire personnel de rôle, fonctionnent dans le même environnement et ont accès aux mêmes fichiers. Les utilisateurs peuvent endosser les rôles à partir de la ligne de commande à l'aide de la commande `su` ainsi que du nom et du mot de passe des rôles. Les utilisateurs peuvent également endosser un rôle dans l'outil de la console de gestion Solaris.

Un rôle ne peut pas se connecter directement. Un utilisateur se connecte, puis endosse un rôle. Après avoir endossé un rôle, l'utilisateur ne peut pas en endosser un autre tant qu'il n'a pas quitté son rôle actuel. Après avoir quitté son rôle, l'utilisateur peut alors en endosser un autre.

Vous pouvez empêcher une connexion `root` anonyme en remplaçant l'utilisateur `root` par un rôle, comme illustré à la section "Procédure de changement d'un utilisateur `root` en rôle" à la page 220. Si la commande shell de profil, `pfexec`, est en cours d'audit, la piste d'audit contient l'UID réel de l'utilisateur de connexion, les rôles que l'utilisateur a endossés et les actions que le rôle a effectuées. Pour auditer le système ou un utilisateur particulier pour les opérations de rôle, reportez-vous à la section "Procédure d'audit des rôles" à la page 219.

Aucun rôle prédéfini n'est livré avec le logiciel Oracle Solaris. Cependant, les profils de droits livrés avec le logiciel sont conçus pour correspondre aux rôles. Par exemple, le profil de droits Administrateur principal peut permettre de créer le rôle Administrateur principal.

- Pour configurer le rôle Administrateur principal, reportez-vous à la section "Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*.

- Pour configurer d'autres rôles, reportez-vous à la section "Procédure de création et d'attribution d'un rôle à l'aide de l'interface graphique" à la page 211.
- Pour créer des rôles sur la ligne de commande, reportez-vous à la section "Gestion de RBAC (liste des tâches)" à la page 227.

Shells de profil et RBAC

Les rôles peuvent exécuter des applications privilégiées à partir du lanceur de la console de gestion Solaris ou d'un shell de profil. Un *shell de profil* est un shell spécial qui reconnaît les attributs de sécurité inclus dans un profil de droits. Les shells de profil sont lancés lorsque cet utilisateur exécute la commande `su` pour endosser un rôle. Les shells de profil sont `pfsh`, `pfcsh` et `pfksh`. Ces shells correspondent au shell Bourne (`sh`), au shell C (`csh`) et au shell Korn (`ksh`), respectivement.

Les utilisateurs auxquels un profil de droits a été assigné directement doivent appeler un shell de profil pour exécuter les commandes avec les attributs de sécurité. La section "Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité " à la page 196 contient les points en prendre en considération en matière d'utilisation et de sécurité.

Toutes les commandes exécutées dans le cadre d'un shell de profil peuvent faire l'objet d'un audit. Pour plus d'informations, reportez-vous à la section "Procédure d'audit des rôles" à la page 219.

Champ d'application du service de noms et RBAC

Le champ d'application du service de noms permet de mieux comprendre RBAC. Le champ d'application d'un rôle peut être limité à un hôte unique. Il peut également inclure tous les hôtes pris en charge par un service de nommage, tel que NIS, NIS+ ou LDAP. Le champ d'application du service de noms pour un système est indiqué dans le fichier `/etc/nsswitch.conf`. La recherche s'arrête à la première correspondance. Si, par exemple, un profil de droits existe dans deux champs d'application du service de noms, seules les entrées dans le premier champ d'application du service de noms sont utilisées. Si `files` est la première correspondance, le champ d'application de ce rôle est limité à l'hôte local.

Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité

En général, un utilisateur obtient ses capacités d'administration par le biais d'un rôle. Les autorisations et les commandes privilégiées sont regroupées dans un profil de droits. Le profil de droits est inclus dans un rôle et le rôle est assigné à un utilisateur.

L'affectation directe des profils de droits et des attributs de sécurité est également possible :

- Les profils de droits, privilèges et autorisations peuvent être attribués directement aux utilisateurs.
- Les privilèges et les autorisations peuvent être attribués directement aux utilisateurs et aux rôles.

Toutefois, l'affectation directe de privilèges ne constitue pas une pratique sécurisée. Les utilisateurs et les rôles auxquels un privilège est affecté directement peuvent remplacer la stratégie de sécurité partout où ce privilège est requis par le noyau. Une pratique plus sécurisée consiste à attribuer le privilège en tant qu'attribut de sécurité d'une commande dans un profil de droits. Ce privilège n'est alors disponible que pour cette commande par un utilisateur doté de ce profil de droits.

Étant donné que les autorisations agissent au niveau de l'utilisateur, l'affectation directe d'autorisations constitue un moindre risque que l'affectation directe de privilèges. Cependant, les autorisations peuvent permettent à un utilisateur d'effectuer des tâches hautement sécurisées, comme l'affectation d'indicateurs d'audit par exemple.

Un profil de droits attribué directement à un utilisateur présente des problèmes d'utilisation plus que des problèmes de sécurité. Les commandes avec des attributs de sécurité dans le profil de droits ne peuvent être exécutées que dans un shell de profil. L'utilisateur ne doit pas oublier d'ouvrir un shell de profil, puis de saisir les commandes dans ce shell. Un rôle auquel est affecté un profil de droits obtient un shell de profil automatiquement. Par conséquent, les commandes sont exécutées avec succès dans le shell du rôle.

Privilèges (présentation)

La gestion des droits de processus permet de restreindre les processus au niveau de la commande, du rôle, du système ou de l'utilisateur. Oracle Solaris met en œuvre la gestion des droits de processus via des *privilèges*. En termes de sécurité, les privilèges diminuent le risque qu'un utilisateur ou un processus puisse disposer des capacités de superutilisateur complètes sur un système. Les privilèges et les contrôles RBAC offrent une solution de substitution intéressante au modèle superutilisateur traditionnel.

- Pour plus d'informations sur le contrôle RBAC, reportez-vous à la section “Contrôle d'accès basé sur les rôles (présentation) ” à la page 186.
- Pour plus d'informations sur la gestion des privilèges, reportez-vous à la section Chapitre 11, “Privilèges (tâches)”.
- Pour obtenir des informations de référence sur les privilèges, reportez-vous à la section Chapitre 12, “Privilèges (référence)”.

Protection des processus noyau par les privilèges

Un privilège est un droit discret dont a besoin un processus pour réaliser une opération. Le droit est appliqué dans le noyau. Un programme qui s'exécute dans les limites du *jeu de base* de privilèges Oracle Solaris fonctionne dans les limites de la stratégie de sécurité système. Les programmes `setuid` sont des exemples de programmes qui fonctionnent en dehors des limites de la stratégie de sécurité système. Les privilèges permettent aux programmes d'éliminer la nécessité d'appeler `setuid`.

Les privilèges énumèrent discrètement les types d'opérations possibles sur un système. Les programmes peuvent être exécutés avec les privilèges exacts nécessaires à leur réussite. Par exemple, un programme qui définit la date et l'enregistre dans un fichier d'administration peut nécessiter les privilèges `file_dac_write` et `sys_time`. Cette capacité élimine la nécessite d'exécuter les programmes en tant que `root`.

Historiquement, les systèmes n'ont pas suivi le modèle de privilège. Ils ont plutôt utilisé le modèle de superutilisateur. Dans le modèle de superutilisateur, les processus s'exécutaient en tant que `root` ou en tant qu'utilisateur. L'action des processus utilisateur était limitée au niveau des répertoires et fichiers de l'utilisateur. Les processus `root` pouvaient créer des répertoires et fichiers en tout point du système. Un processus qui devait créer un répertoire en dehors du répertoire de l'utilisateur devait s'exécuter avec `UID=0`, c'est-à-dire, en tant que `root`. La stratégie de sécurité s'appuyait sur le contrôle d'accès discrétionnaire (DAC, Discretionary Access Control) pour protéger les fichiers système. Les nœuds de périphérique étaient protégés par DAC. Par exemple, les périphériques appartenant au groupe `sys` ne pouvaient être ouverts que par les membres du groupe `sys`.

Cependant, les programmes `setuid`, les autorisations de fichier et les comptes d'administration sont vulnérables à une utilisation abusive. Les actions qu'un processus `setuid` est autorisé à réaliser sont plus nombreuses qu'il n'est nécessaire au processus pour terminer son opération. Un programme `setuid` peut être compromis par un intrus qui s'exécute ensuite en tant qu'utilisateur `root` disposant de tous les pouvoirs. De même, tout utilisateur ayant accès au mot de passe `root` peut compromettre l'ensemble du système.

En revanche, un système appliquant la stratégie avec des privilèges permet l'instauration d'une graduation entre les capacités utilisateur et les capacités `root`. Un utilisateur peut se voir accorder des privilèges nécessaires à la réalisation d'activités dépassant les capacités des utilisateurs standard et `root` peut voir le nombre de ses privilèges actuels réduit. Avec RBAC, une commande qui s'exécute avec les privilèges peut être isolée dans un profil de droits et assignée à un utilisateur ou à un rôle. Le Tableau 8–1 résume la graduation entre les capacités utilisateur et les capacités root que le modèle RBAC plus privilèges fournit.

Le modèle de privilèges offre une plus grande sécurité que le modèle superutilisateur. Les privilèges supprimés d'un processus ne peuvent pas être exploités. Les privilèges de processus empêchent un programme ou compte d'administration d'accéder à toutes les capacités. Les privilèges de processus peuvent fournir une protection supplémentaire pour les fichiers sensibles, où les protections DAC seules peuvent être exploitées pour obtenir l'accès.

Les privilèges peuvent alors restreindre les programmes et processus aux capacités qu'ils nécessitent. Cette capacité s'appelle le *principe du moindre privilège*. Sur un système appliquant ce privilège, un intrus qui capture un processus n'a accès qu'aux privilèges dont dispose ce processus. Le reste du système ne peut pas être compromis.

Descriptions des privilèges

Les privilèges sont logiquement regroupés sur la base de la zone du privilège.

- Privilège `FILE` : les privilèges qui commencent par la chaîne `file` fonctionnent sur les objets du système de fichiers. Par exemple, le privilège `file_dac_write` remplace le contrôle d'accès discrétionnaire lors de l'écriture dans les fichiers.
- Privilèges `IPC` : les privilèges qui commencent par la chaîne `ipc` remplacent les contrôles d'accès aux objets IPC. Par exemple, le privilège `ipc_dac_read` permet à un processus de lire une mémoire partagée distante et protégée par le contrôle DAC.
- Privilège `NET` : les privilèges qui commencent par la chaîne `net` offrent l'accès à des fonctionnalités réseau spécifiques. Par exemple, le privilège `net_rawaccess` permet à un périphérique de se connecter au réseau.
- Privilège `PROC` : les privilèges qui commencent par la chaîne `proc` permettent aux processus de modifier les propriétés restreintes du processus lui-même. Les privilèges `PROC` comprennent des privilèges ayant un effet très limité. Par exemple, le privilège `proc_clock_highres` permet à un processus d'utiliser des horloges haute résolution.
- Privilège `SYS` : les privilèges qui commencent par la chaîne `sys` offrent aux processus l'accès illimité à diverses propriétés système. Par exemple, le privilège `sys_linkdir` permet à un processus de créer et de rompre des liens physiques vers des répertoires.

Certains privilèges ont un effet limité sur le système, d'autres un effet important. La définition du privilège `proc_taskid` indique son effet limité :

```
proc_taskid
        Allows a process to assign a new task ID to the calling process.
```

La définition du privilège `file_setid` indique son large effet :

```
net_rawaccess
        Allow a process to have direct access to the network layer.
```

La page de manuel `privileges(5)` contient la description de chaque privilège. La commande `ppriv -lv` imprime une description de chaque privilège à la sortie standard.

Différences administratives sur un système disposant de privilèges

Un système disposant de privilèges présente plusieurs différences visibles avec un système qui n'en possède pas. Le tableau suivant énumère certaines différences.

TABLEAU 8–2 Différences visibles entre un système avec des privilèges et un système sans privilèges

Fonctionnalité	Aucun privilège	Privilèges
Démons	Les démons s'exécutent en tant que `root`.	Les démons s'exécutent en tant que `démon` utilisateur. Par exemple, les démons suivants ont reçu les privilèges appropriés et s'exécutent en tant que `démons` : `lockd`, `nfsd` et `rpcbind`.
Propriété du fichier journal	Les fichiers journaux appartiennent à `root`.	Les fichiers journaux sont désormais la propriété du `démon`, qui a créé le fichier journal. L'utilisateur `root` ne détient pas la propriété du fichier.
Messages d'erreur	Les messages d'erreur se rapportent au superutilisateur. Par exemple, `chroot: not superuser`.	Les messages d'erreur reflètent l'utilisation des privilèges. Par exemple, le message d'erreur équivalent pour l'échec `chroot` est `chroot: exec failed`.
Programmes `setuid`	Les programmes utilisent `setuid` pour terminer les tâches que les utilisateurs standard ne sont pas autorisés à effectuer.	De nombreux programmes `setuid` ont été modifiés afin d'être exécutés avec des privilèges. Par exemple, les utilitaires suivants utilisent des privilèges : `ufsdump`, `ufsrestore`, `rsh`, `rlogin`, `rcp` , `rdist`, `ping`, `traceroute` et `newtask`.
Autorisations de fichier	Les autorisations d'accès aux périphériques sont contrôlées par DAC. Par exemple, les membres du groupe `sys` peuvent ouvrir `/dev/ip`.	Les autorisations de fichier (DAC) ne prédisent pas qui peut ouvrir un périphérique. Les périphériques sont protégés par DAC *et* par la stratégie de périphériques. Par exemple, le fichier `/dev/ip` a `666` autorisations, mais le périphérique ne peut être ouvert que par un processus disposant des privilèges appropriés. Les sockets bruts sont toujours protégés par CAD.
Événements d'audit	L'audit de l'utilisation de la commande `su` couvre de nombreuses fonctions d'administration.	L'audit de l'utilisation des privilèges couvre la plupart des fonctions d'administration. Les classes d'audit `pm` et `as` incluent les événements d'audit qui configurent la stratégie de périphériques et les événements d'audit qui définissent les privilèges.
Processus	Les processus sont protégés par leur propriétaire.	Les processus sont protégés par des privilèges. Les privilèges de processus et les indicateurs de processus sont visibles sous la forme d'une nouvelle entrée dans le répertoire `/proc/<pid>`, `priv`.

TABLEAU 8–2 Différences visibles entre un système avec des privilèges et un système sans privilèges *(Suite)*

Fonctionnalité	Aucun privilège	Privilèges
Débogage	Aucune référence aux privilèges dans les fichiers core dump.	La section de note ELF des fichiers core dump comprend des informations sur les privilèges et les indicateurs de processus dans les notes `NT_PRPRIV` et `NT_PRPRIVINFO`. L'utilitaire `ppriv` et d'autres utilitaires indiquent le nombre correct de jeux de taille adéquate. Les utilitaires font correspondre correctement les bits dans les jeux de bits avec les noms de privilège.

Privilèges et ressources du système

À partir de la version Solaris 10 8/07, les contrôles de ressources `project.max-locked-memory` et `zone.max-locked-memory` peuvent être utilisés pour limiter la consommation mémoire des processus auxquels le privilège `PRIV_PROC_LOCK_MEMORY` est affecté. Ce privilège permet à un processus de verrouiller des pages dans la mémoire physique.

Si vous affectez le privilège `PRIV_PROC_LOCK_MEMORY` à un profil de droits, vous pouvez attribuer aux processus qui disposent de ce privilège la capacité de verrouiller la totalité de la mémoire. À titre de protection, définissez un contrôle de ressources pour empêcher l'utilisateur de ce privilège de verrouiller toute la mémoire. Pour les processus privilégiés qui s'exécutent dans une zone non globale, définissez le contrôle de ressources `zone.max-locked-memory`. Pour les processus privilégiés qui s'exécutent sur un système, créez un projet et définissez le contrôle de ressources `project.max-locked-memory` . Pour plus d'informations sur ces contrôles de ressources, reportez-vous au Chapitre 6, “Contrôles des ressources (présentation)” du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris* et au Chapitre 17, “Configuration des zones non globales (présentation)” du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Mise en œuvre des privilèges

Chaque processus dispose de quatre jeux de privilèges qui déterminent s'il peut utiliser un privilège particulier. Le noyau calcule automatiquement le *jeu effectif* de privilèges. Vous pouvez modifier le *jeu héritable* de privilèges. Un programme codé pour utiliser des privilèges peut réduire le *jeu autorisé* du programme. Vous pouvez réduire le *jeu limite* de privilèges.

- **Jeu de privilèges effectif ou E (Effective) :** jeu de privilèges actuellement en vigueur. Un processus peut ajouter des privilèges du jeu autorisé dans le jeu effectif. Un processus peut également supprimer des privilèges de E.
- **Jeu de privilèges autorisés ou P (Permitted):** jeu de privilèges disponible pour l'utilisation. Les privilèges peuvent être disponibles à un programme après héritage ou par affectation. Un profil d'exécution est un moyen d'affecter des privilèges à un programme. La commande `setuid` affecte tous les privilèges dont dispose `root` sur un programme. Les privilèges

peuvent être supprimés du jeu autorisé, mais ils ne peuvent pas y être ajoutés. Les privilèges supprimés de P sont automatiquement supprimés de E.

Un programme *conscient des privilèges* supprime les privilèges qu'un programme n'utilise jamais de son jeu autorisé. De cette manière, les privilèges superflus ne peuvent pas être exploités par le programme ou un processus malveillant. Pour plus d'informations sur les programmes prenant en charge les privilèges, reportez-vous au Chapitre 2, "Developing Privileged Applications" du *Developer's Guide to Oracle Solaris Security*.

- **Jeu de privilèges héritable ou I (Inheritable) :** jeu de privilèges qu'un processus peut hériter d'un appel à `exec`. Après l'appel à `exec`, les jeux autorisé et effectif sont égaux, à l'exception du cas particulier d'un programme `setuid`.

  Pour un programme `setuid`, après l'appel à `exec`, le jeu héritable est d'abord restreint par le jeu limite. Ensuite, les privilèges hérités (I), moins les privilèges qui se trouvaient dans le jeu limite (L), sont affectés à P et E pour ce processus.

- **Jeu de privilèges de limite ou L (Limit) :** limite extérieure des privilèges disponibles à un processus et à ses fils. Par défaut, le jeu limite contient tous les privilèges. Les processus peuvent réduire le jeu limite mais ne peuvent jamais l'étendre. L est utilisé pour limiter I. Par conséquent, l limite P et E au moment de l'`exécution`.

  Si un utilisateur s'est vu affecter un profil qui inclut un programme qui a reçu des privilèges, l'utilisateur peut généralement exécuter ce programme. Sur un système non modifié, les privilèges affectés du programme se trouvent dans le jeu limite de l'utilisateur. Les privilèges affectés au programme deviennent partie intégrante du jeu autorisé de l'utilisateur. C'est à partir d'un shell de profil que l'utilisateur doit exécuter le programme auquel des privilèges ont été affectés.

Le noyau reconnaît un *jeu de privilèges de base*. Sur un système non modifié, le jeu héritable initial de chaque utilisateur correspond au jeu de base défini au moment de la connexion. Vous pouvez modifier le jeu héritable initial de l'utilisateur. Vous ne pouvez pas modifier le jeu de base.

Sur un système non modifié, les jeux de privilèges de l'utilisateur à la connexion ressemble à ce qui suit :

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

Par conséquent, au moment de la connexion, tous les utilisateurs ont le jeu de base dans leur jeu hérité, leur jeu autorisé et leur jeu effectif. Le jeu limite de l'utilisateur contient tous les privilèges. Pour ajouter des privilèges au jeu effectif de l'utilisateur, vous devez affecter un profil de droits à ce dernier. Le profil de droits doit inclure les commandes pour lesquelles vous avez ajouté les privilèges. Vous pouvez également affecter des privilèges directement à l'utilisateur ou au rôle, bien que de telles affectations de privilèges puissent comporter un risque. Pour une description des risques, reportez-vous à la section "Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité " à la page 196.

Comment les processus obtiennent des privilèges

Les processus peuvent hériter de privilèges. Des privilèges peuvent aussi leur être affectés. Un processus hérite des privilèges de son processus parent. Au moment de la connexion, le jeu de privilèges héritable initial détermine les privilèges disponibles pour les processus de l'utilisateur. Tous les processus fils de la connexion initiale de l'utilisateur héritent de ce jeu.

Vous pouvez également affecter directement des privilèges à des programmes, des utilisateurs et des rôles. Lorsqu'un programme requiert des privilèges, vous affectez les privilèges à l'exécutable du programme dans un profil de droits. Les utilisateurs et les rôles autorisés à exécuter le programme se voient affecter le profil qui comprend le programme. Au moment de la connexion ou lorsqu'un shell de profil est saisi, le programme s'exécute avec le privilège lorsque l'exécutable du programme est entré dans le shell de profil. Par exemple, un rôle qui inclut le profil Gestion de l'accès aux objets peut exécuter la commande `chmod` avec le privilège `file_chown`.

Lorsqu'un rôle ou un utilisateur exécute un programme auquel un privilège supplémentaire a été affecté directement, celui-ci est ajouté au jeu héritable du rôle ou de l'utilisateur. Les processus fils du programme auquel des privilèges ont été affectés héritent des privilèges de leur parent. Si le processus fils nécessite plus de privilèges que le processus parent, ces privilèges doivent lui être affectés directement.

Les programmes codés pour utiliser des privilèges sont appelés des programmes conscients des privilèges. Un programme *conscient des privilèges* active l'utilisation des privilèges et désactive l'utilisation des privilèges lors de l'exécution du programme. Pour réussir dans un environnement de production, le programme doit se voir affecter les privilèges qu'il active et désactive.

Pour des exemples de code prenant en charge les privilèges, reportez-vous au Chapitre 2, “Developing Privileged Applications” du *Developer's Guide to Oracle Solaris Security*. Pour affecter des privilèges à un programme qui requiert les privilèges, voir l'“Ajout de privilèges à une commande” à la page 264.

Affectation de privilèges

En votre qualité d'administrateur système, vous êtes responsable de l'affectation des privilèges. En règle générale, vous affectez les privilèges à une commande dans un profil de droits. Le profil de droits est ensuite affecté à un rôle ou à un utilisateur. La console de gestion Solaris fournit l'interface utilisateur graphique nécessaire à l'affectation des privilèges. Les privilèges peuvent également être affectés à l'aide de commandes telles que `smuser` et `smrole` . Pour plus d'informations sur l'affectation de privilèges à l'aide de l'interface utilisateur graphique, reportez-vous au Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles (tâches)”.

Les privilèges peuvent également être affectés directement à un utilisateur. Si vous estimez qu'un sous-ensemble d'utilisateurs est suffisamment responsable pour utiliser un privilège au

cours de sessions, vous pouvez lui affecter directement ce privilège. Les bons candidats à l'affectation directe sont les privilèges ayant un effet limité, tels que `proc_clock_highres`. Les mauvais candidats à l'affectation directe sont les privilèges ayant des effets importants, tels que `file_dac_write`.

Les privilèges peuvent également être refusés à un utilisateur ou à un système. Procédez avec prudence lorsque vous supprimez des privilèges du jeu héritable initial ou du jeu limite d'un utilisateur ou d'un système.

Extension des privilèges d'un utilisateur ou d'un rôle

Les utilisateurs et les rôles disposent d'un jeu héritable de privilèges et d'un jeu limite de privilèges. Le jeu limite ne peut pas être étendu, car il contient initialement tous les privilèges. Le jeu héritable initial peut être étendu pour les utilisateurs, les rôles et les systèmes. Un privilège qui ne figure pas dans le jeu héritable peut également être affecté à un processus.

L'affectation des privilèges par processus est le moyen le plus précis pour ajouter des privilèges. Vous pouvez augmenter le nombre des opérations privilégiées qu'un utilisateur est autorisé à effectuer en permettant à l'utilisateur d'endosser un rôle. Le rôle se voit affecter des profils qui comprennent des commandes avec des privilèges ajoutés. Lorsque l'utilisateur endosse le rôle, il reçoit le shell de profil du rôle. Lorsqu'il ouvre le shell du rôle, les commandes dans les profils du rôle s'exécutent avec les privilèges ajoutés.

Vous pouvez également affecter un profil à l'utilisateur plutôt qu'à un rôle que l'utilisateur endosse. Le profil comprend des commandes avec des privilèges ajoutés. Lorsque l'utilisateur ouvre un shell de profil, tel que `pfksh`, il peut exécuter les commandes dans son profil avec privilège. Dans un shell standard, les commandes ne s'exécutent pas avec des privilèges. Le processus privilégié peut s'exécuter uniquement dans un shell privilégié.

Développer le jeu héritable initial de privilèges pour des utilisateurs, des rôles ou des systèmes est une manière d'affecter des privilèges plus risquée. Tous les privilèges dans le jeu héritable figurent dans le jeu autorisé et le jeu effectif. Toutes les commandes que l'utilisateur ou le rôle tape dans un shell peuvent utiliser les privilèges affectés directement. Les privilèges affectés directement permettent à un utilisateur ou à un rôle d'effectuer facilement des opérations qui peuvent figurer en dehors des limites de leurs responsabilités administratives.

Lorsque vous ajoutez des privilèges au jeu héritable initial sur un système, tous les utilisateurs qui se connectent au système disposent d'un jeu de privilèges de base plus grand. Cette affectation directe permet à tous les utilisateurs du système d'effectuer facilement des opérations qui figurent probablement en dehors des limites des utilisateurs standard.

Remarque – Le jeu limite ne peut pas être étendu, car il contient initialement tous les privilèges.

Restriction des privilèges d'un utilisateur ou d'un rôle

La suppression de privilèges permet d'empêcher les utilisateurs et les rôles d'exécuter certaines tâches. Vous pouvez supprimer des privilèges du jeu héritable initial et du jeu limite. Vous devez soigneusement tester la suppression de privilèges avant de distribuer un jeu héritable initial ou un jeu limite, plus petit que le jeu par défaut. En supprimant des privilèges du jeu héritable initial, vous risquez d'empêcher les utilisateurs de se connecter. Lorsque des privilèges sont supprimés du jeu limite, un ancien programme `setuid` peut échouer, car il nécessite un privilège qui a été supprimé.

Affectation de privilèges à un script

Les scripts sont exécutables, tout comme les commandes. Par conséquent, dans un profil de droits, vous pouvez ajouter des privilèges à un script de la même façon que vous pouvez ajouter des privilèges à une commande. Le script s'exécute avec les privilèges ajoutés lorsqu'un utilisateur ou un rôle à qui le profil a été affecté exécute le script dans un shell de profil. Si le script contient des commandes qui nécessitent des privilèges, les commandes avec les privilèges ajoutés doivent également figurer dans le profil.

Les programmes conscients des privilèges peuvent restreindre les privilèges par processus. Votre tâche en ce qui concerne un programme conscient des privilèges consiste à affecter à l'exécutable seulement les privilèges dont le programme a besoin. Vous devez ensuite tester le programme pour vérifier qu'il accomplit ses tâches correctement. Vous devez également vérifier que le programme ne fait pas une utilisation abusive des privilèges.

Privilèges et périphériques

Le modèle de privilège utilise des privilèges pour protéger les interfaces système qui, dans le modèle de superutilisateur, ne sont protégées par des autorisations de fichier. Dans un système doté de privilèges, les autorisations de fichier sont trop faibles pour protéger les interfaces. Un privilège comme `proc_owner` peut remplacer les autorisations de fichier et donner ensuite l'accès complet au système.

Par conséquent, la propriété du répertoire de périphérique n'est pas suffisante pour ouvrir un périphérique. Par exemple, les membres du groupe `sys` ne sont plus automatiquement autorisés à accéder au périphérique `/dev/ip`. Les autorisations de fichier sur `/dev/ip` sont `0666`, mais le privilège `net_rawaccess` est requis pour ouvrir le périphérique.

La stratégie de périphériques est contrôlée par des privilèges. La commande `getdevpolicy` affiche la stratégie pour chaque périphérique. La commande de configuration de périphérique `devfsadm` installe la stratégie de périphérique. La commande `devfsadm` lie les jeux de privilèges avec `open` pour la lecture ou l'écriture de périphériques. Pour plus d'informations, reportez-vous aux pages de manuel `getdevpolicy(1M)` et `devfsadm(1M)`.

La stratégie de périphériques offre une plus grande souplesse dans l'octroi d'autorisations pour ouvrir des périphériques. Vous pouvez nécessiter d'autres privilèges ou plus de privilèges que ceux prévus par la stratégie de périphérique par défaut. Les exigences en matière de privilèges peuvent être modifiées pour la stratégie de périphérique et les propriétés du pilote. Vous pouvez modifier les privilèges lors de l'installation, de l'ajout ou de la mise à jour d'un pilote de périphérique.

Les commandes `add_drv` et `update_drv` peuvent modifier les entrées de stratégie de périphérique et les privilèges spécifiques au pilote. Vous devez exécuter un processus avec le jeu complet de privilèges pour modifier la stratégie de périphérique. Pour plus d'informations, reportez-vous aux pages de manuel `add_drv(1M)` et `update_drv(1M)`.

Privilèges et débogage

Oracle Solaris fournit des outils pour déboguer les défaillances des privilèges. Les commandes `ppriv` et `truss` fournissent le résultat du débogage. Pour consulter des exemples, reportez-vous à la page de manuel `ppriv(1)`. Pour connaître la procédure, reportez-vous à la section "Détermination des privilèges requis par un programme" à la page 262.

◆ ◆ ◆ CHAPITRE 9

Utilisation du contrôle d'accès basé sur les rôles (tâches)

Ce chapitre traite des tâches permettant de répartir les capacités de superutilisateur à l'aide de rôles discrets. Les mécanismes pouvant être utilisés par les rôles comprennent les profils de droits, les autorisations et les privilèges. Vous trouverez ci-après une liste des tâches contenues dans ce chapitre.

Pour une présentation de RBAC, reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186. Pour obtenir des informations de référence, reportez-vous au Chapitre 10, "Contrôle d'accès basé sur les rôles (référence)". Pour utiliser les privilèges avec ou sans RBAC, reportez-vous au Chapitre 11, "Privilèges (tâches)".

Utilisation de RBAC (liste des tâches)

L'utilisation de RBAC requiert de planifier et configurer RBAC et de savoir endosser un rôle. Une fois familiarisé avec les rôles, vous pouvez personnaliser davantage RBAC pour gérer de nouvelles opérations. La liste des tâches suivante présente les principales tâches à effectuer.

Tâche	Description	Voir
Planification et configuration de RBAC	Configurez RBAC sur votre site.	"Configuration de RBAC (liste des tâches)" à la page 208
Utilisation de rôles	Endossez des rôles à partir de la ligne de commande et de l'interface graphique de la console de gestion Solaris.	"Utilisation des rôles (liste des tâches)" à la page 223
Personnalisation de RBAC	Personnalisez RBAC pour votre site.	"Gestion de RBAC (liste des tâches)" à la page 227

Configuration de RBAC (liste des tâches)

L'utilisation efficace de RBAC requiert une planification. Utilisez la liste des tâches ci-dessous pour planifier et implémenter initialement RBAC sur votre site.

Tâche	Description	Voir
1. Planification de RBAC	Analysez les besoins de sécurité de votre site et décidez de l'utilisation de RBAC sur votre site.	"Procédure de planification de votre implémentation RBAC" à la page 209
2. Apprentissage de l'utilisation de la console de gestion Solaris	Familiarisez-vous avec la console de gestion Solaris.	Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*
3. Configuration du premier utilisateur et du premier rôle	Utilisez les outils de configuration de RBAC dans la console de gestion Solaris pour créer un utilisateur et un rôle, et pour attribuer le rôle à l'utilisateur.	"Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*
4. (Facultatif) Création d'autres utilisateurs pouvant endosser des rôles	Assurez-vous qu'il existe des utilisateurs qui peuvent endosser un rôle d'administration.	"Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*
5. (Recommandé) Création d'autres rôles et attribution de ces rôles à des utilisateurs	Utilisez les outils RBAC pour créer des rôles pour certaines zones d'administration et les attribuer à des utilisateurs.	"Procédure de création et d'attribution d'un rôle à l'aide de l'interface graphique" à la page 211
		Exemple 9–5
	Utilisez la ligne de commande pour créer des rôles et les attribuer à des utilisateurs	"Procédure de création d'un rôle à partir de la ligne de commande" à la page 214
		"Procédure d'attribution d'un rôle à un utilisateur local" à la page 217
6. (Recommandé) Audit des actions des rôles	Présélectionnez une classe d'audit incluant l'événement d'audit qui enregistre les actions de rôles.	"Procédure d'audit des rôles" à la page 219
7. (Facultatif) Changement d'un utilisateur `root` en rôle	Empêchez la connexion `root` anonyme, qui constitue une faille de sécurité.	"Procédure de changement d'un utilisateur `root` en rôle" à la page 220

Configuration de RBAC

RBAC peut être configuré à l'aide des utilitaires suivants :

- **Interface graphique de la console de gestion Solaris :** la méthode recommandée pour l'exécution des tâches liées à RBAC est l'utilisation de l'interface graphique. Les outils de la console pour gérer les éléments RBAC sont contenus dans la collection d'outils des utilisateurs.
- **Commandes de la console de gestion Solaris :** grâce aux interfaces de ligne de commande de la console de gestion Solaris, telles que `smrole`, vous pouvez travailler sur n'importe quel service de noms. Les commandes de la console de gestion Solaris nécessitent une authentification pour se connecter au serveur. Par conséquent, ces commandes ne sont pas pratiques à utiliser dans des scripts.
- **Commandes locales :** grâce au jeu d'interfaces de ligne de commande `user*` et `role*`, telles que `useradd`, vous pouvez travailler sur les fichiers locaux uniquement. Les commandes permettant d'agir sur les fichiers locaux doivent être exécutées par un superutilisateur ou par un rôle doté des privilèges appropriés.

▼ Procédure de planification de votre implémentation RBAC

RBAC peut faire partie intégrante de la façon dont une entreprise gère ses sources d'informations. La planification requiert une connaissance approfondie des fonctionnalités de RBAC et des exigences en matière de sécurité de votre organisation.

1 Découvrez les concepts RBAC de base.

Lisez la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186. L'utilisation de RBAC pour administrer un système est très différente de l'utilisation des pratiques administratives UNIX conventionnelles. Vous devez vous familiariser avec les concepts RBAC avant de commencer l'implémentation. Pour plus de détails, reportez-vous au Chapitre 10, "Contrôle d'accès basé sur les rôles (référence)".

2 Examinez votre stratégie de sécurité.

La stratégie de sécurité de votre entreprise doit détailler les menaces potentielles pour votre système, mesurer les risques de chaque menace et disposer d'une stratégie pour les contrer. L'isolation des tâches liées à la sécurité par le biais de RBAC peut être une partie de la stratégie. Bien que vous puissiez installer les rôles recommandés et leurs configurations en l'état, vous pouvez être amené à personnaliser votre configuration RBAC pour adhérer à la stratégie de sécurité en vigueur.

3 Décidez du degré de nécessité de RBAC pour votre organisation.

En fonction de vos besoins en matière de sécurité, vous pouvez utiliser différents degrés de RBAC, comme suit :

- **Pas de RBAC :** vous pouvez effectuer toutes les tâches en tant qu'utilisateur `root`. Dans cette configuration, vous devez vous connecter en tant que vous-même. Puis, vous entrez `root` comme utilisateur lorsque vous sélectionnez un outil de la console de gestion Solaris.
- **Rôle unique seulement :** cette méthode ajoute un rôle. Le rôle unique se voit attribuer le profil de droits de l'administrateur principal. Cette méthode est similaire au modèle du superutilisateur, car le rôle dispose de capacités de superutilisateur. Cependant, cette méthode vous permet de suivre l'utilisateur qui a endossé le rôle.
- **Rôles recommandés :** cette méthode crée trois rôles basés sur les profils de droits suivants : administrateur principal, administrateur système et opérateur. Les rôles sont bien adaptés pour les organisations ayant des administrateurs à différents niveaux de responsabilité.
- **Rôles personnalisés :** vous pouvez créer vos propres rôles pour répondre aux exigences de sécurité de votre organisation. Les nouveaux rôles peuvent être basés sur des profils de droits existants ou personnalisés. Pour personnaliser des profils de droits permettant d'appliquer la séparation des tâches, reportez-vous à la section "Création de rôles et d'utilisateurs dans Trusted Extensions" du *Guide de configuration d'Oracle Solaris Trusted Extensions*.
- **Utilisateur root en tant que rôle :** cette méthode empêche tout utilisateur de se connecter en tant que `root`. Au lieu de cela, les utilisateurs doivent se connecter en tant qu'utilisateurs standard avant d'endosser le rôle `root`. Pour plus de détails, reportez-vous à la section "Procédure de changement d'un utilisateur `root` en rôle" à la page 220.

4 Déterminez les rôles recommandés appropriés pour votre organisation.

Passez en revue les capacités des rôles recommandés et des profils de droits par défaut. Les profils de droits par défaut permettent aux administrateurs de configurer un rôle recommandé en utilisant un seul profil.

Trois profils de droits par défaut sont disponibles pour la configuration des rôles recommandés :

- **Profil de droits de l'administrateur principal :** pour configurer un rôle pouvant effectuer toutes les tâches d'administration, accorder des droits à d'autres personnes et modifier des droits associés à des rôles d'administration. Un utilisateur de ce rôle peut attribuer ce rôle et accorder des droits à d'autres utilisateurs.
- **Profil de droits de l'administrateur système :** pour configurer un rôle pouvant effectuer la plupart des tâches d'administration qui ne sont pas liées à la sécurité. Par exemple, l'administrateur système peut ajouter de nouveaux comptes utilisateur, mais ne peut pas définir les mots de passe ou accorder des droits à d'autres utilisateurs.
- **Profil de droits de l'opérateur :** pour configurer un rôle pouvant effectuer des tâches d'administration simples, telles que la sauvegarde de supports ou la maintenance d'imprimantes.

Pour examiner de manière plus approfondie les profils de droits, lisez l'un des textes suivants :

- Dans le répertoire `/etc/security`, lisez le contenu de la base de données `prof_attr` et la base de données `exec_attr`.
- Dans la console de gestion Solaris, utilisez l'outil de droits pour afficher le contenu d'un profil de droits.
- Dans ce manuel, reportez-vous à la section "Contenu des profils de droits" à la page 241 pour obtenir le résumé de certains profils de droits habituels.

5 Déterminez si l'un des rôles ou des profils de droits supplémentaires sont appropriés pour votre organisation.

Recherchez d'autres applications ou familles d'applications sur votre site susceptibles de bénéficier d'un accès limité. Les applications affectant la sécurité, pouvant entraîner des problèmes de déni de service ou nécessitant une formation d'administrateur système particulière constituent de bons candidats pour RBAC. Vous pouvez personnaliser des rôles et des profils de droits pour gérer les exigences de sécurité de votre organisation.

a. Déterminez les commandes nécessaires pour la nouvelle tâche.

b. Choisissez le profil de droits approprié pour cette tâche.

Vérifiez si un profil de droits existant peut traiter cette tâche ou si un autre profil de droits doit être créé.

c. Déterminez le rôle approprié pour ce profil de droits.

Choisissez si le profil de droits pour cette tâche doit être attribué à un rôle existant ou si un nouveau rôle doit être créé. Si vous utilisez un rôle existant, assurez-vous que les autres profils de droits sont appropriés pour les utilisateurs affectés à ce rôle.

6 Déterminez les utilisateurs devant être affectés aux rôles disponibles.

Selon le principe du moindre privilège, vous devez affecter des utilisateurs à des rôles adaptés à leur niveau de confiance. Lorsque vous empêchez les utilisateurs d'accéder à des tâches qu'ils n'ont pas besoin d'effectuer, vous réduisez les problèmes potentiels.

▼ Procédure de création et d'attribution d'un rôle à l'aide de l'interface graphique

Pour créer un nouveau rôle, vous pouvez être connecté en tant que superutilisateur ou vous pouvez utiliser le rôle d'administrateur principal. Dans cette procédure, le créateur du nouveau rôle a endossé le rôle d'administrateur principal.

Avant de commencer

- Vous avez déjà créé des utilisateurs pouvant endosser un rôle sur votre site. Si les utilisateurs ne sont pas encore créés, créez-les en suivant les instructions de la section "Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*.
- Le rôle d'administrateur principal vous a été attribué en suivant les procédures de la section "Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*.

1 Démarrez la console de gestion Solaris.

```
# /usr/sbin/smc &
```

Pour plus d'instructions sur la connexion, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226.

2 Cliquez sur l'icône des rôles d'administration.

3 Sélectionnez Add Administrative Role (Ajouter un rôle d'administration) dans le menu Action.

4 Créez un nouveau rôle en remplissant les champs de la série de boîtes de dialogue.

Pour les rôles disponibles, reportez-vous aux Exemple 9–1 à Exemple 9–4.

Astuce – Tous les outils de la console de gestion Solaris affichent des informations dans la section inférieure de la page ou dans la partie gauche d'un panneau de l'assistant. Sélectionnez Help (Aide) à tout moment pour trouver des informations supplémentaires sur l'exécution de tâches dans cette interface.

---

5 Attribuez le rôle à un utilisateur.

Astuce – Après avoir rempli les propriétés du rôle, la dernière boîte de dialogue vous invite à sélectionner un utilisateur pour le rôle.

---

6 Dans une fenêtre de terminal, redémarrez le démon nscd.

```
# svcadm restart system/name-service-cache
```

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

Exemple 9–1 Création d'un rôle pour le profil de droits de l'administrateur système

Dans cet exemple, le nouveau rôle peut effectuer des tâches d'administration système qui ne sont pas liées à la sécurité. Le rôle est créé en effectuant la procédure précédente avec les paramètres suivants :

- Nom de rôle : `sysadmin`
- Nom de rôle complet : `System Administrator`

- Description du rôle : `Performs non-security admin tasks`
- Profil de droits : `System Administrator`

  Ce profil de droits s'affiche en haut de la liste des profils inclus dans le rôle.

Exemple 9–2 Création d'un rôle pour le profil de droits de l'opérateur

Le profil de droits de l'opérateur peut gérer les imprimantes et sauvegarder le système sur un support hors ligne. Vous pouvez souhaiter attribuer le rôle à un utilisateur de chaque équipe. Pour ce faire, vous devez sélectionner l'option de liste de diffusion du rôle dans la boîte de dialogue Step 1: Enter a Role Name (Étape 1 : entrez un nom de rôle). Le rôle est créé en effectuant la procédure précédente avec les paramètres suivants :

- Nom de rôle : `operadm`
- Nom de rôle complet : `Operator`
- Description du rôle : `Backup operator`
- Profil de droits : `Operator`

  Ce profil de droits doit s'afficher en haut de la liste des profils inclus dans le rôle.

Exemple 9–3 Création d'un rôle pour le profil de droits liés à la sécurité

Par défaut, le seul profil de droits contenant des commandes et des droits liés à la sécurité est le profil d'administrateur principal. Si vous souhaitez un rôle qui ne soit pas aussi puissant que l'administrateur principal, mais qui puisse gérer certaines tâches liées à la sécurité, vous devez créer ce rôle.

Dans l'exemple suivant, le rôle protège les périphériques. Le rôle est créé en effectuant la procédure précédente avec les paramètres suivants :

- Nom de rôle : `devicesec`
- Nom de rôle complet : `Device Security`
- Description du rôle : `Configures Devices`
- Profil de droits : `Device Security`

Dans l'exemple suivant, le rôle protège les systèmes et les hôtes sur le réseau. Le rôle est créé en effectuant la procédure précédente avec les paramètres suivants :

- Nom de rôle : `netsec`
- Nom de rôle complet : `Network Security`
- Description du rôle : `Handles IPsec, IKE, and SSH`
- Profil de droits : `Network Security`

Exemple 9–4 Création d'un rôle pour un profil de droits de portée limitée

Un certain nombre de profils de droits ont une portée limitée. Dans cet exemple, l'unique tâche du rôle est de gérer DHCP. Le rôle est créé en effectuant la procédure précédente avec les paramètres suivants :

- Nom de rôle : `dhcpmgt`
- Nom de complet : `DHCP Management`
- Description du rôle : `Manages Dynamic Host Config Protocol`
- Profil de droits : `DHCP Management`

Exemple 9–5 Modification de l'attribution d'un rôle à un utilisateur

Dans cet exemple, un rôle est ajouté à un utilisateur existant. L'attribution d'un rôle à l'utilisateur est modifiée en cliquant sur l'icône des comptes utilisateur dans l'outil des utilisateurs de la console de gestion Solaris, en double-cliquant sur l'utilisateur et en suivant l'aide en ligne pour ajouter un rôle aux capacités de l'utilisateur.

Erreurs fréquentes

Vérifiez ce qui suit si le rôle ne dispose pas des capacités attendues :

- Les profils de droits du rôle s'affichent-ils dans l'interface graphique du plus puissant au moins puissant ?

  Par exemple, si le profil de droits `All` s'affiche en haut de la liste, aucune commande n'est exécutée avec les attributs de sécurité. Un profil contenant des commandes avec des attributs de sécurité doit précéder le profil de droits `All` dans la liste.
- Les commandes des profils de droits du rôle disposent-elles des attributs de sécurité appropriés ?

  Par exemple, lorsque la stratégie est `suser`, certaines commandes requièrent `uid=0` plutôt que `euid=0`.
- Le profil de droits est-il défini dans le champ d'application du service de noms approprié ? Le rôle est-il utilisé dans le champ d'application du service de noms où le profil de droits est défini ?
- Le cache de service de noms, `svc:/system/name-service-cache`, a-t-il été redémarré ?

  Le démon `nscd` peut avoir un long intervalle de durée de vie. En redémarrant le démon, vous mettez à jour le service de noms avec les données en cours.

▼ Procédure de création d'un rôle à partir de la ligne de commande

L'interface graphique de la console de gestion Solaris est la méthode recommandée pour la gestion de RBAC. Pour utiliser l'interface graphique, reportez-vous à la section “Procédure de

création et d'attribution d'un rôle à l'aide de l'interface graphique” à la page 211. Vous pouvez également utiliser les interfaces de ligne de commande, de la manière décrite dans cette procédure.

Remarque – Ne tentez pas d'administrer RBAC à l'aide de la ligne de commande et de l'interface graphique en même temps. Des modifications conflictuelles pourraient être apportées à la configuration et le comportement du système serait imprévisible. Vous pouvez utiliser ces deux outils pour administrer RBAC, mais pas simultanément.

Avant de commencer Pour créer un rôle, vous devez soit endosser un rôle incluant le profil de droits d'administrateur principal, soit vous connectez en tant qu'utilisateur `root`.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Choisissez l'une des commandes suivantes pour créer un rôle sur la ligne de commande.

- **Pour les rôles dans le champ d'application du service de noms local, utilisez la commande `roleadd`.**

Remarque – La commande `roleadd` est plus limitée que l'interface graphique de la console de gestion Solaris ou les interfaces de ligne de commande. Après avoir exécuté la commande `roleadd`, vous devez exécuter la commande `usermod` pour attribuer le rôle à un utilisateur. Ainsi, l'utilisateur doit ensuite définir le mot de passe pour le rôle, tel qu'illustré dans la section “Procédure d'attribution d'un rôle à un utilisateur local” à la page 217.

```
# roleadd -c comment \
-g group -m homedir -u UID -s shell \
-P profile rolename
```

`-c` *comment*	Commentaire décrivant *rolename*.
`-g` *group*	Affectation du groupe pour *rolename*.
`-m` *homedir*	Chemin d'accès au répertoire personnel pour *rolename*.
`-u` *UID*	UID pour *rolename*.
`-s` *shell*	Shell de connexion pour *rolename*. Ce shell doit être un shell de profil.
`-P` *profile*	Un ou plusieurs profils de droits pour *rolename*.
rolename	Nom du nouveau rôle local.

- **Utilisez la commande `smrole add`.**

  Cette commande crée un rôle dans un DNS, tel que NIS, NIS+ ou LDAP. Cette commande s'exécute en tant que client du serveur de la console de gestion Solaris.

  ```
  $ /usr/sadm/bin/smrole -D domain-name \
  -r admin-role -l <Type admin-role password> \
  add -- -n rolename -a rolename -d directory\
  -F full-description -p profile
  ```

`-D` *domain-name*	Nom du domaine que vous souhaitez gérer.
`-r` *admin-role*	Nom du rôle d'administration pouvant modifier le rôle. Le rôle d'administration doit disposer de l'autorisation `solaris.role.assign`. Si vous modifiez un rôle que vous avez endossé, il doit avoir l'autorisation `solaris.role.delegate`.
`-l`	Invite pour le mot de passe de *admin-role*.
`--`	Séparateur requis entre les options d'authentification et les options de sous-commande.
`-n` *rolename*	Nom du nouveau rôle.
`-c` *comment*	Commentaire qui décrit les capacités du rôle.
`-a` *username*	Nom de l'utilisateur qui peut endosser *rolename*.
`-d` *directory*	Répertoire personnel pour *rolename*.
`-F` *full-description*	Description complète de *rolename*. Cette description s'affiche dans l'interface graphique de la console de gestion Solaris.
`-p` *profile*	Profil de droits qui est inclus dans les capacités de *rolename*. Cette option donne des commandes avec des capacités d'administration au rôle. Vous pouvez spécifier plusieurs options `-p` *profile*.

3. **Pour appliquer les modifications apportées, reportez-vous à la section "Procédure d'attribution d'un rôle à un utilisateur local" à la page 217.**

Exemple 9–6 Création d'un rôle d'opérateur personnalisé à l'aide de la commande `smrole`

La commande `smrole` spécifie un nouveau rôle et ses attributs dans un service de noms. Dans l'exemple suivant, l'administrateur principal crée une nouvelle version du rôle de sauvegarde des supports. Le rôle inclut le profil de droits de sauvegarde des supports standard ainsi que le profil de droits de gestion FTP. Notez que la commande vous invite à saisir un mot de passe pour le nouveau rôle.

```
% su - primaryadm
Password:       <Type primaryadm password>
$ /usr/sadm/bin/smrole add -H myHost -- -c "FTP and Backup Operator" \
```

```
-n operadm2 -a janedoe -d /export/home/operadm \
-F "Backup/FTP Operator" -p "Media Backup" -p "FTP Management"
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::     <Type primaryadm password>

Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::    <Type operadm2 password>

$ svcadm restart system/name-service-cache
```

La commande `smrole` avec la sous-commande `list` est utilisée pour afficher le nouveau rôle :

```
$ /usr/sadm/bin/smrole list --
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::     <Type primaryadm password>

Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.
root                    0            Superuser
primaryadm            100            Most powerful role
sysadmin              101            Performs non-security admin tasks
operadm               102            Backup Operator
operadm2              103            Backup/FTP Operator
```

Notez que les profils de droits qui incluent la sauvegarde des supports ou la restauration des supports fournissent un rôle disposant d'un accès à l'intégralité du système de fichiers root. Par conséquent, l'administrateur doit attribuer ces profils de droits aux utilisateurs de confiance. L'administrateur peut également choisir de ne pas attribuer ces profils de droits. Dans ce cas, seul le superutilisateur peut procéder à la sauvegarde et la restauration.

▼ Procédure d'attribution d'un rôle à un utilisateur local

Cette procédure permet d'attribuer un rôle local à un utilisateur local, redémarre le démon cache du nom, puis affiche la manière dont l'utilisateur peut endosser le rôle.

Pour attribuer un rôle à un utilisateur dans un DNS, reportez-vous aux sections “Procédure de création d'un rôle à partir de la ligne de commande” à la page 214 et “Procédure de modification des propriétés d'un rôle” à la page 230.

Avant de commencer Vous avez ajouté un rôle local, comme indiqué à la section “Procédure de création d'un rôle à partir de la ligne de commande” à la page 214. Vous devez soit endosser un rôle incluant le profil de droits de l'administrateur principal, soit devenir l'utilisateur `root`.

1 Attribuez le rôle à un utilisateur local.

Si vous avez ajouté un rôle local avec la commande `roleadd`, cette étape est obligatoire. Cette étape est facultative lorsque vous utilisez la commande `smrole` et la console de gestion Solaris pour créer un rôle.

```
# usermod -u UID -R rolename login-name
```

`-u` *UID*	UID de l'utilisateur.
`-R` *rolename*	Rôle qui est attribué à l'utilisateur.
login-name	Nom de connexion de l'utilisateur.

2 Pour appliquer les modifications apportées, redémarrez le démon nscd.

```
# svcadm restart system/name-service-cache
```

Si vous avez ajouté un rôle à l'aide d'une interface de la console de gestion Solaris, reportez-vous à la section “Utilisation des rôles (liste des tâches)” à la page 223. Dans le cas contraire, passez à l'étape suivante.

3 (Facultatif) Pour déverrouiller le compte du rôle, l'utilisateur doit créer un mot de passe.

Si vous avez ajouté un rôle local avec la commande `roleadd`, cette étape est obligatoire.

```
% su - rolename
Password:       <Type rolename password>
Confirm Password:       <Retype rolename password>
$
```

Exemple 9–7 Création et attribution d'un rôle local à partir de la ligne de commande

Dans cet exemple, un rôle est créé pour l'administration de la structure cryptographique Oracle Solaris. Le profil de droits de gestion de la cryptographie contient la commande `cryptoadm` pour l'administration des services cryptographiques matériels et logiciels sur un système local.

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m /export/home/cryptoadm -u 104 -s pfksh \
-P "Crypto Management" cryptomgt
# usermod -u 1111 -R cryptomgt
# svcadm restart system/name-service-cache
```

```
% su - cryptomgt
Password:      <Type cryptomgt password>
Confirm Password:      <Retype cryptomgt password>
$ /usr/ucb/whoami
cryptomgt
$
```

Pour plus d'informations sur la structure cryptographique Oracle Solaris, reportez-vous au Chapitre 13, “Structure cryptographique Oracle Solaris (présentation)”. Pour l'administration de la structure, reportez-vous à la rubrique “Administration de la structure cryptographique (liste des tâches)” à la page 303.

▼ Procédure d'audit des rôles

Les actions qu'un rôle effectue peuvent faire l'objet d'un audit. Le nom de connexion de l'utilisateur qui endosse le rôle, le nom de rôle, ainsi que l'action que le rôle effectue sont inclus dans l'enregistrement d'audit. L'événement d'audit `6180:AUE_prof_cmd:profile command:ua,as` collecte les informations. En présélectionnant la classe `as` ou la `ua`, vous pouvez effectuer un audit des actions du rôle.

1 Planifiez l'audit et modifiez les fichiers de configuration d'audit.

Pour plus d'informations, reportez-vous à la section “Audit Oracle Solaris (liste des tâches) ” à la page 619.

2 Incluez la classe `ua` ou `as` à la ligne `flags` du fichier `audit_control`.

```
## audit_control file
flags:lo,as
naflags:lo
plugin:name=audit_binfile.so; p_dir=/var/audit
```

Les classes `ua` et `as` incluent d'autres événements d'audit. Pour voir les événements d'audit qui sont inclus dans une classe, lisez le fichier `audit_event`. Vous pouvez également utiliser la commande `bsmrecord`, tel qu'illustré dans l'Exemple 30–27.

3 Terminez la configuration du service d'audit, puis activez l'audit.

Pour plus d'informations, reportez-vous à la section “Configuration et activation du service d'audit (tâches) ” à la page 631.

▼ Procédure de changement d'un utilisateur `root` en rôle

Cette procédure montre la modification d'un utilisateur de connexion `root` en un rôle root. Lorsque vous effectuez la procédure ci-dessous, vous ne pouvez plus vous connecter directement au système en tant que `root`, sauf en mode monoutilisateur. Le rôle `root` doit vous être affecté et `su` doit être attribué à `root`.

En modifiant l'utilisateur `root` en un rôle, vous empêchez toute connexion `root` anonyme. Étant donné qu'un utilisateur doit se connecter, *puis* endosser le rôle `root`, l'ID de connexion de l'utilisateur est fourni au service d'audit et se trouve dans le fichier `sulog`.

Dans cette procédure, vous créez un utilisateur local et attribuez le rôle `root` à l'utilisateur. Pour empêcher les utilisateurs d'endosser le rôle, reportez-vous à l'Exemple 9–8.

Avant de commencer Vous ne pouvez pas effectuer cette procédure lorsque vous êtes directement connecté en tant que `root`. Vous devez vous connecter en tant que vous-même, puis attribuez `su` à `root`.

1 En tant qu'utilisateur standard, connectez-vous au système cible.

2 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour savoir comment créer le rôle et l'assigner à un utilisateur, reportez-vous à la section "Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)" du *Guide d'administration système : administration de base*.

3 Créez un utilisateur local qui peut endosser le rôle `root`.

Pour des raisons de sécurité, le rôle `root` doit être attribué à au moins un utilisateur local.

`$ useradd -c` *comment* `-u` *uid* `-d` *homedir username*

`-c` *comment*	Commentaire décrivant l'utilisateur.
`-d` *homedir*	Répertoire personnel de l'utilisateur. Ce répertoire doit se trouver sur le système local.
`-u` *uid*	Numéro d'identification de l'utilisateur.
username	Nom du nouvel utilisateur local.

```
# useradd -c "JDoe's local account" -u 123 -d /export/home1 jdoe-local
```

4 Donnez un mot de passe à l'utilisateur.

```
# passwd -r files jdoe-local
New Password:          <Type password>
Re-enter new Password:      <Retype password>
```

```
passwd: password successfully changed for jdoe-local
#
```

5 Assurez-vous de ne pas être connecté en tant que `root`.

```
# who
jdoe    console      May 24 13:51    (:0)
jdoe    pts/5        May 24 13:51    (:0.0)
jdoe    pts/4        May 24 13:51    (:0.0)
jdoe    pts/10       May 24 13:51    (:0.0)
```

6 Modifiez l'utilisateur `root` en rôle.

```
# usermod -K type=role root
```

7 Vérifiez que `root` est un rôle.

L'entrée `root` dans le fichier `user_attr` doit ressembler à ce qui suit :

```
# grep root /etc/user_attr
root::::type=role;auths=solaris.*,solaris.grant;profiles=...
```

8 Attribuez le rôle `root` à votre compte local.

```
# usermod -R root jdoe-local
```

Attention – Si vous n'attribuez pas le rôle `root` à un utilisateur, personne ne peut devenir superutilisateur, sauf en mode monoutilisateur. Vous devez saisir un mot de passe root pour entrer en mode monoutilisateur.

9 Configurez le service de noms à renvoyer en cas d'échec.

a. Ouvrez une nouvelle fenêtre de terminal et endossez le rôle `root`.

```
% whoami
jdoe
% su - jdoe-local
Enter password:        <Type jdoe-local password>
% roles
root
% su - root
Enter password:        <Type root password>
#
```

b. Modifiez le fichier `nsswitch.conf`.

Par exemple, les entrées suivantes du fichier `nsswitch.conf` activent le service de noms à renvoyer.

```
passwd:  files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
group:  files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
```

10 (Facultatif) Attribuez le rôle `root` pour les comptes utilisateur sélectionnés dans le service de noms.

Pour plus d'informations sur cette procédure, reportez-vous à la section “Procédure de modification des propriétés RBAC d'un utilisateur” à la page 235.

Exemple 9–8 Interdiction de l'utilisation du rôle `root` pour configurer un système

Dans cet exemple, la stratégie de sécurité du site requiert que plusieurs rôles discrets configurent le système. Ces rôles discrets ont été créés et testés. Pour empêcher que le compte `root` soit utilisé pour configurer le système, l'administrateur de sécurité change `root` en rôle, mais n'attribue pas le rôle. Le rôle `root` conserve un mot de passe pour entrer dans le système en mode monoutilisateur.

Tout d'abord, l'administrateur vérifie que `root` n'est pas un rôle attribué.

```
% whoami
jdoe-local
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local::::type=normal;roles=secadmin
kdoe-local::::type=normal;roles=sysadmin
```

Toujours dans le compte `root`, l'administrateur change `root` en rôle.

```
# usermod -K type=role root
```

Ensuite, l'administrateur vérifie le changement dans l'entrée `root` du fichier `user_attr`.

```
# grep root /etc/user_attr
root::::type=role;auths=solaris.*,solaris.grant;profiles=...
```

Exemple 9–9 Retour du rôle `root` en utilisateur `root`

Dans cet exemple, l'administrateur désactive un système et souhaite se connecter au bureau en tant que superutilisateur. Le système a été supprimé du réseau.

Tout d'abord, l'administrateur endosse le rôle `root` pour supprimer toutes les attributions de rôle `root`.

```
% whoami
jdoe-local
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local::::type=normal;roles=root
kdoe-local::::type=normal;roles=root
# usermod -R "" jdoe-local
```

```
# usermod -R "" kdoe-local
# grep roles /etc/user_attr
#
```

Toujours dans le rôle `root`, l'administrateur change `root` en utilisateur.

```
# rolemod -K type=normal root
```

Ensuite, l'administrateur vérifie le changement dans l'entrée `root` du fichier `user_attr`.

```
# grep root /etc/user_attr
root::::type=normal;auths=solaris.*,solaris.grant;profiles=...
```

Erreurs fréquentes

Dans un environnement de bureau, vous ne pouvez pas vous connecter directement en tant que `root` lorsque `root` est un rôle. Un message de diagnostic indique que `root` est un rôle sur votre système. Si vous ne disposez pas d'un compte local pouvant endosser le rôle `root`, créez-en un. En tant que `root`, connectez-vous au système en mode monoutilisateur, créez un compte utilisateur local et attribuez le rôle `root` au nouveau compte. Ensuite, connectez-vous en tant que nouvel utilisateur et endossez le rôle `root`.

Personne ne peut devenir superutilisateur si vous modifiez l'utilisateur `root` en rôle et ne parvenez pas à appliquer l'une des attributions suivantes :

- Attribution du rôle `root` à un utilisateur valide.
- Attribution d'un profil de droits équivalent au profil de droits de `root` à un utilisateur valide. Le profil d'administrateur principal est un profil de droits équivalent pour les capacités de `root`.
- Création d'un rôle possédant les capacités de `root` et attribution du rôle à un utilisateur valide. Un rôle auquel le profil d'administrateur principal est attribué équivaut au rôle `root`.

Utilisation des rôles (liste des tâches)

La liste des tâches suivante présente les procédures d'utilisation du rôle après leur attribution.

Tâche	Description	Voir
Utilisation de la console de gestion Solaris	Authentifiez-vous en tant que rôle pour effectuer des tâches d'administration dans la console de gestion Solaris.	"Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226
Endossement d'un rôle dans une fenêtre de terminal	Effectuez des tâches d'administration de ligne de commande dans un shell de profil.	"Procédure d'endossement d'un rôle dans une fenêtre de terminal" à la page 224

Utilisation de rôles

Une fois que des rôles ont été configurés avec des profils de droits Oracle Solaris par défaut et attribués à des utilisateurs, ceux-ci peuvent être utilisés. Un rôle peut être endossé sur la ligne de commande. Dans la console de gestion Solaris, un rôle peut également être utilisé pour l'administration du système au niveau local et sur le réseau.

▼ Procédure d'endossement d'un rôle dans une fenêtre de terminal

Avant de commencer Le rôle doit déjà vous être affecté. Le service de noms doit être mis à jour avec ces informations.

1 Dans une fenêtre de terminal, déterminez les rôles que vous pouvez endosser.

```
% roles
Comma-separated list of role names is displayed
```

2 Utilisez la commande su pour endosser un rôle.

```
% su - rolename
Password:       <Type rolename password>
$
```

La commande `su -` *rolename* change le shell en shell de profil pour le rôle. Un shell de profil reconnaît les attributs de sécurité (autorisations, privilèges et bits ID définis).

3 Vérifiez que vous endossez à présent un rôle.

```
$ /usr/ucb/whoami
rolename
```

Vous pouvez maintenant effectuer des tâches de ce rôle dans cette fenêtre de terminal.

4 (Facultatif) Affichez les capacités de votre rôle.

Pour plus d'informations sur cette procédure, reportez-vous à la section "Détermination des commandes privilégiées qu'un rôle peut exécuter" à la page 271.

Exemple 9–10 Endossement du rôle d'administrateur principal

Dans l'exemple suivant, l'utilisateur endosse le rôle d'administrateur principal. Dans la configuration par défaut, ce rôle équivaut au superutilisateur. Le rôle vérifie ensuite les privilèges disponibles pour toute commande saisie dans le shell de profil pour ce rôle.

```
% roles
sysadmin,oper,primaryadm
% su - primaryadm
Password:       <Type primaryadm password>
$ /usr/ucb/whoami       Prompt has changed to role prompt
```

```
primaryadm
$ ppriv $$
1200:   pfksh
flags = <none>
        E (Effective): all
        I (Inheritable): basic
        P (Permitted): all
        L (Limit): all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section "Privilèges (présentation)" à la page 197.

Exemple 9–11 Endossement du rôle `root`

Dans l'exemple suivant, l'utilisateur endosse le rôle `root`. Le rôle a été créé à la section "Procédure de changement d'un utilisateur `root` en rôle" à la page 220.

```
% roles
root
% su - root
Password:      <Type root password>
# /usr/ucb/whoami       Prompt has changed to role prompt
root
$ ppriv $$
1200:   pfksh
flags = <none>
        E: all
        I: basic
        P: all
        L: all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section "Privilèges (présentation)" à la page 197.

Exemple 9–12 Endossement du rôle d'administrateur système

Dans l'exemple suivant, l'utilisateur endosse le rôle d'administrateur système. À différence du rôle d'administrateur principal, l'administrateur système dispose du jeu de privilèges de base dans son jeu effectif.

```
% roles
sysadmin,oper,primaryadm
% su - sysadmin
Password:      <Type sysadmin password>
$ /usr/ucb/whoami       Prompt has changed to role prompt
sysadmin
$ ppriv $$
1200:   pfksh
```

```
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section “Privilèges (présentation)” à la page 197. Pour obtenir une brève description des possibilités offertes par le rôle, reportez-vous à la section “Profil de droits de l'administrateur système” à la page 243.

▼ Procédure d'endossement d'un rôle dans la console de gestion Solaris

La modification d'informations dans l'interface graphique de la console de gestion Solaris requiert des capacités d'administration. Un rôle vous offre des capacités d'administration. Si vous souhaitez afficher des informations, vous devez avoir l'autorisation `solaris.admin.usermgr.read`. Le profil de droits de l'utilisateur Solaris de base inclut cette autorisation.

Avant de commencer Un rôle d'administration pouvant modifier les propriétés des utilisateurs ou des rôles doit déjà vous avoir été affecté. Par exemple, le rôle d'administrateur principal peut modifier les propriétés des utilisateurs ou des rôles.

1 Démarrez la console de gestion Solaris.

```
% /usr/sbin/smc &
```

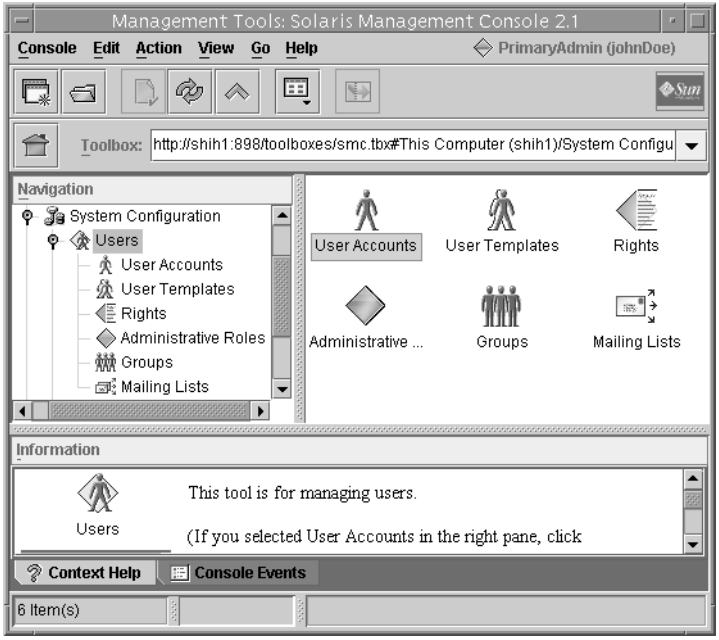
Pour obtenir des instructions détaillées, reportez-vous à la section “Utilisation des outils de gestion Solaris avec RBAC (liste des tâches)” du *Guide d'administration système : administration de base*.

2 Sélectionnez la boîte à outils pour votre tâche.

Naviguez jusqu'à la boîte à outils qui contient l'outil ou la collection dans le champ d'application du service de noms approprié et cliquez sur l'icône. Les champs d'application sont des fichiers (locaux), NIS, NIS+ et LDAP. Si la boîte à outils appropriée n'est pas affichée dans le volet de navigation, choisissez Open Toolbox (Ouvrir une boîte à outils) dans le menu de la console et chargez la boîte à outils nécessaire.

3 **Sélectionnez l'outil à utiliser.**

Accédez à l'outil ou à la collection et cliquez sur l'icône. Les outils de gestion des éléments RBAC se trouvent dans l'outil des utilisateurs, comme indiqué dans la figure suivante.



4 **Saisissez votre nom d'utilisateur et votre mot de passe dans la boîte de dialogue Login: User Name (Connexion : nom utilisateur).**

5 **Authentifiez-vous dans la boîte de dialogue Login: Role (Connexion : rôle).**

Le menu d'options de rôles dans la boîte de dialogue affiche les rôles qui vous sont attribués. Choisissez un rôle, puis tapez le mot de passe du rôle.

Gestion de RBAC (liste des tâches)

La liste des tâches suivante présente les procédures de personnalisation du contrôle d'accès basé sur les rôles (RBAC) après l'implémentation initiale de RBAC.

Tâche	Description	Voir
Changement du mot de passe d'un rôle	Un utilisateur ou un rôle autorisé modifie le mot de passe d'un autre rôle.	"Procédure de modification du mot de passe d'un rôle" à la page 228

Tâche	Description	Voir
Modification des propriétés d'un rôle	Modifie les capacités (privilèges, commandes privilégiées, profils ou autorisations) d'un rôle.	"Procédure de modification des propriétés d'un rôle" à la page 230
Création ou modification de profils de droits	Crée un profil de droits. Ou modifie les autorisations, commandes privilégiées ou profils de droits supplémentaires d'un profil de droits.	"Procédure de création ou de modification d'un profil de droits" à la page 232
Modification des capacités d'administration d'un utilisateur	Ajoute un rôle, un profil de droits, une autorisation ou des privilèges à un utilisateur standard.	"Procédure de modification des propriétés RBAC d'un utilisateur" à la page 235
Sécurisation d'anciennes applications	Active les autorisations d'ID définis pour les anciennes applications. Les scripts peuvent contenir des commandes avec des ID définis. Les anciennes applications peuvent vérifier les autorisations, le cas échéant.	"Procédure d'ajout de propriétés RBAC aux anciennes applications" à la page 237

Ces procédures gèrent les éléments utilisés dans RBAC. Pour connaître les procédures de gestion des utilisateurs, reportez-vous au Chapitre 5, "Gestion des comptes utilisateur et des groupes (tâches) " du *Guide d'administration système : administration de base*.

Gestion de RBAC

L'interface graphique de la console de gestion Solaris est la méthode recommandée pour la gestion de RBAC.

Remarque – Ne tentez pas d'administrer RBAC à l'aide de la ligne de commande et de l'interface graphique en même temps. Des modifications conflictuelles pourraient être apportées à la configuration et le comportement du système serait imprévisible. Ces deux outils permettent d'administrer RBAC, mais ils ne peuvent pas être utilisés simultanément.

▼ Procédure de modification du mot de passe d'un rôle

Avant de commencer Vous devez avoir endossé un rôle incluant le profil de sécurité des utilisateurs ou vous être connecté en tant que superutilisateur. Vous ne pouvez pas endosser le rôle dont vous souhaitez modifier le mot de passe. Un rôle ne peut pas changer son propre mot de passe.

- **Utilisez l'une des méthodes suivantes pour changer le mot de passe d'un rôle.**
  - **En tant que superutilisateur ou rôle incluant le profil de droits de sécurité des utilisateurs, exécutez la commande `passwd`.**

    ```
    $ passwd -r naming-service target-rolename
    ```

`-r` *naming-service*	Applique le changement de mot de passe à l'un des référentiels suivants : `files`, `nis`, `nisplus` ou `ldap`. Si aucun référentiel n'est spécifié, le mot de passe est changé dans `files`.
target-rolename	Nom d'un rôle existant que vous souhaitez modifier.

Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `passwd(1)`.

- **Changez le mot de passe dans la console de gestion Solaris.**

  Pour démarrer la console, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226.

  a. **Connectez-vous à la console en tant que superutilisateur ou endossez un rôle incluant le profil de droits de sécurité des utilisateurs.**

     Le rôle de connexion ne peut pas être le rôle cible.

  b. **Choisissez le champ d'application approprié.**

     Le champ d'application `files` modifie le mot de passe du rôle sur le système local. Le champ d'application `LDAP` modifie le mot de passe du rôle sur le service de nommage LDAP.

  c. **Accédez aux rôles d'administration et suivez les instructions fournies dans le volet de gauche.**

     Pour plus d'informations, reportez-vous à l'aide en ligne.

- **En tant que superutilisateur ou dans un rôle incluant le profil de droits de sécurité des utilisateurs, exécutez la commande `smrole` avec la sous-commande `modify`.**

  Cette commande s'exécute en tant que client du serveur de la console de gestion Solaris.

  ```
  $ /usr/sadm/bin/smrole -D domain-name -r admin-role -l <Type admin-role password> \
  modify -- -n target-rolename  -P password
  ```

`-D` *domain-name*	Nom du domaine que vous souhaitez gérer.
`-r` *admin-role*	Nom du rôle d'administration pouvant modifier le rôle cible. Le rôle d'administration doit disposer de l'autorisation `solaris.admin.usermgr.pswd`. Le rôle d'administration et le rôle cible ne peuvent pas être identiques.
`-l`	Invite pour le mot de passe de *admin-role*.
`--`	Séparateur requis entre les options d'authentification et les options de sous-commande.
`-n` *target-rolename*	Nom du rôle cible.
`-P` *password*	Nouveau mot de passe pour *target-rolename*.

Pour la liste complète des options de commande, reportez-vous à la page de manuel `smrole(1M)`.

Exemple 9–13 Modification du mot de passe d'un rôle local avec la commande `passwd`

Dans cet exemple, le superutilisateur modifie le mot de passe du rôle `operadm` local.

```
# passwd -r files  operadm
New password:       Type new password
Re-enter new password:       Retype new password
```

Exemple 9–14 Modification du mot de passe d'un rôle dans un référentiel LDAP

Dans cet exemple, le rôle d'administrateur principal modifie le mot de passe du rôle `operadm` dans le service d'annuaire LDAP.

```
$ passwd -r ldap operadm
New password:       Type new password
Re-enter new password:       Retype new password
```

Exemple 9–15 Modification du mot de passe d'un rôle à l'aide de la commande `smrole modify`

Dans cet exemple, l'administrateur contacte le serveur de la console de gestion Solaris pour changer le mot de passe `operadm` dans le domaine NIS. Lorsque l'administrateur ne fournit pas le mot de passe avant d'appuyer sur la touche Entrée, l'invite `New Password:` s'affiche.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n operadm -P       Press the Return key
New Password: a!2@3#4$5%6*7
$
```

▼ Procédure de modification des propriétés d'un rôle

Avant de commencer

Vous devez soit endosser un rôle incluant le profil de droits d'administrateur principal, soit vous connecter en tant qu'utilisateur `root` pour modifier les propriétés d'un rôle. Les propriétés du rôle incluent le mot de passe, les profils de droits et les autorisations.

Remarque – Pour changer la propriété de mot de passe d'un rôle, reportez-vous à la section "Procédure de modification du mot de passe d'un rôle" à la page 228.

- **Utilisez l'une des méthodes suivantes pour modifier les propriétés d'un rôle.**

  - **Utilisez l'outil des utilisateurs dans la console de gestion Solaris.**

    Pour démarrer la console, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226. Suivez les instructions données dans le volet gauche pour modifier un rôle dans Administrative Roles. Pour plus d'informations, reportez-vous à l'aide en ligne.

  - **Utilisez la commande `rolemod`.**

    Cette commande modifie les attributs d'un rôle défini dans le service de noms local.

    ```
    $ rolemod -c comment -P profile-list rolename
    ```

`-c` *comment*	Nouveau commentaire décrivant les capacités du rôle.
`-P` *profile-list*	Liste des profils inclus dans le rôle. Cette liste remplace la liste actuelle des profils.
rolename	Nom d'un rôle local existant que vous souhaitez modifier.

    Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `rolemod`(1M).

  - **Utilisez la commande `smrole` avec la sous-commande `modify`.**

    Cette commande permet de modifier les attributs d'un rôle dans un service DNS, tel que NIS, NIS+ ou LDAP. Cette commande s'exécute en tant que client du serveur de la console de gestion Solaris.

    ```
    $ /usr/sadm/bin/smrole -D domain-name \
    -r admin-role -l <Type admin-role password> \
    modify -- -n rolename  -r username -u username
    ```

`-D` *domain-name*	Nom du domaine que vous souhaitez gérer.
`-r` *admin-role*	Nom du rôle d'administration pouvant modifier le rôle. Le rôle d'administration doit disposer de l'autorisation `solaris.role.assign`. Si vous modifiez un rôle que vous avez endossé, il doit avoir l'autorisation `solaris.role.delegate`.
`-l`	Invite pour le mot de passe de *admin-role*.
`--`	Séparateur requis entre les options d'authentification et les options de sous-commande.
`-n` *rolename*	Nom du nouveau rôle.
`-r` *username*	Nom de l'utilisateur ne pouvant plus endosser *rolename*.
`-u` *username*	Nom de l'utilisateur pouvant désormais endosser *rolename*.

Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `smrole(1M)`.

Exemple 9–16 Modification des propriétés d'un rôle local avec la commande `rolemod`

Dans cet exemple, le rôle `operadm` est modifié pour inclure le profil de droits de gestion FTP.

```
$ rolemod -c "Handles printers, backup, and FTP" \
-P "Operator,FTP Management,All" operadm
```

Ces profils de droits sont ajoutés aux profils accordés par l'intermédiaire du fichier `policy.conf`.

Exemple 9–17 Modification des propriétés d'un rôle local avec la commande `smrole modify`

Dans l'exemple suivant, le rôle `operadm` est modifié pour ajouter le profil de droits de gestion FTP.

```
$ /usr/sadm/bin/smrole -r primaryadm -l <Type primaryadm password> \
modify -- -n operadm -c "Handles printers, backup, and FTP" \
-p "FTP Management"
```

Exemple 9–18 Modification d'un rôle dans un domaine avec la commande `smrole modify`,

Dans l'exemple suivant, le rôle `clockmgr` est modifié. L'utilisateur NIS dont l'ID est `108` ne peut plus endosser le rôle. L'utilisateur NIS dont l'ID est `110` peut endosser le rôle `clockmgr`.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n clockmgr -r 108 -u 110
```

▼ Procédure de création ou de modification d'un profil de droits

Un profil de droits est une propriété d'un rôle. Vous devez créer ou modifier un profil de droits lorsque la base de données `prof_attr` ne contient pas de profil de droits correspondant à vos besoins. Pour plus d'informations sur les profils de droits, reportez-vous à la section "Profils de droits RBAC" à la page 194.

Avant de commencer Pour créer ou modifier un profil de droits, vous devez avoir endossé le rôle d'administrateur principal ou vous être connecté en tant que superutilisateur.

- **Utilisez l'une des méthodes suivantes pour créer ou modifier un profil de droits.**

  - **Utilisez l'outil des utilisateurs dans la console de gestion Solaris.**

    Pour démarrer la console, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226. Suivez les instructions du volet gauche pour créer ou modifier un profil de droits dans l'outil de droits. Pour plus d'informations, reportez-vous à l'aide en ligne.

  - **Utilisez la commande `smprofile`.**

    Cette commande vous permet d'ajouter, de modifier, de répertorier ou de supprimer un profil de droits. La commande fonctionne sur des fichiers et dans un service DNS, tel que NIS, NIS+ ou LDAP. La commande `smprofile` s'exécute en tant que client du serveur de la console de gestion Solaris.

    ```
    $ /usr/sadm/bin/smprofile -D domain-name \
    -r admin-role -l <Type admin-role password> \
    add | modify -- -n profile-name \
    -d description  -m help-file -p supplementary-profile
    ```

`-D` *domain-name*	Nom du domaine que vous souhaitez gérer.
`-r` *admin-role*	Nom du rôle d'administration pouvant modifier le rôle. Le rôle d'administration doit disposer de l'autorisation `solaris.role.assign`. Si vous modifiez un rôle que vous avez endossé, il doit avoir l'autorisation `solaris.role.delegate`.
`-l`	Invite pour le mot de passe de *admin-role*.
`--`	Séparateur requis entre les options d'authentification et les options de sous-commande.
`-n` *profile-name*	Nom du nouveau profil.
`-d` *description*	Brève description du profil.
`-m` *help-file*	Nom du fichier d'aide HTML que vous avez créé et placé dans le répertoire `/usr/lib/help/profiles/locale/C`.
`-p` *supplementary-profile*	Nom d'un profil de droits existant inclus dans ce profil de droits. Vous pouvez spécifier plusieurs options `-p` *supplementary-profile*.

    Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `smprofile(1M)`.

Exemple 9–19 Modification d'un profil de droits à partir de la ligne de commande

Dans l'exemple suivant, le profil de droits de gestion du réseau est un profil supplémentaire du profil de droits de sécurité réseau. Le rôle contenant le profil de sécurité réseau peut désormais configurer le réseau et les hôtes, ainsi qu'exécuter des commandes liées à la sécurité.

```
$ /usr/sadm/bin/smprofile -D nisplus:/example.host/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n "Network Security" \
-d "Manage network and host configuration and security" \
-m RtNetConfSec.html -p "Network Management"
```

L'administrateur a créé un nouveau fichier d'aide, `RtNetConfSec.html`, et l'a placé dans le répertoire `/usr/lib/help/profiles/locale/C`, avant d'exécuter cette commande.

Exemple 9–20 Création d'un nouveau profil de droits avec l'outil de droits

Le tableau suivant présente des données d'exemple pour un profil de droits hypothétique appelé "Build Administrator" (administrateur de versions). Ce profil de droits inclut les commandes dans le sous-répertoire `/usr/local/swctrl/bin`. Ces commandes ont un UID effectif de `0`. Le profil de droits de l'administrateur de versions peut être utile pour les administrateurs gérant les différentes versions pour le développement de logiciels.

Onglet	Champ	Exemple
Généralités	Nom	Administrateur de version
	Description	Gestion des versions logicielles.
	Nom du fichier d'aide	`BuildAdmin.html`
Commandes	Ajouter un répertoire	Cliquez sur Add Directory (Ajouter un répertoire), entrez `/usr/local/swctrl/bin` dans la boîte de dialogue, puis cliquez sur OK.
	Commandes refusées / Commandes autorisées	Déplacez `/usr/local/swctrl/bin` dans la colonne Commands Permitted (Commandes autorisées).
	Définir les attributs de sécurité	Sélectionnez `/usr/local/swctrl/bin`, cliquez sur Set Security Attributes (Définir les attributs de sécurité) et définissez Effective UID = `root`.
Autorisations	Autorisations exclues / Autorisations incluses	*Aucune autorisation.*
Droits supplémentaires	Droits exclus / Droits inclus	*Aucun profil de droits supplémentaire.*

Erreurs fréquentes

Vérifiez les points suivants si le profil de droits ne fournit pas le rôle avec les capacités attendues :

- Les profils de droits pour le rôle s'affichent-ils dans l'interface graphique dans l'ordre du plus puissant au moins puissant ?

  Par exemple, si le profil de droits `All` s'affiche en haut de la liste, aucune commande n'est exécutée avec les attributs de sécurité. Un profil contenant des commandes avec des attributs de sécurité doit précéder le profil de droits `All` dans la liste.

- Une commande est-elle répertoriée plus d'une fois dans les profils de droits du rôle ? Si tel est le cas, la première instance de la commande dispose-t-elle de tous les attributs de sécurité nécessaires ?

  Par exemple, une commande peut nécessiter des privilèges pour des options particulières. Pour que les options nécessitant des privilèges s'exécutent correctement, la première instance de la commande dans le profil de droits situé le plus haut dans la liste doit disposer des privilèges attribués.

- Les commandes des profils de droits du rôle disposent-elles des attributs de sécurité appropriés ?

  Par exemple, lorsque la stratégie est `suser`, certaines commandes requièrent `uid=0` plutôt que `euid=0` pour s'exécuter correctement.

- Le cache de service de noms, `svc:/system/name-service-cache`, a-t-il été redémarré ?

  Le démon `nscd` peut avoir un long intervalle de durée de vie. En redémarrant le démon, vous mettez à jour le service de noms avec les données en cours.

▼ Procédure de modification des propriétés RBAC d'un utilisateur

Les propriétés de l'utilisateur incluent le mot de passe, les profils de droits, les rôles et les autorisations. La méthode la plus sûre pour accorder des capacités d'administration à un utilisateur est de lui attribuer un rôle. Pour plus de détails, reportez-vous à la section "Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité " à la page 196.

Avant de commencer

Vous devez soit endosser un rôle incluant le profil de droits de l'administrateur principal, soit vous connecter en tant qu'utilisateur `root`.

- **Utilisez l'une des méthodes suivantes pour modifier les propriétés RBAC d'un utilisateur.**

  - **Utilisez l'outil des utilisateurs dans la console de gestion Solaris.**

    Pour démarrer la console, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226. Suivez les instructions données dans le volet gauche pour modifier un utilisateur dans User Accounts. Pour plus d'informations, reportez-vous à l'aide en ligne.

    Astuce – Il n'est pas recommandé d'attribuer des autorisations, des privilèges ou des profils de droits directement à des utilisateurs. La meilleure approche consiste à attribuer un rôle aux utilisateurs. Les utilisateurs endossent ensuite un rôle pour effectuer des opérations requérant des privilèges.

  - **Utilisez la commande `usermod`.**

    Cette commande permet de modifier les attributs d'un utilisateur défini dans le service de noms local.

    ```
    $ usermod -R rolename username
    ```

    `-R` *rolename* Nom du rôle local existant.

    username Nom d'un utilisateur local existant que vous souhaitez modifier.

    Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `usermod`(1M).

  - **Utilisez la commande `smuser` avec la sous-commande `modify`.**

    Cette commande permet de modifier les attributs d'un utilisateur dans un service DNS, tel que NIS, NIS+ ou LDAP. Cette commande s'exécute en tant que client du serveur de la console de gestion Solaris.

    ```
    $ /usr/sadm/bin/smuser -D domain-name \
    -r admin-role -l <Type admin-role password> \
    modify -- -n username -a rolename
    ```

    `-D` *domain-name* Nom du domaine que vous souhaitez gérer.

    `-r` *admin-role* Nom du rôle d'administration pouvant modifier le rôle. Le rôle d'administration doit disposer de l'autorisation `solaris.role.assign`. Si vous modifiez un rôle que vous avez endossé, il doit avoir l'autorisation `solaris.role.delegate`.

    `-l` Invite pour le mot de passe de *admin-role*.

    `--` Séparateur requis entre les options d'authentification et les options de sous-commande.

    `-n` *username* Nom de l'utilisateur auquel *rolename* est attribué.

`-a` *rolename* Nom du rôle que vous attribuez au *username*. Vous pouvez spécifier plusieurs options `-a` *rolename*.

Pour obtenir d'autres options de commande, reportez-vous à la page de manuel `smuser(1M)`.

Exemple 9–21 Modification des propriétés RBAC d'un utilisateur local à partir de la ligne de commande

Dans cet exemple, l'utilisateur `jdoe` peut désormais endosser le rôle d'administrateur système.

```
$ usermod -R sysadmin jdoe
```

Ce rôle est ajouté aux rôles pouvant être endossés par l'utilisateur.

Exemple 9–22 Modification des propriétés RBAC d'un utilisateur avec la commande `smuser`

Dans cet exemple, l'utilisateur `jdoe` se voit attribuer deux rôles : administrateur système et opérateur. L'utilisateur et les rôles étant définis localement, l'option `-D` n'est pas nécessaire.

```
$ /usr/sadm/bin/smuser -r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm
```

Dans l'exemple suivant, l'utilisateur est défini dans le service de noms NIS. Par conséquent, l'option `-D` est requise. Deux rôles sont définis dans le service de noms. Un rôle, `root`, est défini localement.

```
$ /usr/sadm/bin/smuser -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm -a root
```

▼ Procédure d'ajout de propriétés RBAC aux anciennes applications

Une ancienne application est une commande ou un jeu de commandes. Les attributs de sécurité sont définis pour chaque commande dans un profil de droits. Le profil de droits est ensuite inclus dans un rôle. Un utilisateur qui endosse le rôle peut exécuter l'ancienne application avec les attributs de sécurité.

Pour ajouter d'anciennes applications à la console de gestion Solaris, reportez-vous à la section "Ajout d'outils à la console de gestion Solaris" du *Guide d'administration système : administration de base*.

Avant de commencer Vous devez avoir endossé le rôle d'administrateur principal ou vous être connecté en tant que superutilisateur pour modifier les attributs de sécurité d'une commande dans un profil de droits.

1. **Utilisez l'outil des utilisateurs dans la console de gestion Solaris.**

   Pour démarrer la console, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226. Suivez les instructions du volet gauche pour modifier un profil de droits dans l'outil de droits. Pour plus d'informations, reportez-vous à l'aide en ligne.

2. **Ajoutez les attributs de sécurité aux commandes qui implémentent l'ancienne application.**

   Vous pouvez ajouter les attributs de sécurité à une ancienne application de la même façon que vous le feriez pour n'importe quelle commande. Vous devez ajouter la commande avec les attributs de sécurité à un profil de droits. Pour une commande héritée, donnez-lui les attributs de sécurité `euid=0` ou `uid=0`. Pour plus d'informations sur cette procédure, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" à la page 232.

3. **Après l'ajout de l'ancienne application à un profil de droits, incluez le profil de droits dans la liste des profils d'un rôle.**

   Pour ajouter un profil de droits à un rôle, reportez-vous à la section "Procédure de modification des propriétés d'un rôle" à la page 230.

Exemple 9–23 Ajout d'attributs de sécurité à des commandes dans un script

Si une commande d'un script doit avoir le bit `setuid` ou `setgid` défini pour s'exécuter correctement, les attributs de sécurité du fichier exécutable du script *et* de la commande doivent être ajoutés dans un profil de droits. Ensuite, le profil de droits est inclus dans un rôle et le rôle est assigné à un utilisateur. Lorsque l'utilisateur endosse le rôle et exécute le script, la commande s'exécute avec les attributs de sécurité.

Pour ajouter les attributs de sécurité à une commande ou un script shell, reportez-vous à la section "Procédure de création ou de modification d'un profil de droits" à la page 232.

Exemple 9–24 Recherche d'autorisations dans un script ou un programme

Pour avoir un script pour les autorisations, vous devez ajouter un test basé sur la commande `auths`. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel `auths(1)`.

Par exemple, la ligne suivante vérifie si l'utilisateur dispose de l'autorisation fournie comme argument `$1` :

```
if [ `/usr/bin/auths|/usr/xpg4/bin/grep $1` ]; then
        echo Auth granted
else
        echo Auth denied
fi
```

Pour être plus complet, le test doit inclure une logique vérifiant la présence d'autres autorisations utilisant des caractères génériques. Par exemple, pour tester si l'utilisateur dispose de l'autorisation `solaris.admin.usermgr.write`, vous devez recherchez les chaînes suivantes :

- `solaris.admin.usermgr.write`
- `solaris.admin.usermgr.*`
- `solaris.admin.*`
- `solaris.*`

Si vous écrivez un programme, utilisez la fonction `getauthattr()` pour effectuer un test d'autorisation.

◆ ◆ ◆ CHAPITRE 10

Contrôle d'accès basé sur les rôles (référence)

Ce chapitre fournit des informations de référence sur le RBAC. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre :

Pour plus d'informations sur l'utilisation de RBAC, reportez-vous au Chapitre 9, "Utilisation du contrôle d'accès basé sur les rôles (tâches)". Pour obtenir des informations de présentation, reportez-vous à la section "Contrôle d'accès basé sur les rôles (présentation) " à la page 186.

Contenu des profils de droits

Cette section décrit des profils de droits typiques. Les profils de droits peuvent inclure des autorisations, des commandes avec des attributs de sécurité et des profils de droits supplémentaires. Les profils de droits sont répertoriés dans l'ordre de puissance décroissante. Pour obtenir des suggestions sur la façon de distribuer les profils de droits aux rôles de votre site, reportez-vous à la section "Procédure de planification de votre implémentation RBAC" à la page 209.

- **Profil de droits de l'administrateur principal (Primary Administrator) :** fournit les capacités de superutilisateur dans un profil.
- **Profil de droits de l'administrateur système (System Administrator) :** fournit un profil pouvant effectuer la plupart des tâches qui ne sont pas en rapport avec la sécurité. Ce profil inclut plusieurs autres profils permettant de créer un rôle puissant.
- **Profil de droits de l'opérateur (Operator) :** fournit des capacités limitées pour gérer des fichiers et des supports hors ligne. Ce profil inclut des profils de droits supplémentaires pour créer un rôle simple.

- **Profil de droits de gestion d'imprimantes (Printer Management) :** fournit un nombre limité de commandes et d'autorisations pour la gestion de l'impression. Ce profil est l'un des nombreux profils couvrant une seule partie de l'administration.
- **Profil de droits de l'utilisateur Solaris de base (Basic Solaris User) :** permet aux utilisateurs d'utiliser le système dans les limites de la stratégie de sécurité. Ce profil est répertorié par défaut dans le fichier `policy.conf`.
- **Profil de droits Tous (All) :** permet aux rôles d'accéder aux commandes n'ayant pas d'attribut de sécurité.

Chaque profil de droits est associé à un fichier d'aide. Les fichiers d'aide sont au format HTML et sont personnalisables. Les fichiers sont stockés dans le répertoire `/usr/lib/help/profiles/locale/C`.

Profil de droits de l'administrateur principal

Le profil de droits de l'administrateur principal est attribué au rôle le plus puissant sur le système. Le rôle qui inclut le profil de droits d'administrateur principal possède des capacités de superutilisateur.

- L'autorisation `solaris.*` attribue toutes les autorisations qui sont fournies par le logiciel Oracle Solaris.
- L'autorisation `solaris.grant` permet à un rôle d'affecter n'importe quelle autorisation à n'importe quel profil de droits, rôle ou utilisateur.
- L'assignation de la commande `*:uid=0;gid=0` offre la possibilité d'exécuter n'importe quelle commande avec `UID=0` et `GID=0`.

Vous pouvez personnaliser le fichier d'aide `RtPriAdmin.html` pour votre site, si nécessaire. Les fichiers d'aide sont stockés dans le répertoire `/usr/lib/help/profiles /locale/C`.

Notez également que si le profil de droits de l'administrateur principal n'est pas cohérent avec la stratégie de sécurité d'un site, ce profil peut être modifié ou ne pas être attribué du tout. Toutefois, les fonctions de sécurité du profil de droits de l'administrateur principal devront être gérées dans un ou plusieurs autres profils de droits. Ces autres profils doivent alors être attribués à des rôles.

TABLEAU 10–1 Contenu du profil de droits de l'administrateur principal

Objectif	Contenu
Effectuer toutes les tâches d'administration	**Commandes** : `*:uid=0;gid=0`
	Autorisations : `solaris.*`, `solaris.grant`
	Fichier d'aide : `RtPriAdmin.html`

Profil de droits de l'administrateur système

Le profil de droits de l'administrateur système est prévu pour le rôle d'administrateur système. L'administrateur système n'ayant pas l'amplitude des capacités de l'administrateur principal, les caractères génériques ne sont pas utilisés. À la place, ce profil est constitué d'un jeu de profils de droits d'administration discrets supplémentaires n'ayant pas trait à la sécurité. Les commandes avec des attributs de sécurité issus de l'un des profils de droits supplémentaires sont affichées.

Notez que le profil de droits Tous est attribué à la fin de la liste des profils de droits supplémentaires.

TABLEAU 10–2 Contenu du profil de droits de l'administrateur système

Objectif	Contenu
Pour effectuer la plupart des tâches d'administration (hors sécurité)	**Profil de droits supplémentaires** : vérification d'audit, gestion d'imprimantes, gestion cron, gestion des périphériques, gestion des systèmes de fichiers, gestion de la messagerie, maintenance et réparation, gestion du service de noms, gestion du réseau, gestion de l'accès aux objets, gestion des processus, installation des logiciels, gestion de projets, gestion des utilisateurs, tous **Fichier d'aide** : `RtSysAdmin.html`
Commandes issues de l'un des profils supplémentaires	**Profil de droits de gestion de l'accès aux objets**, stratégie `solaris` : `/usr/bin/chgrp:privs=file_chown`, `/usr/bin/chmod:privs=file_chown`, `/usr/bin/chown:privs=file_chown` , `/usr/bin/setfacl:privs=file_chown` Stratégie `suser` : `/usr/bin/chgrp:euid=0`, `/usr/bin/chmod:euid=0`, `/usr/bin/chown:euid=0`, `/usr/bin/getfacl:euid=0`, `/usr/bin/setfacl:euid=0`

Profil de droits de l'opérateur

Le profil de droits de l'opérateur est un profil moins puissant, qui offre la capacité d'effectuer des sauvegardes et la maintenance d'imprimantes. La possibilité de restaurer les fichiers implique davantage de conséquences en matière de sécurité. C'est pourquoi, dans ce profil, la possibilité de restaurer les fichiers n'est pas incluse par défaut.

TABLEAU 10–3 Contenu du profil de droits de l'opérateur

Objectif	Contenu
Effectuer des tâches d'administration simples	**Profils de droits supplémentaires** : gestion d'imprimantes, sauvegarde des supports, tous **Fichier d'aide** : `RtOperator.html`

Profil de droits de gestion d'imprimantes

La gestion d'imprimantes et un profil de droits typiques prévu pour un type de tâches spécifique. Ce profil inclut les autorisations et les commandes. Le tableau suivant présente une liste partielle des commandes.

TABLEAU 10–4 Contenu du profil de droits de gestion d'imprimantes

Objectif	Contenu
Gérer les imprimantes, les démons et le spool	**Autorisations** : `solaris.print.*`, `solaris.label.print`, `solaris.admin.printer.delete`, `solaris.admin.printer.modify`, `solaris.admin.printer.read` , `solaris.smf.manage.discovery.printers.*`, `solaris.smf.value.discovery.printers.*` **Commandes** : `/usr/lib/lp/local/lpadmin:uid=lp;gid =lp`, `/usr/sbin/lpfilter:euid=lp;uid=lp`, `/usr/sbin/lpforms:euid=lp`, `/usr/sbin/lpusers:euid=lp`, `/usr/sbin/ppdmgr:euid=0` **Fichier d'aide** : `RtPrntMngmnt.html`

Profil de droits de l'utilisateur Solaris de base

Par défaut, le profil de droits de l'utilisateur Solaris de base est attribué automatiquement à tous les utilisateurs par le biais du fichier `policy.conf`. Ce profil contient des autorisations de base qui sont utiles dans le cadre d'un fonctionnement normal. Notez que les avantages proposés par le profil de droits de l'utilisateur Solaris de base doivent être contrebalancés avec les exigences en matière de sécurité du site. Les sites nécessitant une sécurité plus stricte préféreront peut-être supprimer ce profil du fichier `policy.conf`.

TABLEAU 10–5 Contenu du profil de droits de l'utilisateur Solaris de base

Objectif	Contenu
Pour attribuer automatiquement des droits à tous les utilisateurs	**Autorisations** : `solaris.profmgr.read`, `solaris.jobs.user`, `solaris.mail.mailq`, `solaris.device.mount.removable`, `solaris.admin.usermgr.read` , `solaris.admin.logsvc.read`, `solaris.admin.fsmgr.read`, `solaris.admin.serialmgr.read`, `solaris.admin.diskmgr.read`, `solaris.admin.procmgr.user`, `solaris.compsys.read` , `solaris.admin.printer.read`, `solaris.admin.prodreg.read`, `solaris.admin.dcmgr.read`, `solaris.snmp.read`, `solaris.project.read`, `solaris.admin.patchmg.read` , `solaris.network.hosts.read`, `solaris.admin.volmgr.read` **Profils de droits supplémentaires** : tous **Fichier d'aide** : `RtDefault.html`

Profils de droits Tous

Le profil de droits Tous utilise le caractère générique pour inclure toutes les commandes. Ce profil fournit un rôle avec l'accès à l'ensemble des commandes qui ne sont pas explicitement attribuées dans d'autres profils de droits. Sans le profil de droits Tous ou d'autres profils de droits utilisant les caractères génériques, un rôle a uniquement accès aux commandes explicitement attribuées. Ce type d'ensemble de commandes n'est pas très pratique. Aucune autorisation n'est incluse dans ce profil.

S'il est utilisé, le profil de droits Tous doit être le dernier profil de droits attribué. Cette dernière position assure l'application d'attributs de sécurité explicites dans d'autres profils de droits.

TABLEAU 10–6 Contenu du profil de droits Tous

Objectif	Contenu
Exécuter n'importe quelle commande en tant qu'utilisateur ou rôle	**Commandes** : * **Fichier d'aide** : `RtAll.html`

Ordre des profils de droits

Les commandes des profils de droits sont interprétées dans l'ordre. La première occurrence d'une commande est la seule version de la commande utilisée pour ce rôle ou utilisateur. Des profils de droits différents peuvent inclure la même commande. D'où l'importance de l'ordre des profils de droits dans la liste correspondante. Le profil de droits doté du plus grand nombre de capacités doit figurer en premier.

Les profils de droits sont répertoriés dans l'interface graphique de la console de gestion Solaris et dans le fichier `prof_attr`. Dans l'interface graphique de la console de gestion Solaris, le profil de droits doté du plus grand nombre de capacités doit être le premier dans la liste des profils de droits attribués. Dans le fichier `prof_attr`, le profil de droits doté du plus grand nombre de capacités doit être le premier d'une liste de profils supplémentaires. Cette position permet de s'assurer qu'une commande avec des attributs de sécurité est répertoriée avant la même commande sans attributs de sécurité.

Affichage du contenu des profils de droits

L'outil des droits de la console de gestion Solaris (Solaris Management Console Rights) fournit un moyen de contrôler le contenu des profils de droits.

Les fichiers `prof_attr` et `exec_attr` offrent une vue plus fragmentée. Le fichier `prof_attr` contient le nom de chaque profil de droits défini sur le système. Le fichier comprend également les autorisations, les privilèges et les profils de droits supplémentaires pour chaque profil. Le fichier `exec_attr` contient les noms des profils de droits et de leurs commandes avec les attributs de sécurité.

Délégation et nommage des autorisations

Une *autorisation* RBAC est un droit discret qui peut être accordé à un rôle ou à un utilisateur. Les autorisations sont vérifiées par les applications conformes aux normes RBAC avant qu'un utilisateur n'ait accès à l'application ou aux opérations spécifiques au sein de l'application. Cette vérification remplace les tests dans les applications UNIX conventionnelles pour `UID=0`.

Conventions de nommage des autorisations

Une autorisation a un nom qui est utilisé en interne et dans des fichiers. Par exemple, `solaris.admin.usermgr.pswd` est le nom d'une autorisation. Une autorisation est accompagnée d'une description courte, qui s'affiche dans les interfaces graphiques. Par exemple, `Change Passwords` est la description de l'autorisation `solaris.admin.usermgr.pswd`.

Par convention, les noms d'autorisations sont construits dans l'ordre inverse suivant : nom du fournisseur Internet, partie de l'objet, toutes sous-parties et fonction. Les parties du nom d'autorisation sont séparées par des points. Un exemple serait `com.xyzcorp.device.access`. Les exceptions à cette convention sont les autorisations de Sun Microsystems, Inc., qui utilisent le préfixe `solaris` au lieu d'un nom Internet. La convention de nommage permet aux administrateurs d'appliquer des autorisations de manière hiérarchique. Un caractère générique (*) peut représenter des chaînes à droite d'un point.

Exemple de granularité d'autorisation

Exemple d'utilisation des autorisations : un utilisateur dans le rôle d'opérateur peut être limité à l'autorisation `solaris.admin.usermgr.read` qui fournit un accès en lecture, mais non en écriture aux fichiers de configuration utilisateur. Le rôle d'administrateur système dispose naturellement des autorisations `solaris.admin.usermgr.read` et `solaris.admin.usermgr.write` lui permettant d'apporter des modifications aux fichiers utilisateur. Toutefois, sans l'autorisation `solaris.admin.usermgr.pswd`, l'administrateur système ne peut pas changer les mots de passe. L'administrateur principal possède ces trois autorisations.

L'autorisation `solaris.admin.usermgr.pswd` est nécessaire pour effectuer des modifications de mot de passe dans l'outil utilisateur de la console de gestion Solaris. Cette autorisation est également requise pour l'utilisation des options de modification de mot de passe dans les commandes `smuser`, `smmultiuser` et `smrole`.

Pouvoir de délégation dans les autorisations

Une autorisation se terminant par le suffixe `grant` permet à un utilisateur ou à un rôle de déléguer à d'autres utilisateurs des autorisations attribuées commençant par le même préfixe.

Par exemple, un rôle avec les autorisations `solaris.admin.usermgr.grant` et `solaris.admin.usermgr.read` peut déléguer l'autorisation `solaris.admin.usermgr.read` à un autre utilisateur. Un rôle avec les autorisations `solaris.admin.usermgr.grant` et `solaris.admin.usermgr.*` peut déléguer toutes les autorisations portant le préfixe `solaris.admin.usermgr` à d'autres utilisateurs.

Bases de données prenant en charge RBAC

Les quatre bases de données suivantes stockent les données pour les éléments RBAC :

- **Base de données d'attributs utilisateur étendus** (`user_attr`) **:** associe des utilisateurs et des rôles à des autorisations, des privilèges et des profils de droits.
- **Base de données d'attributs de profils de droits** (`prof_attr`) **:** définit les profils de droits, répertorie les autorisations et mots de passe attribués des profils et identifie le fichier d'aide associé.
- **Base de données d'attributs d'autorisations** (`auth_attr`) **:** définit les autorisations et leurs attributs, et identifie le fichier d'aide associé.
- **Base de données d'attributs d'exécution** (`exec_attr`) **:** identifie les commandes portant des attributs de sécurité attribués à des profils de droits spécifiques.

La base de données `policy.conf` contient des autorisations, des privilèges et des profils de droits appliqués à tous les utilisateurs. Pour plus d'informations, reportez-vous à la section "Fichier `policy.conf`" à la page 254.

Relations avec la base de données RBAC

Chaque base de données RBAC utilise une syntaxe *key=value* pour stocker les attributs. Cette méthode tient compte des possibilités d'extension future des bases de données. La méthode permet également à un système de continuer à fonctionner lorsqu'il rencontre un mot-clé inconnu de sa stratégie. Le contenu de *key=value* lie les fichiers. Les entrées suivantes liées à partir des quatre bases de données illustrent la façon dont les bases de données RBAC fonctionnent ensemble.

EXEMPLE 10–1 Affichage des connexions de base de données RBAC

Dans l'exemple suivant, l'utilisateur `jdoe` obtient les capacités du profil de droits de gestion des systèmes de fichiers par l'attribution du rôle `filemgr`.

1. L'utilisateur `jdoe` se voit attribuer le rôle `filemgr` dans l'entrée utilisateur `jdoe` de la base de données `user_attr`.

   ```
   # user_attr - user definition
   jdoe::::type=normal;roles=filemgr
   ```

2. Le rôle `filemgr` se voit attribuer le profil de droits de gestion des systèmes de fichiers dans l'entrée du rôle dans la base de données `user_attr`.

   ```
   # user_attr - role definition
   filemgr::::profiles=File System Management;type=role
   ```

   L'utilisateur et le rôle sont uniquement définis dans les fichiers `passwd` et `shadow` sur le système local ou dans les bases de données équivalentes distribués dans un service DNS.

3. Le profil de droits de gestion de systèmes de fichiers est défini dans la base de données `prof_attr`. Cette base de données attribue également trois jeux d'autorisations à l'entrée de gestion de systèmes de fichiers.

   ```
   # prof_attr - rights profile definitions and assigned authorizations
   File System Management:::Manage, mount, share file systems:
   help=RtFileSysMngmnt.html;
   auths=solaris.admin.fsmgr.*,solaris.admin.diskmgr.*,solaris.admin.volmgr.*
   ```

4. Les autorisations sont définies dans la base de données `auth_attr`.

   ```
   # auth_attr - authorization definitions
   solaris.admin.fsmgr.:::Mounts and Shares::help=AuthFsmgrHeader.html
   solaris.admin.fsmgr.read:::View Mounts and Shares::help=AuthFsmgrRead.html
   solaris.admin.fsmgr.write:::Mount and Share Files::help=AuthFsmgrWrite.html
   ```

5. Le profil de droits de gestion de systèmes de fichiers se voit affecter des commandes avec des attributs de sécurité dans la base de données `exec_attr`.

EXEMPLE 10–1 Affichage des connexions de base de données RBAC *(Suite)*

```
# exec_attr - rights profile names with secured commands
File System Management:suser:cmd:::/usr/sbin/mount:uid=0
File System Management:suser:cmd:::/usr/sbin/dfshares:euid=0
...
File System Management:solaris:cmd:::/usr/sbin/mount:privs=sys_mount
...
```

Bases de données RBAC et services de nommage

Le champ d'application du service de noms des bases de données RBAC s'applique uniquement à l'hôte local. Elle peut également inclure tous les hôtes qui sont pris en charge par un service de nommage, tel que NIS, NIS+ ou LDAP. L'affectation de la priorité à un service de nommage donné est définie pour chacune des bases de données dans le fichier `/etc/nsswitch.conf`.

- `auth_attr` **(entrée) :** définit la priorité d'un service de nommage pour la base de données `auth_attr`.
- `passwd` **(entrée) :** définit la priorité d'un service de nommage pour la base de données `user_attr`.
- `prof_attr` **(entrée) :** définit la priorité d'un service de nommage pour la base de données `prof_attr`. Définit également la priorité d'un service de nommage pour la base de données `exec_attr`.

  Par exemple, si une commande dotée d'attributs de sécurité est attribuée à un profil de droits existant dans les deux services de nommage, seule l'entrée du premier service est utilisée.

Base de données `user_attr`

La base de données `user_attr` contient des informations sur l'utilisateur et le rôle qui complètent les bases de données `passwd` et `shadow`. La base de données `user_attr` contient des attributs utilisateur étendus tels que les autorisations, les profils de droits, les privilèges et les rôles attribués. Les champs dans la base de données `user_attr` sont séparés par deux points, comme suit :

```
user:qualifier:res1:res2:attr
```

Les champs ont les significations suivantes :

`user`
: Nom de l'utilisateur ou du rôle comme indiqué dans la base de données `passwd`.

`qualifier:res1:res2`
: Ces champs sont réservés pour une utilisation ultérieure.

`attr`
: Liste optionnelle de paires clé-valeur séparées par des points-virgules (`;`) qui décrit les attributs de sécurité à appliquer lorsque l'utilisateur exécute des commandes. Les quatre clés correctes sont `type`, `auths`, `profiles` et `roles`.

  - Le mot-clé `type` peut être défini sur `normal`, si ce compte est pour un utilisateur standard. Le `type` est `role` si ce compte est pour un rôle.
  - Le mot-clé `auths` indique une liste de noms d'autorisations séparés par des virgules qui sont choisis parmi des noms définis dans la base de données `auth_attr`. Les noms d'autorisations peuvent inclure l'astérisque (`*`) comme caractère générique. Par exemple, `solaris.device.*` signifie toutes les autorisations des périphériques Oracle Solaris.
  - Le mot-clé `profiles` indique une liste de noms de profils de droits ordonnés, séparés par des virgules et issus de la base de données `prof_attr`. L'ordre des profils de droits fonctionne de façon similaire aux chemins de recherche UNIX. Le premier profil de la liste qui contient la commande à exécuter définit les attributs de sécurité (le cas échéant) devant être appliqués à la commande.
  - Le mot-clé `roles` spécifie une liste de noms de rôles séparés par des virgules. Notez que les rôles sont définis dans la même base de données `user_attr`. Les rôles sont indiqués en définissant la valeur type sur `role`. Les rôles ne peuvent pas être attribués à d'autres rôles.

L'exemple suivant montre comment le rôle d'opérateur est défini dans une base de données `user_attr` standard. L'exemple illustre la façon dont le rôle est attribué à l'utilisateur `jdoe`. Les rôles et les utilisateurs sont différenciés par le mot-clé `type`.

```
% grep operator /etc/user_attr
jdoe::::type=normal;roles=operator
operator::::profiles=Operator;type=role
```

Base de données `auth_attr`

Toutes les autorisations sont stockées dans la base de données `auth_attr`. Les autorisations peuvent être affectées à des utilisateurs, des rôles ou aux profils de droits. La meilleure méthode consiste à placer les autorisations dans un profil de droits, afin d'inclure le profil dans la liste des profils d'un rôle, puis d'affecter le rôle à un utilisateur.

Les champs dans la base de données `auth_attr` sont séparés par deux points, comme suit :

```
authname:res1:res2:short_desc:long_desc:attr
```

Les champs ont les significations suivantes :

`authname`
: Chaîne de caractère unique utilisée pour identifier l'autorisation au format *prefix*.[*suffix*]. Autorisations pour qu'Oracle Solaris utilise `solaris` comme préfixe. Toutes les autres autorisations doivent utiliser un préfixe qui commence par le nom de domaine Internet dans l'ordre inverse de

l'organisation créant l'autorisation (par exemple, `com.xyzcompany`). Le suffixe indique ce qui est autorisé, c'est-à-dire généralement la zone fonctionnelle et l'opération.

Lorsque `authname` se compose d'un préfixe et d'une zone fonctionnelle et se termine par un point, `authname` sert d'en-tête à utiliser par les applications dans leurs interfaces graphiques. Un nom d'autorisation `authname` en deux parties n'est pas une véritable autorisation. Le nom d'autorisation `authname` de `solaris.printmgr.` est un exemple d'en-tête.

Quand `authname` se termine par le mot “grant”, `authname` sert d'autorisation d'attribution de droits. Cette autorisation permet à l'utilisateur de déléguer à d'autres utilisateurs des autorisations avec le même préfixe et la même zone fonctionnelle. `authname` de `solaris.printmgr.grant` est un exemple d'autorisation d'attribution de droits. `solaris.printmgr.grant` donne à l'utilisateur le droit de déléguer à d'autres utilisateurs des autorisations telles que `solaris.printmgr.admin` et `solaris.printmgr.nobanner`.

`res1:res2` Réservé à une utilisation ultérieure.

`short_desc` Nom court pour l'autorisation. Ce nom court est adapté pour un affichage dans des interfaces utilisateur, comme dans une liste déroulante d'une interface graphique.

`long_desc` Description longue. Ce champ identifie l'objectif de l'autorisation, les applications dans lesquelles l'autorisation est utilisée et le type d'utilisateur pouvant utiliser l'autorisation. La description longue peut être affichée dans le texte de l'aide d'une application.

`attr` Liste optionnelle de paires clé-valeur séparées par des points-virgules (;) décrivant les attributs d'une autorisation. Zéro ou plusieurs clés peuvent être spécifiées.

Le mot-clé `help` identifie un fichier d'aide au format HTML. Les fichiers d'aide sont accessibles à partir du fichier `index.html` dans le répertoire `/usr/lib/help/auths/locale/C`.

L'exemple suivant montre une base de données `auth_attr` avec certaines valeurs types :

```
% grep printer /etc/security/auth_attr
solaris.admin.printer.:::Printer Information::help=AuthPrinterHeader.html
solaris.admin.printer.delete:::Delete Printer Information::help=AuthPrinterDelete.html
solaris.admin.printer.modify:::Update Printer Information::help=AuthPrinterModify.html
solaris.admin.printer.read:::View Printer Information::help=AuthPrinterRead.html
```

Notez que `solaris.admin.printer.` est défini comme un en-tête, car le nom de l'autorisation se termine par un point (.). Les en-têtes sont utilisés par les interfaces graphiques afin d'organiser les familles d'autorisations.

Base de données `prof_attr`

La base de données `prof_attr` contient le nom, la description, l'emplacement du fichier d'aide, les privilèges et les autorisations qui sont affectés à des profils de droits. Les commandes et les attributs de sécurité qui sont affectés à des profils de droits sont stockés dans la base de données `exec_attr`. Pour plus d'informations, reportez-vous à la section "Base de données `exec_attr`" à la page 253. Les champs dans la base de données `prof_attr` sont séparés par deux points, comme suit :

```
profname:res1:res2:desc:attr
```

Les champs ont les significations suivantes :

`profname` Nom du profil de droits. Les noms des profils de droits sont sensibles à la casse. Ce nom est également utilisé par la base de données `user_attr` pour indiquer les profils attribués à des rôles et à des utilisateurs.

`res1:res2` Réservé à une utilisation ultérieure.

`desc` Description longue. Ce champ doit expliquer l'objectif du profil de droits, y compris le type d'utilisateur susceptible d'être intéressé par l'utilisation du profil. La description longue doit être adaptée pour son affichage dans le texte de l'aide d'une application.

`attr` Une liste optionnelle de paires clé-valeur séparées par des points-virgules (;) qui décrit les attributs de sécurité à appliquer à l'objet lors de l'exécution. Zéro ou plusieurs clés peuvent être spécifiées. Les clés correctes sont `help`. `profiles` et `auths`.

Le mot-clé `help` identifie un fichier d'aide au format HTML. Les fichiers d'aide sont accessibles à partir du fichier `index.html` dans le répertoire `/usr/lib/help/profiles/locale/C`.

Le mot-clé `profiles` spécifie une liste de profils de droits séparés par des virgules. Ces profils sont appelés des *profils de droits supplémentaires*.

Le mot-clé `auths` spécifie une liste de noms d'autorisations séparés par des virgules qui sont choisis à partir des noms définis dans la base de données `auth_attr`. Les noms d'autorisations peuvent être spécifiés avec l'astérisque (*) comme caractère générique.

Le mot-clé `privs` spécifie une liste de privilèges séparés par des virgules. Ces privilèges sont en vigueur pour toutes les commandes d'un shell de profil.

L'exemple suivant illustre deux entrées de la base de données `prof_attr` standard. Notez que le profil de droits de gestion d'imprimantes est un profil de droits supplémentaires du profil de droits Opérateur. L'exemple est renvoyé à des fins d'affichage.

```
% grep 'Printer Management' /etc/security/prof_attr
Printer Management:::                    Name of rights profile
Manage printers, daemons, spooling:      Description
help=RtPrntAdmin.html;                   Help file
auths=solaris.admin.printer.read,        Authorizations
solaris.admin.printer.modify,solaris.admin.printer.delete
...
Operator:::                              Name of rights profile
Can perform simple administrative tasks:     Description
profiles=Printer Management,             Supplementary rights profiles
Media Backup,All;
help=RtOperator.html                     Help file
```

Base de données exec_attr

La base de données exec_attr définit les commandes nécessitant des attributs de sécurité pour la réussite de l'opération. Les commandes font partie d'un profil de droits. Une commande avec ses attributs de sécurité peut être exécutée par les rôles ou utilisateurs auxquels le profil est attribué.

Les champs dans la base de données exec_attr sont séparés par deux points, comme suit :

```
name:policy:type:res1:res2:id:attr
```

Les champs ont les significations suivantes.

profname	Nom du profil de droits. Les noms des profils de droits sont sensibles à la casse. Le nom fait référence à un profil dans la base de données prof_attr.
policy	Stratégie de sécurité associée à cette entrée. Actuellement, suser et solaris sont les entrées valides. La stratégie solaris reconnaît les privilèges, contrairement à la stratégie suser.
type	Type d'entité spécifié. Actuellement, le seul le type d'entité valide est cmd (commande).
res1:res2	Réservé à une utilisation ultérieure.
ID	Chaîne qui identifie l'entité. Les commandes doivent avoir le chemin d'accès complet ou un chemin d'accès avec un caractère générique (*). Pour spécifier des arguments, écrivez un script avec les arguments et dirigez l'id vers le script.
attr	Liste optionnelle de paires clé-valeur séparées par des points-virgules (;) décrivant les attributs de sécurité à appliquer à l'entité au moment de l'exécution. Zéro ou plusieurs clés peuvent être spécifiées. La liste de mots-clés corrects dépend de la stratégie mise en application. Pour la stratégie suser, les quatre clés correctes sont euid, uid, egid et gid.

- Les mots-clés `euid` et `uid` contiennent un seul nom d'utilisateur ou un ID utilisateur numérique (UID). Les commandes qui sont désignées par `euid` s'exécutent avec l'UID fourni, qui est similaire à la définition du bit `setuid` sur un fichier exécutable. Les commandes qui sont désignées avec `uid` s'exécutent à la fois avec l'UID réel et l'UID effectif.
- Les mots-clés `egid` et `gid` contiennent un seul nom de groupe ou ID de groupe numérique (GID). Les commandes désignées par `egid` s'exécutent avec l'UID fourni, qui est similaire à la définition du bit `setgid` sur un fichier exécutable. Les commandes désignées avec `gid` s'exécutent à la fois avec le GID réel et le GID effectif.

Pour la stratégie `solaris`, le mot-clé valide est `privs`. La valeur est constituée d'une liste de privilèges séparés par des virgules.

L'exemple suivant présente quelques valeurs typiques d'une base de données `exec_attr` :

```
% grep 'File System Management' /etc/security/exec_attr
File System Management:suser:cmd:::/usr/sbin/ff:euid=0
File System Management:solaris:cmd:::/usr/sbin/mount:privs=sys_mount
...
```

Fichier `policy.conf`

Le fichier `policy.conf` fournit un moyen d'accorder des profils de droits, des autorisations et des privilèges spécifiques à tous les utilisateurs. Les entrées correspondantes dans le fichier sont constitués de paires *key=value* :

- `AUTHS_GRANTED=`*authorizations* : fait référence à une ou plusieurs autorisations.
- `PROFS_GRANTED=`*rights profiles* : fait référence à un ou plusieurs profils de droits.
- `PRIV_DEFAULT=`*privileges* : fait référence à un ou plusieurs privilèges.
- `PRIV_LIMIT=`*privileges* : fait référence à tous les privilèges.

L'exemple suivant illustre certaines valeurs typiques issues de la base de données `policy.conf` :

```
# grep AUTHS /etc/security/policy
AUTHS_GRANTED=solaris.device.cdrw

# grep PROFS /etc/security/policy
PROFS_GRANTED=Basic Solaris User

# grep PRIV /etc/security/policy

#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section “Privilèges (présentation)” à la page 197.

Commandes RBAC

Cette section répertorie les commandes utilisées pour administrer RBAC. Elle fournit également un tableau des commandes dont l'accès peut être contrôlé par des autorisations.

Commandes pour la gestion de RBAC

Même si vous pouvez modifier les bases de données RBAC locales manuellement, ce type de modification est fortement déconseillé. Les commandes suivantes sont disponibles pour la gestion de l'accès aux tâches avec RBAC.

TABLEAU 10–7 Commandes d'administration RBAC

Page de manuel pour les commandes	Description
`auths`(1)	Affiche les autorisations d'un utilisateur.
`makedbm`(1M)	Crée un fichier `dbm`.
`nscd`(1M)	Name Service Cache Daemon (démon cache de service de noms), utile pour la mise en mémoire cache des bases de données `user_attr`, `prof_attr` et `exec_attr`. Utilisez la commande `svcadm` pour redémarrer le démon.
`pam_roles`(5)	Module de gestion des comptes pour les rôles de PAM. Vérifie la présence de l'autorisation pour endosser un rôle.
`pfexec`(1)	Utilisé par des shells de profil pour exécuter des commandes avec les attributs de sécurité spécifiés dans la base de données `exec_attr`.
`policy.conf`(4)	Fichier de configuration des stratégies de sécurité du système. Répertorie les autorisations accordées, les privilèges accordés et d'autres informations de sécurité.
`profiles`(1)	Affiche les profils de droits d'un utilisateur spécifié.
`roles`(1)	Affiche les rôles qu'un utilisateur spécifique peut endosser.
`roleadd`(1M)	Ajoute un rôle à un système local.
`roledel`(1M)	Supprime un rôle d'un système local.
`rolemod`(1M)	Modifie les propriétés d'un rôle sur un système local.

TABLEAU 10–7 Commandes d'administration RBAC *(Suite)*

Page de manuel pour les commandes	Description
smattrpop(1M)	Fusionne la base de données d'attributs de sécurité source dans la base de données cible. À utiliser dans des situations où les bases de données locales doivent être fusionnées dans un service de nommage. À utiliser également dans les mises à niveau où les scripts de conversion ne sont pas fournis.
smexec(1M)	Gère les entrées dans la base de données `exec_attr`. Exige une authentification.
smmultiuser(1M)	Gère des opérations en masse sur les comptes utilisateur. Exige une authentification.
smprofile(1M)	Gère les profils de droits dans les bases de données `prof_attr` et `exec_attr`. Exige une authentification.
smrole(1M)	Gère les rôles et les utilisateurs dans les comptes de rôles. Exige une authentification.
smuser(1M)	Gère les entrées utilisateur. Exige une authentification.
useradd(1M)	Ajoute un compte utilisateur au système. L'option `-R` attribue un rôle au compte d'un utilisateur.
userdel(1M)	Supprime l'identifiant de connexion d'un utilisateur dans le système.
usermod(1M)	Modifie les propriétés du compte d'un utilisateur sur le système.

Commandes nécessitant des autorisations

Le tableau suivant fournit des exemples de la façon dont les autorisations sont utilisées pour limiter les options de commande sur un système Oracle Solaris. Pour plus d'informations sur les autorisations, reportez-vous à la section "Délégation et nommage des autorisations" à la page 246.

TABLEAU 10–8 Commandes et autorisations associées

Page de manuel pour les commandes	Autorisations requises
at(1)	`solaris.jobs.user` requise pour toutes les options (lorsque ni les fichiers `at.allow` ni les fichiers `at.deny` n'existent)
atq(1)	`solaris.jobs.admin` requise pour toutes les options
cdrw(1)	`solaris.device.cdrw` requise pour toutes les options et accordée par défaut dans le fichier `policy.conf`

TABLEAU 10–8 Commandes et autorisations associées *(Suite)*

Page de manuel pour les commandes	Autorisations requises
crontab(1)	`solaris jobs.user` requise pour l'option permettant de soumettre une tâche (lorsque ni les fichiers `crontab.allow` ni les fichiers `crontab.deny` n'existent) `solaris jobs.admin` requise pour les options permettant de répertorier ou de modifier les fichiers `crontab` d'autres utilisateurs
allocate(1)	`solaris.device.allocate` (ou toute autre autorisation spécifiée dans le fichier `device_allocate`) requise pour attribuer un périphérique `solaris.device.revoke` (ou toute autre autorisation spécifiée dans le fichier `device_allocate`) requise pour allouer un périphérique à un autre utilisateur (option `-F`)
deallocate(1)	`solaris.device.allocate` (ou toute autre autorisation spécifiée dans le fichier `device_allocate`) requise pour libérer un périphérique d'un autre utilisateur `solaris.device.revoke` (ou toute autre autorisation spécifiée dans `device_allocate`) requise pour forcer la libération du périphérique spécifié (option `-F`) ou de tous les périphériques (option `-I`)
list_devices(1)	`solaris.device.revoke` requise pour répertorier les périphériques d'un autre utilisateur (option `-U`)
sendmail(1M)	`solaris.mail` requise pour accéder aux fonctions de sous-système de messagerie ; `solaris.mail.mailq` requise pour afficher la file d'attente du courrier

◆ ◆ ◆ CHAPITRE 11

Privilèges (tâches)

Ce chapitre fournit des instructions étape par étape pour la gestion des privilèges et l'utilisation des privilèges sur votre système. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour obtenir une présentation des privilèges, reportez-vous à la section "Privilèges (présentation)" à la page 197. Pour des informations de référence, reportez-vous au Chapitre 12, "Privilèges (référence)".

Gestion et utilisation des privilèges (liste des tâches)

La liste des tâches suivante vous dirige vers les listes des tâches pour la gestion et l'utilisation des privilèges.

Tâche	Description	Voir
Utilisation de privilèges sur votre site	Comprend l'attribution, la suppression, l'ajout et le débogage de l'utilisation de privilèges.	"Gestion des privilèges (liste des tâches)" à la page 260
Utilisation de privilèges lors de l'exécution d'une commande	Comprend l'utilisation des privilèges qui vous ont été attribués.	"Détermination des privilèges (liste des tâches)" à la page 268

Gestion des privilèges (liste des tâches)

Les liste des tâches suivante vous dirige vers les procédures relatives à l'affichage des privilèges, l'attribution de privilèges et l'exécution d'un script contenant des commandes privilégiées.

Tâche	Description	Voir
Détermination des privilèges dans un processus	Dresse la liste des jeux de privilèges effectifs, héritables, autorisés et limite pour un processus.	"Détermination de privilèges sur un processus" à la page 260
Détermination des privilèges manquants dans un processus	Dresse la liste des privilèges requis par un processus ayant échoué pour s'exécuter correctement.	"Détermination des privilèges requis par un programme" à la page 262
Ajout de privilèges à une commande	Ajoute des privilèges à une commande dans un profil de droits. Le profil de droits peut être attribué à des utilisateurs ou des rôles. Les utilisateurs peuvent ensuite exécuter la commande avec les privilèges attribués dans un shell de profil.	"Ajout de privilèges à une commande" à la page 264
Attribution de privilèges à un utilisateur	Développe le jeu de privilèges héritables d'un utilisateur ou d'un rôle. Utilisez cette procédure avec discernement.	"Attribution de privilèges à un utilisateur ou à un rôle" à la page 264
Limitation des privilèges d'un utilisateur	Limite le jeu de privilèges de base d'un utilisateur. Utilisez cette procédure avec discernement.	"Limitation des privilèges d'un utilisateur ou d'un rôle" à la page 266
Exécution d'un script shell privilégié	Ajoute un privilège à un script shell et aux commandes du script shell. Exécute ensuite le script dans un shell de profil.	"Exécution d'un script shell avec des commandes privilégiées" à la page 267

Gestion des privilèges

Le moyen le plus sûr de gérer les privilèges pour les utilisateurs et les rôles est de limiter leur utilisation aux commandes comprises dans un profil de droits. Le profil de droits est ensuite inclus dans un rôle. Le rôle est attribué à un utilisateur. Lorsque l'utilisateur endosse le rôle affecté, les commandes privilégiées peuvent être exécutées dans un shell de profil. Les procédures ci-dessous décrivent l'attribution des privilèges, la suppression des privilèges et le débogage de l'utilisation de privilèges.

▼ Détermination de privilèges sur un processus

Cette procédure présente la détermination des privilèges disponibles pour vos processus. La liste n'inclut pas les privilèges attribués à des commandes particulières.

- **Dresse la liste des privilèges disponibles pour le processus de votre shell.**

  ```
  % ppriv pid
  $ ppriv -v pid
  ```

  pid Numéro du processus. Utilisez le symbole double dollar (`$$`) pour transmettre le numéro de processus du shell parent à la commande.

  `-v` Fournit une liste détaillée des noms des privilèges.

Exemple 11–1 Détermination des privilèges dans votre shell actuel

Dans l'exemple ci-dessous, les privilèges dans le processus parent du processus de shell de l'utilisateur sont répertoriés. Dans le deuxième exemple, les noms complets des privilèges sont répertoriés. Les lettres dans la sortie font référence aux jeux de privilèges suivants :

`E` Jeu de privilèges effectif.

`I` Jeu de privilèges héritable.

`P` Jeu de privilèges autorisé.

`L` Jeu de privilèges de limite.

```
% ppriv $$
1200:   -csh
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
% ppriv -v $$
1200:   -csh
flags = <none>
        E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

Exemple 11–2 Détermination des privilèges d'un rôle que vous pouvez prendre

Les rôles utilisent un shell d'administration ou un shell de profil. Vous devez endosser un rôle et utiliser son shell pour répertorier les privilèges qui lui ont été directement attribués. Dans l'exemple suivant, le rôle `sysadmin` n'a pas de privilèges attribués directement.

```
% su - sysadmin
Password:      <Type sysadmin password>
$ /usr/ucb/whoami
sysadmin
$ ppriv -v $$
1400:   pfksh
flags = <none>
```

```
E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

▼ Détermination des privilèges requis par un programme

Cette procédure détermine les privilèges nécessaires à l'exécution correcte d'une commande ou d'un processus.

Avant de commencer Cette procédure fonctionne uniquement après l'échec de la commande ou du processus.

1 Saisissez la commande ayant échoué en tant qu'argument de la commande de débogage `ppriv`.

```
% ppriv -eD touch /etc/acct/yearly
touch[11365]: missing privilege "file_dac_write"
     (euid = 130, syscall = 224) needed at ufs_direnter_cm+0x27c
touch: /etc/acct/yearly cannot create
```

2 Déterminez l'appel système défaillant en recherchant le numéro `syscall` dans le fichier `/etc/name_to_sysnum`.

```
% grep 224 /etc/name_to_sysnum
creat64                 224
```

Exemple 11–3 Utilisation de la commande `truss` pour examiner l'utilisation des privilèges

La commande `truss` peut déboguer l'utilisation des privilèges dans un shell standard. Par exemple, la commande suivante débogue le processus `touch` défaillant :

```
% truss -t creat touch /etc/acct/yearly
creat64("/etc/acct/yearly", 0666)
                      Err#13 EACCES [file_dac_write]
touch: /etc/acct/yearly cannot create
```

Les interfaces `/proc` étendues signalent les privilèges manquants après le code d'erreur dans la sortie `truss`.

Exemple 11–4 Utilisation de la commande `ppriv` pour l'examen de l'utilisation des privilèges dans un shell de profil

La commande `ppriv` peut déboguer l'utilisation des privilèges dans un shell de profil. Si vous attribuez un profil de droits à un utilisateur et que ce profil comprend des commandes avec des

privilèges, les commandes doivent être saisies dans un shell de profil. Lorsque les commandes privilégiées sont saisies dans un shell standard, les commandes ne sont pas exécutées avec les privilèges.

Dans cet exemple, l'utilisateur `jdoe` peut endosser le rôle `objadmin`. Le rôle `objadmin` comprend le profil de droits de gestion de l'accès aux objets. Ce profil de droits permet au rôle `objadmin` de modifier les autorisations pour les fichiers dont `objadmin` n'est pas propriétaire.

Dans l'exemple ci-dessous, `jdoe` ne parvient pas à changer les autorisations pour le fichier `useful.script` :

```
jdoe% ls -l useful.script
-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script
jdoe% chown objadmin useful.script
chown: useful.script: Not owner
jdoe% ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
            (euid = 130, syscall = 16) needed at ufs_setattr+0x258
chown: useful.script: Not owner
```

Lorsque `jdoe` endosse le rôle `objadmin`, les autorisations pour le fichier sont modifiées :

```
jdoe% su - objadmin
Password:      <Type objadmin password>
$ ls -l useful.script
-rw-r--r--  1 aloe  staff  2303 Apr 10 10:10 useful.script
$ chown objadmin useful.script
$ ls -l useful.script
-rw-r--r--  1 objadmin  staff  2303 Apr 10 10:10 useful.script
$ chgrp admin useful.script
$ ls -l objadmin.script
-rw-r--r--  1 objadmin  admin  2303 Apr 10 10:11 useful.script
```

Exemple 11–5 Modification d'un fichier appartenant à l'utilisateur `root`

Cet exemple illustre les protections contre l'escalade des privilèges. Pour plus de détails, reportez-vous à la section “Prévention de l'escalade de privilèges ” à la page 278. Le fichier appartient à l'utilisateur `root`. Le rôle le moins puissant, `objadmin`, a besoin de tous les privilèges pour modifier la propriété du fichier, de sorte que l'opération échoue.

```
jdoe% su - objadmin
Password:      <Type objadmin password>
$ cd /etc; ls -l system
-rw-r--r--  1 root  sys   1883 Oct 10 10:20 system
$ chown objadmin system
chown: system: Not owner
$ ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
```

```
     (euid = 101, syscall = 16) needed at ufs_setattr+0x258
chown: system: Not owner
```

▼ Ajout de privilèges à une commande

Vous ajoutez des privilèges à une commande lorsque vous ajoutez la commande à un profil de droits. Les privilèges permettent au rôle incluant le profil de droits d'exécuter la commande d'administration, sans attribuer aucune autre capacité de superutilisateur.

Avant de commencer La commande ou le programme doit être conscient des privilèges. Pour plus d'information, reportez-vous à la section "Comment les processus obtiennent des privilèges " à la page 203.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2. **Ouvrez l'interface graphique de la console de gestion Solaris.**

   Pour plus d'instructions, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226.

3. **Utilisez les outils de droits pour mettre à jour un profil approprié.**

   Sélectionnez la commande à inclure. Pour chaque commande incluse, ajoutez les privilèges requis par la commande.

Attention – Lorsque vous incluez des commandes dans un profil de droits et ajoutez des privilèges à ces commandes, les commandes s'exécutent avec ces privilèges lorsqu'elles sont exécutées dans un shell de profil.

L'ordre des profils est important. Le shell de profil exécute une commande ou une action avec les attributs de sécurité spécifiés dans le profil apparaissant en premier dans la liste des profils du compte. Par exemple, si la commande `chgrp` se trouve dans le profil de droits de gestion de l'accès aux objets avec privilèges, et si la gestion de l'accès aux objets est le premier profil dans lequel la commande `chgrp` se trouvée, la commande `chgrp` s'exécute avec les privilèges indiqués dans le profil de gestion de l'accès aux objets.

▼ Attribution de privilèges à un utilisateur ou à un rôle

Vous pouvez affecter un privilège particulier à certains utilisateurs de façon permanente. Les privilèges très spécifiques ayant une incidence sur une petite partie du système peuvent être

facilement concédés à un utilisateur. Pour obtenir plus de détails sur les implications des privilèges attribués directement, reportez-vous à la section “Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité ” à la page 196.

La procédure suivante permet à l'utilisateur `jdoe` d'utiliser des horloges haute résolution.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Ajoutez le privilège attribuant des horloges haute résolution au jeu de privilèges héritable initial de l'utilisateur.**

   ```
   $ usermod -K defaultpriv=basic,proc_clock_highres jdoe
   ```

   Les valeurs pour le mot-clé `defaultpriv` remplacent les valeurs existantes. Par conséquent, pour que l'utilisateur conserve les privilèges `basic`, la valeur `basic` doit être spécifiée. Dans la configuration par défaut, tous les utilisateurs disposent de privilèges de base.

3. **Lisez l'entrée `user_attr` obtenue.**

   ```
   $ grep jdoe /etc/user_attr
   jdoe::::type=normal;defaultpriv=basic,proc_clock_highres
   ```

Exemple 11–6 Création d'un rôle disposant des privilèges pour configurer le temps système

Dans cet exemple, le rôle créé a pour seule tâche de gérer l'heure du système.

```
$ /usr/sadm/bin/smrole -D nisplus:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
add -- -n clockmgr \
-c "Role that sets system time" \
-F "Clock Manager" \
-s /bin/pfksh \
-u 108 \
-P <Type clockmgr password> \
-K defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

La ligne `-K` est renvoyée à des fins d'affichage.

Si le rôle a été créé en local, l'entrée `user_attr` pour le rôle se présente comme suit :

```
clockmgr:::Role that sets system time:
type=role;defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

▼ Limitation des privilèges d'un utilisateur ou d'un rôle

Vous pouvez limiter les privilèges à la disposition d'un utilisateur ou d'un rôle en réduisant le jeu de base ou le jeu limite. Vous devez avoir une bonne raison de limiter les privilèges de l'utilisateur de cette manière, car ces limitations peuvent avoir des effets secondaires involontaires.

Attention – Vous devez tester de manière approfondie toutes les capacités de l'utilisateur pour lesquelles le jeu de base ou de limite a été modifié.

- Lorsque le jeu de base est plus limité que le jeu par défaut, les utilisateurs peuvent se voir empêchés d'utiliser le système.
- Lorsque le jeu limite est inférieur à tous les privilèges, les processus devant s'exécuter avec un UID effectif `UID=0` risquent d'échouer.

1 Déterminez les privilèges dans le jeu de base ou de limite d'un utilisateur.

Pour plus d'informations sur cette procédure, reportez-vous à la section "Détermination de privilèges sur un processus" à la page 260.

2 (Facultatif) Supprimez l'un des privilèges du jeu de base.

```
$ usermod -K defaultpriv=basic,!priv-name username
```

En supprimant le privilège `proc_session`, vous empêchez l'utilisateur d'examiner les processus à l'extérieur de sa session en cours. En supprimant le privilège `file_link_any`, vous empêchez l'utilisateur de créer des liens physiques vers des fichiers n'appartenant pas à l'utilisateur.

Attention – Ne supprimez pas le privilège `proc_fork` ou `proc_exec`. Sans ces privilèges, l'utilisateur n'est pas en mesure d'utiliser le système. En fait, ces deux privilèges ne doivent être supprimés que sur des démons qui ne clonent (`fork()`) ni exécutent (`exec()`) d'autres processus.

3 (Facultatif) Retirez l'un des privilèges du jeu limite.

```
$ usermod -K limitpriv=all,!priv-name username
```

4 Testez les capacités de *username*.

Connectez-vous en tant que *username* et essayez de réaliser les tâches que *username* doit exécuter sur le système.

Exemple 11–7 Suppression de privilèges du jeu limite d'un utilisateur

Dans l'exemple suivant, toutes les sessions dérivées de la connexion initiale de `jdoe` ne peuvent pas utiliser le privilège `sys_linkdir`. C'est-à-dire que l'utilisateur ne peut pas créer de liens physiques vers les répertoires, ni rompre un lien vers des répertoires et ce, même après avoir exécuté la commande `su`.

```
$ usermod -K limitpriv=all,!sys_linkdir jdoe
$ grep jdoe /etc/user_attr
jdoe::::type=normal;defaultpriv=basic;limitpriv=all,!sys_linkdir
```

Exemple 11–8 Suppression de privilèges du jeu de base d'un utilisateur

Dans l'exemple suivant, toutes les sessions qui proviennent de la connexion initiale de `jdoe` ne peuvent pas utiliser le privilège `proc_session`. C'est-à-dire que l'utilisateur ne peut pas examiner les processus à l'extérieur de sa session et ce, même après avoir exécuté la commande `su`.

```
$ usermod -K defaultpriv=basic,!proc_session jdoe

$ grep jdoe /etc/user_attr
jdoe::::type=normal;defaultpriv=basic,!proc_session;limitpriv=all
```

▼ Exécution d'un script shell avec des commandes privilégiées

Remarque – Lorsque vous créez un script shell exécutant des commandes avec des privilèges hérités, le profil de droits approprié doit contenir les commandes avec les privilèges qui leur sont attribués.

1. **Commencez le script avec `/bin/pfsh`, ou tout autre shell de profil, sur la première ligne.**

   ```
   #!/bin/pfsh
   # Copyright (c) 2009, 2011 by Oracle Corporation
   ```

2. **Déterminez les privilèges requis pas les commandes du script.**

   ```
   % ppriv -eD script-full-path
   ```

3. **Ouvrez l'interface graphique de la console de gestion Solaris.**

   Pour plus d'instructions, reportez-vous à la section "Procédure d'endossement d'un rôle dans la console de gestion Solaris" à la page 226. Choisissez un rôle, l'administrateur principal par exemple, qui peut créer un profil de droits.

4 **Utilisez les outils de droits pour créer un profil approprié.**

Sélectionnez le script et incluez dans le profil de droits chacune des commandes du script shell dont l'exécution nécessite des privilèges. Pour chaque commande incluse, ajoutez les privilèges requis par la commande.

Attention – L'ordre des profils de droits est important. Le shell de profil exécute la première instance d'une commande dans la liste des profils. Par exemple, si la commande `chgrp` se trouve dans le profil de droits de gestion de l'accès aux objets, et si la gestion de l'accès aux objets est le premier profil dans lequel la commande `chgrp` se trouve, la commande `chgrp` s'exécute avec les privilèges indiqués dans le profil de gestion de l'accès aux objets.

5 **Ajoutez le profil de droits à un rôle et attribuez le rôle à un utilisateur.**

Pour exécuter le profil, l'utilisateur endosse le rôle et exécute le script dans le shell de profil du rôle.

Détermination des privilèges (liste des tâches)

La liste des tâches suivante vous dirige vers les procédures liées à l'utilisation des privilèges qui vous ont été attribués.

Tâche	Description	Voir
Affichage de vos privilèges en tant qu'utilisateur dans n'importe quel shell	Affiche les privilèges qui vous ont été directement attribués. Tous les processus s'exécutent avec ces privilèges.	"Détermination des privilèges qui vous sont attribués directement" à la page 269
Détermination des commandes que vous pouvez exécuter avec un privilège	Lorsque des privilèges sont attribués aux exécutables dans un profil de droits, l'exécutable doit être saisi dans un shell de profil.	"Détermination des commandes privilégiées que vous pouvez exécuter" à la page 270
Détermination des commandes qu'un rôle peut exécuter avec des privilèges	Endosse le rôle pour déterminer les commandes qu'il peut exécuter avec des privilèges.	"Détermination des commandes privilégiées qu'un rôle peut exécuter" à la page 271

Détermination des privilèges qui vous sont attribués

Lorsqu'un utilisateur se voit affecter directement des privilèges, ces derniers sont appliqués dans chaque shell. Lorsque les privilèges ne lui sont pas directement attribués, l'utilisateur doit ouvrir un shell de profil. Par exemple, lorsque les commandes ayant des privilèges attribués se trouvent dans un profil de droits répertorié dans la liste de profils de droits de l'utilisateur, l'utilisateur doit exécuter la commande dans un shell de profil.

▼ Détermination des privilèges qui vous sont attribués directement

La procédure suivante montre comment déterminer si des privilèges vous ont été directement attribués.

Attention – L'utilisation inappropriée de privilèges attribués directement peut entraîner des violations involontaires de sécurité. Pour plus de détails, reportez-vous à la section "Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité " à la page 196.

1. **Répertoriez les privilèges pouvant être utilisés par vos processus.**

   Reportez-vous à la section "Détermination de privilèges sur un processus" à la page 260 pour connaître la procédure.

2. **Appelez des actions et exécutez des commandes dans un shell.**

   Les privilèges répertoriés dans le jeu effectif sont en vigueur dans l'ensemble de votre session. Si des privilèges vous ont été directement attribués en plus du jeu de base, ceux-ci sont répertoriés dans le jeu effectif.

Exemple 11–9 Détermination des privilèges qui vous sont attribués directement

Si des privilèges vous ont été attribués directement, votre jeu de base contient plus que le jeu de base par défaut. Dans cet exemple, l'utilisateur a toujours accès au privilège `proc_clock_highres`.

```
% /usr/ucb/whoami
jdoe
% ppriv -v $$
1800:   pfksh
flags = <none>
        E: file_link_any,...,proc_clock_highres,proc_session
        I: file_link_any,...,proc_clock_highres,proc_session
        P: file_link_any,...,proc_clock_highres,proc_session
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
% ppriv -vl proc_clock_highres
        Allows a process to use high resolution timers.
```

Exemple 11–10 Détermination des privilèges directement attribués à un rôle

Les rôles utilisent un shell d'administration ou un shell de profil. Les utilisateurs endossant un rôle peuvent utiliser son shell pour répertorier les privilèges qui lui ont été directement attribués. Dans l'exemple suivant, des privilèges ont été directement attribués au rôle `realtime` pour gérer les programmes de date et d'heure.

```
% su - realtime
Password:      <Type realtime password>
$ /usr/ucb/whoami
realtime
$ ppriv -v $$
1600:   pfksh
flags = <none>
        E: file_link_any,...,proc_clock_highres,proc_session,sys_time
        I: file_link_any,...,proc_clock_highres,proc_session,sys_time
        P: file_link_any,...,proc_clock_highres,proc_session,sys_time
        L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

▼ Détermination des commandes privilégiées que vous pouvez exécuter

Lorsque les privilèges ne sont pas attribués directement à un utilisateur, celui-ci a accès aux commandes privilégiées par l'intermédiaire d'un profil de droits. Les commandes d'un profil de droits doivent être exécutées dans un shell de profil.

Avant de commencer L'utilisateur ou le rôle s'authentifiant sur la console de gestion Solaris doit disposer de l'autorisation `solaris.admin.usermgr.read`. Le profil de droits de l'utilisateur Solaris de base inclut cette autorisation.

1 Déterminez les profils de droits qui vous ont été attribués.

```
$ /usr/sadm/bin/smuser list -- -n username -l

Authenticating as user: admin
... Please enter a string value for: password ::
...
User name:      username
User ID (UID):  130
Primary group:  staff
Secondary groups:
Comment: object mgt jobs
Login Shell: /bin/sh
Home dir server: system
Home directory: /export/home/username
AutoHome setup: True
Mail server: system
Rights: Object Access Management
Assigned Roles:
```

2 Recherchez la ligne commençant par "Rights".

Cette ligne répertorie les noms des profils de droits qui vous ont été attribués directement.

3 Recherchez les noms des profils de droits dans la base de données `exec_attr`.

```
$ cd /etc/security
$ grep "Object Access Management" exec_attr
Object Access Management:solaris:cmd:::/usr/bin/chgrp:privs=file_chown
Object Access Management:solaris:cmd:::/usr/bin/chown:privs=file_chown
Object Access Management:suser:cmd:::/usr/bin/chgrp:euid=0
Object Access Management:suser:cmd:::/usr/bin/chmod:euid=0
...
```

Les commandes ayant des privilèges ajoutés sont répertoriées à la fin des entrées de stratégie `solaris`.

4 Saisissez les commandes qui requièrent des privilèges dans un shell de profil.

Lorsque les commandes sont saisies dans un shell standard, elles s'exécutent sans privilège et échouent.

```
% pfsh
$
```

Exemple 11–11 Exécution de commandes privilégiées dans un shell de profil

Dans l'exemple suivant, l'utilisateur `jdoe` ne peut pas modifier les autorisations du groupe sur un fichier issu de son shell standard. Cependant, `jdoe` peut changer les autorisations lors de la saisie de la commande dans un shell de profil.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 nodoe eng 262 Apr 2 10:52 useful.script
chgrp staff useful.script
chgrp: useful.script: Not owner
% pfksh
$ /usr/ucb/whoami
jdoe
$ chgrp staff useful.script
$ chown jdoe useful.script
$ ls -l useful.script
-rwxr-xr-- 1 jdoe staff 262 Apr 2 10:53 useful.script
```

▼ Détermination des commandes privilégiées qu'un rôle peut exécuter

Un rôle obtient l'accès aux commandes privilégiées par l'intermédiaire d'un profil de droits contenant des commandes dotées de privilèges attribués. Le moyen le plus sûr pour qu'un utilisateur puisse accéder aux commandes privilégiées est de lui attribuer un rôle. Une fois le rôle endossé, l'utilisateur peut exécuter toutes les commandes privilégiées incluses dans les profils de droits pour ce rôle.

Avant de commencer L'utilisateur ou le rôle s'authentifiant sur la console de gestion Solaris doit disposer de l'autorisation `solaris.admin.usermgr.read`. Le profil de droits de l'utilisateur Solaris de base inclut cette autorisation.

1 Déterminez les rôles que vous pouvez endosser.

```
$ /usr/sadm/bin/smuser list -- -n username -l
Authenticating as user: primadmin
...
User name:      username
User ID (UID):  110
Primary group:  staff
Secondary groups:
Comment: Has admin roles
Login Shell: /bin/sh
...
Rights:
Assigned Roles: primadmin, admin
```

2 Recherchez la ligne commençant par "Assigned Roles".

Cette ligne répertorie les rôles que vous pouvez endosser.

3 Déterminez les profils de droits inclus dans l'un de vos rôles.

```
% su - devadmin
Enter password:      Type devadmin password
$ whoami
devadmin
$ profiles
Device Security


$ /usr/sadm/bin/smuser list -- -n admin -l
Authenticating as user: primadmin
...
User name:      admin
User ID (UID):  101
Primary group:  sysadmin
Secondary groups:
Comment: system administrator
Login Shell: /bin/pfksh
...
Rights: System Administrator
Assigned Roles:
```

4 Recherchez les noms des profils de droits pour le rôle à la ligne "Rights".

5 Recherchez les profils de droit dans la base de données `prof_attr`.

Étant donné que le profil de l'administrateur système se compose d'un ensemble de profils, vous devez répertorier ces profils dans le profil d'administrateur système.

```
$ cd /etc/security
$ grep "System Administrator" prof_attr
System Administrator:::Can perform most non-security administrative
```

```
tasks:profiles=Audit Review,Printer Management,Cron Management,
Device Management,File System Management,Mail Management,Maintenance
and Repair,Media Backup,Media Restore,Name Service Management,Network
Management,Object Access Management,Process Management,Software
Installation,User Management,All;help=RtSysAdmin.html
```

6 Recherchez chaque profil de droits dans la base de données `exec_attr`.

Par exemple, le profil de gestion du réseau est un profil supplémentaire du profil d'administrateur système. Le profil de gestion du réseau inclut un certain nombre de commandes privilégiées.

```
$ cd /etc/security
$ grep "Network Management" exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
Network Management:solaris:cmd:::/usr/sbin/route:privs=sys_net_config
...
```

Les commandes et leurs privilèges attribués sont les deux derniers champs des entrées de stratégie `solaris`. Vous pouvez exécuter ces commandes dans le shell de profil de votre rôle.

Exemple 11–12 Exécution de commandes privilégiées dans votre rôle

Lorsqu'un utilisateur endosse un rôle, le shell devient un shell de profil. Par conséquent, les commandes sont exécutées avec les privilèges qui leur ont été attribués. Dans l'exemple suivant, le rôle `admin` peut modifier les autorisations pour le fichier `useful.script`.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script
chgrp admin useful.script
chgrp: useful.script: Not owner
% su - admin
Password:      <Type admin password>
$ /usr/ucb/whoami
admin
$ chgrp admin useful.script
$ chown admin useful.script
$ ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script
```

◆ ◆ ◆ CHAPITRE 12

Privilèges (référence)

Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre :

Pour utiliser les privilèges, reportez-vous au Chapitre 11, “Privilèges (tâches)”. Pour obtenir des informations sur la présentation, reportez-vous à la section “Privilèges (présentation)” à la page 197.

Commandes d'administration pour la gestion des privilèges

Le tableau suivant répertorie les commandes disponibles pour gérer les privilèges.

TABLEAU 12–1 Commandes pour la gestion des privilèges

Objectif	Commande	Page de manuel
Examiner les privilèges de processus	`ppriv -v` *pid*	`ppriv(1)`
Définir les privilèges de processus	`ppriv -s` *spec*	
Dresser la liste des privilèges du système	`ppriv -l`	
Répertorier un privilège et sa description	`ppriv -lv` *priv*	
Déboguer les échecs liés aux privilèges	`ppriv -eD` *failed-operation*	
Attribuer des privilèges à un nouvel utilisateur local	`useradd`	`useradd(1M)`

TABLEAU 12–1 Commandes pour la gestion des privilèges *(Suite)*

Objectif	Commande	Page de manuel
Ajouter des privilèges à un utilisateur local existant	`usermod`	`usermod`(1M)
Attribuer des privilèges à un utilisateur dans un service de nommage	`smuser`	`smuser`(1M)
Attribuer des privilèges à un nouveau rôle local	`roleadd`	`roleadd`(1M)
Ajouter des privilèges à un rôle local existant	`rolemod`	`rolemod`(1M)
Attribuer des privilèges à un rôle dans un service de nommage	`smrole`	`smrole`(1M)
Afficher la stratégie de périphériques	`getdevpolicy`	`getdevpolicy`(1M)
Définir la stratégie de périphériques	`devfsadm`	`devfsadm`(1M)
Mettre à jour la stratégie relative aux périphériques ouverts	`update_drv -p` *policy driver*	`update_drv`(1M)
Ajouter la stratégie de périphériques pour un périphérique	`add_drv -p` *policy driver*	`add_drv`(1M)

L'interface graphique de la console de gestion Solaris est l'outil préféré pour attribuer des privilèges à des commandes, des utilisateurs et des rôles. Pour plus d'informations, reportez-vous à la section “Procédure d'endossement d'un rôle dans la console de gestion Solaris” à la page 226.

Fichiers disposant d'informations sur les privilèges

Les fichiers suivants contiennent des informations relatives aux privilèges.

TABLEAU 12–2 Fichiers contenant des informations sur les privilèges

Fichier et page de manuel	Mot-clé	Description
`/etc/security/policy.conf` `policy.conf`(4)	`PRIV_DEFAULT`	Jeu de privilèges héritable pour le système
	`PRIV_LIMIT`	Jeu de privilèges de limite pour le système

TABLEAU 12–2 Fichiers contenant des informations sur les privilèges *(Suite)*

Fichier et page de manuel	Mot-clé	Description
`/etc/user_attr` `user_attr(4)`	Mot-clé `privs` dans l'entrée utilisateur ou rôle Mot-clé `defaultpriv` dans l'entrée utilisateur ou rôle La valeur est généralement définie dans l'interface graphique de la console de gestion Solaris	Jeu de privilèges héritable pour un utilisateur ou un rôle
	Mot-clé `limitpriv` dans l'entrée utilisateur ou rôle La valeur est généralement définie dans l'interface graphique de la console de gestion Solaris	Jeu de privilèges de limite pour un utilisateur ou un rôle
`/etc/security/exec_attr` `exec_attr(4)`	Mot-clé `privs` dans l'entrée du profil pour la commande La stratégie pour la commande doit être `solaris`	Liste des privilèges qui sont attribués à une commande dans un profil de droits
`syslog.conf` `syslog.conf(4)`	Fichier journal du système pour les messages de débogage Chemin défini dans l'entrée `priv.debug`	Journal de débogage des privilèges

Remarque – Ne modifiez pas les bases de données `exec_attr` et `user_attr` directement. Pour administrer les privilèges, utilisez la console de gestion Solaris ou des commandes telles que `smuser`. Pour plus d'informations, reportez-vous aux pages de manuel `smc(1M)` et `smuser(1M)` Pour plus d'informations sur les procédures, reportez-vous à la section "Gestion des privilèges (liste des tâches)" à la page 260.

Privilèges et audit

L'utilisation des privilèges peut être auditée. À chaque fois qu'un processus utilise un privilège, l'utilisation du privilège est enregistrée dans la piste d'audit du jeton d'audit `upriv`. Lorsque les noms de privilèges font partie de l'enregistrement, leur représentation textuelle est utilisée. Les événements d'audit suivants enregistrent l'utilisation de privilèges :

- `AUE_SETPPRIV` **(événement d'audit) :** l'événement génère un enregistrement d'audit lorsqu'un jeu de privilèges est modifié. L'événement d'audit `AUE_SETPPRIV` se trouve dans la classe `pm`.
- `AUE_MODALLOCPRIV` **(événement d'audit) :** l'événement d'audit génère un enregistrement d'audit lorsqu'un privilège est ajouté depuis l'extérieur du noyau. L'événement d'audit `AUE_MODALLOCPRIV` se trouve dans la classe `ad`.
- `AUE_MODDEVPLCY` **(événement d'audit) :** l'événement d'audit génère un enregistrement d'audit lorsque la stratégie liée au périphérique est modifiée. L'événement d'audit `AUE_MODDEVPLCY` se trouve dans la classe `ad`.

- `AUE_prof_cmd` **(événement d'audit) :** l'événement d'audit génère un enregistrement d'audit lorsqu'une commande est exécutée dans un shell de profil. L'événement d'audit `AUE_prof_cmd` se trouve dans les classes d'audit `as` et `ua`. Les noms des privilèges sont inclus dans l'enregistrement d'audit.

L'utilisation réussie de privilèges inclus dans le jeu de base n'est pas auditée. La tentative d'utilisation d'un privilège de base qui a été supprimé du jeu de base d'un utilisateur fait l'objet d'un audit.

Prévention de l'escalade de privilèges

Le noyau Oracle Solaris empêche l'*escalade de privilèges*. Une escalade de privilèges se produit lorsqu'un privilège permet à un processus de faire plus que ce à quoi il est autorisé. Pour empêcher qu'un processus acquière plus de privilèges que ceux qui lui sont accordés normalement, les modifications de système vulnérable exigent le jeu complet de privilèges. Par exemple, un fichier ou un processus détenu par `root` (`UID=0`) ne peut être modifié que par un processus ayant le jeu complet de privilèges. Le compte `root` n'a pas besoin de privilèges pour modifier un fichier appartenant à `root`. Toutefois, un utilisateur non root doit avoir tous les privilèges pour modifier un fichier appartenant à `root`.

De même, les opérations permettant d'accéder aux périphériques requièrent tous les privilèges du jeu effectif.

Les privilèges `file_chown_self` et `proc_owner` sont soumis à l'escalade de privilèges. Le privilège `file_chown_self` permet à un processus d'abandonner ses fichiers. Le privilège `proc_owner` permet à un processus d'examiner des processus dont il n'est pas propriétaire.

Le privilège `file_chown_self` est limité par la variable système `rstchown`. Lorsque la variable `rstchown` est définie sur zéro, le privilège `file_chown_self` est supprimé du jeu héritable initial du système et de tous les utilisateurs. Pour plus d'informations sur la variable système `rstchown`, reportez-vous à la page de manuel `chown(1)`.

Le privilège `file_chown_self` est attribué, pour des raisons de sécurité, à une commande particulière, placée dans un profil et affectée à un rôle pour l'utiliser dans un shell de profil.

Le privilège `proc_owner` n'est pas suffisant pour définir un processus UID sur `0`. Basculer d'un processus de n'importe quel UID à `UID=0` exige tous les privilèges. Étant donné que le privilège `proc_owner` donne un accès illimité en lecture à tous les fichiers sur le système, le privilège est attribué, pour des raisons de sécurité, à une commande particulière, placée dans un profil et affectée à un rôle pour l'utiliser dans un shell de profil.

Attention – Le compte d'un utilisateur peut être modifié afin d'inclure le privilège `file_chown_self` ou `proc_owner` dans le jeu héritable initial de l'utilisateur. Vous devez avoir des raisons de sécurité de poids pour placer ces privilèges puissants dans le jeu de privilèges héritable pour n'importe quel utilisateur, rôle ou système.

Pour plus de détails sur la manière d'empêcher l'escalade de privilèges pour des périphériques, reportez-vous à la section “Privilèges et périphériques ” à la page 205.

Anciennes applications et modèle de privilège

Pour s'adapter aux anciennes applications, l'implémentation de privilèges fonctionne à la fois avec le superutilisateur et les modèles de privilège. Le noyau suit automatiquement l'indicateur `PRIV_AWARE`, qui indique qu'un programme a été conçu pour fonctionner avec des privilèges. Prenons un processus fils qui n'est pas conscient des privilèges. Les privilèges hérités du processus parent sont disponibles dans les jeux effectif et autorisé de l'enfant. Si le processus fils définit un UID sur 0, le processus fils n'a peut-être pas toutes les capacités de superutilisateur. Les jeux effectif et autorisé du processus sont limités aux privilèges dans le jeu limite de l'enfant. Par conséquent, le jeu limite d'un processus conscient des privilèges restreint les privilèges root des processus fils qui ne sont pas conscients des privilèges.

PARTIE IV

Services cryptographiques

Cette section décrit les services centralisés de cryptographie et de technologie à clé publique fournis par SE Oracle Solaris.

◆ ◆ ◆ CHAPITRE 13

Structure cryptographique Oracle Solaris (présentation)

Ce chapitre décrit la structure cryptographique Oracle Solaris. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour administrer et utiliser la structure cryptographique Oracle Solaris, reportez-vous au Chapitre 14, "Structure cryptographique Oracle Solaris (tâches)".

Nouveautés de la structure cryptographique Oracle Solaris

Solaris 10 1/06 : la bibliothèque de structures, `libpkcs11.so`, contient un nouveau composant, le *metaslot*. Le metaslot sert de connecteur virtuel unique avec les possibilités combinées de tous les jetons et connecteurs installés sur la structure. Concrètement, le metaslot permet à une application de se connecter à tout service cryptographique disponible via un seul connecteur, et ce de manière totalement transparente.

- Pour plus d'informations, reportez-vous aux définitions de connecteur, metaslot et jeton à la section "Terminologie utilisée dans la structure cryptographique Oracle Solaris" à la page 285.
- Pour administrer le metaslot, reportez-vous à la page de manuel `cryptoadm(1M)`.

- Vous trouverez une liste complète des nouvelles fonctionnalités d'Oracle Solaris et la description des différentes versions de cette application dans le document *Nouveautés apportées à Oracle Solaris 10 8/11*.

Structure cryptographique Oracle Solaris

La structure cryptographique Oracle Solaris fournit un magasin d'algorithmes et de bibliothèques PKCS #11 commun pour traiter les exigences en matière de cryptographie. Les bibliothèques PKCS #11 sont implémentées conformément au standard suivant : Cryptoki (Cryptographic Token Interface, interface de jetons cryptographiques) pour la bibliothèque PKCS #11 de RSA Security Inc.

Au niveau du noyau, la structure gère actuellement les exigences en matière de cryptographie pour Kerberos et IPsec. Les consommateurs au niveau utilisateur incluent `libsasl` et IKE.

La loi sur les exportations aux États-Unis exige que l'utilisation des interfaces cryptographiques ouvertes soit restreinte. La structure cryptographique Oracle Solaris est conforme à la loi en vigueur en exigeant que les fournisseurs cryptographiques du noyau et PKCS 11 s'identifient. Pour plus d'informations, reportez-vous à la section "Signatures binaires pour les logiciels tiers" à la page 288.

La structure permet aux *fournisseurs* de services cryptographiques de voir leurs services utilisés par de nombreux *consommateurs* dans le SE Oracle Solaris. Les fournisseurs sont également appelés des *plug-ins*. La structure autorise trois types de plug-ins :

- **Plug-ins au niveau de l'utilisateur :** objets partagés qui fournissent des services en utilisant les bibliothèques PKCS #11, telles que `pkcs11_softtoken.so.1`.
- **Plug-ins au niveau du noyau :** modules de noyau qui fournissent l'implémentation d'algorithmes cryptographiques dans les logiciels, tels que AES.

  De nombreux algorithmes de la structure sont optimisés pour les architectures x86 avec le jeu d'instructions SSE2 et pour le matériel SPARC.
- **Plug-in matériel :** pilotes de périphériques et leurs accélérateurs matériels associés. Les puces Niagara, les pilotes de périphériques NCP et N2CP, en sont des exemples. Un accélérateur matériel décharge le système d'exploitation de fonctions cryptographiques coûteuses. La carte Sun Crypto Accelerator 6000 en est un exemple.

La structure implémente une interface standard, la bibliothèque PKCS #11, v2.11, pour les fournisseurs au niveau de l'utilisateur. La bibliothèque peut être utilisée par des applications tierces pour atteindre les fournisseurs. Des tiers peuvent également ajouter à la structure des bibliothèques signées, des modules d'algorithme de noyau signés et des pilotes de périphériques signés. Ces plug-ins sont ajoutés lorsque l'utilitaire `pkgadd` installe le logiciel tiers. Pour visualiser un diagramme des principaux composants de la structure, reportez-vous au Chapitre 8, "Introduction to the Oracle Solaris Cryptographic Framework" du *Developer's Guide to Oracle Solaris Security*.

Terminologie utilisée dans la structure cryptographique Oracle Solaris

La liste suivante de définitions et d'exemples est utile lorsque vous utilisez la structure cryptographique.

- **Algorithmes :** algorithmes cryptographiques. Il s'agit de procédures de calcul récursives établies qui chiffrent ou hachent une entrée. Les algorithmes de chiffrement peuvent être symétriques ou asymétriques. Les algorithmes symétriques utilisent la même clé pour le chiffrement et le déchiffrement. Les algorithmes asymétriques, qui sont utilisés dans le cryptographie par clé publique, nécessitent deux clés. Les fonctions de hachage sont également des algorithmes.

  Quelques exemples d'algorithmes :

  - Algorithmes symétriques, comme AES et ARCFOUR
  - Algorithmes asymétriques, comme Diffie-Hellman et RSA
  - Fonctions de hachage, comme MD5

- **Consommateurs :** utilisateurs des services cryptographiques provenant de fournisseurs. Les consommateurs peuvent être des applications, des utilisateurs finaux ou des opérations de noyau.

  Quelques exemples de consommateurs :

  - Applications, comme IKE
  - Utilisateurs finaux, comme un utilisateur standard exécutant la commande `encrypt`
  - Opérations de noyau, comme IPsec

- **Mécanisme :** application d'un mode d'algorithme pour un objectif 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.

- **Metaslot :** connecteur réunissant les capacités d'autres connecteurs chargés dans la structure. Le metaslot facilite le travail de gestion de toutes les capacités des fournisseurs disponibles par le biais de la structure. Lorsqu'une application utilisant le metaslot demande une opération, le metaslot détermine quel connecteur réel doit effectuer l'opération. Les capacités du metaslot sont configurables, mais la configuration n'est pas nécessaire. Le metaslot est activé par défaut. Pour configurer le metaslot, reportez-vous à la page de manuel `cryptoadm(1M)`.

- **Mode :** version d'un algorithme cryptographique. Par exemple, CBC (Cipher block Chaining, enchaînement des blocs de chiffrement) est un autre mode d'ECB (Electronic Code Book, bloc de contrôle d'événement). L'algorithme AES possède deux modes, CKM_AES_ECB et CKM_AES_CBC.

- **Stratégie :** choix effectué par un administrateur de rendre des mécanismes disponibles pour l'utilisation. Par défaut, tous les fournisseurs et tous les mécanismes sont disponibles pour l'utilisation. La désactivation de tout mécanisme serait une application de la stratégie. L'activation d'un mécanisme désactivé serait également une application de la stratégie.
- **Fournisseurs :** services cryptographiques utilisés par les consommateurs. Étant donné que les fournisseurs se connectent à la structure, ils sont également qualifiés de *plug-ins*.

  Quelques exemples de fournisseurs :

  - Bibliothèques PKCS 11, comme `pkcs11_softtoken.so`
  - Modules d'algorithmes cryptographiques, comme `aes` et `arcfour`
  - Pilotes de périphériques et leurs accélérateurs matériels associés, comme le pilote `mca` pour la carte Sun Crypto Accelerator 6000
- **Connecteur :** interface vers un ou plusieurs périphériques cryptographiques. Chaque emplacement, qui correspond à un lecteur physique ou à une autre interface de périphérique, peut contenir un jeton. Un jeton fournit une vue logique d'un périphérique cryptographique dans la structure.
- **Jeton :** dans un connecteur, un jeton fournit une vue logique d'un périphérique cryptographique dans la structure.

Champ d'application de la structure cryptographique Oracle Solaris

La structure offre des commandes aux administrateurs, utilisateurs et développeurs qui approvisionnent les fournisseurs :

- **Commandes d'administration :** la commande `cryptoadm` fournit une sous-commande `list` pour répertorier les fournisseurs disponibles et leurs capacités. Les utilisateurs standard peuvent exécuter les commandes `cryptoadm list` et `cryptoadm --help`.

  Toutes les autres sous-commandes `cryptoadm` exigent que vous endossiez un rôle incluant le profil de droits de gestion de la cryptographie ou que vous vous connectiez en tant que superutilisateur. Les sous-commandes telles que `disable`, `install` et `uninstall` sont disponibles pour l'administration de la structure. Pour plus d'informations, reportez-vous à la page de manuel `cryptoadm`(1M).

  La commande `svcadm` est utilisée pour gérer le démon `kcfd` et actualiser la stratégie cryptographique dans le noyau. Pour plus d'informations, reportez-vous à la page de manuel `svcadm`(1M).
- **Commandes au niveau de l'utilisateur :** les commandes `digest` et `mac` fournissent des services d'intégrité des fichiers. Les commandes `encrypt` et `decrypt` protègent les fichiers des risques d'écoute informatique. Pour utiliser ces commandes, reportez-vous à la section "Protection de fichiers avec la structure cryptographique Oracle Solaris (liste des tâches)" à la page 292.

- **Signatures binaires pour des fournisseurs tiers :** la commande `elfsign` permet à des tiers de signer des binaires au sein de la structure. Les binaires qui peuvent être ajoutés à la structure sont des bibliothèques PKCS #11, des modules d'algorithme de noyau et des pilotes de périphériques matériels. Pour utiliser la commande `elfsign` , reportez-vous à l'Annexe F, "Packaging and Signing Cryptographic Providers" du *Developer's Guide to Oracle Solaris Security*.

Commandes d'administration dans la structure cryptographique Oracle Solaris

La commande `cryptoadm` administre une structure cryptographique en cours d'exécution. La commande fait partie du profil de droits de gestion de la cryptographie. Ce profil peut être attribué à un rôle pour l'administration sécurisée de la structure cryptographique. La commande `cryptoadm` gère ce qui suit :

- Affichage des informations du fournisseur cryptographique
- Désactivation ou activation de mécanismes du fournisseur
- Solaris 10 1/06 : désactivation ou activation du metaslot

La commande `svcadm` est utilisée pour activer, actualiser et désactiver le démon des services cryptographiques, `kcfd`. Cette commande fait partie de l'utilitaire de gestion des services (SMF). `svc:/system/cryptosvcs` est l'instance de service pour la structure cryptographique. Pour plus d'informations, reportez-vous aux pages de manuel `smf(5)` et `svcadm(1M)`.

Commandes au niveau de l'utilisateur dans la structure cryptographique Oracle Solaris

La structure cryptographique Oracle Solaris fournit des commandes au niveau de l'utilisateur pour vérifier l'intégrité des fichiers et les chiffrer/déchiffrer. Une commande distincte, `elfsign`, permet aux fournisseurs de signer les binaires pour les utiliser avec la structure.

- `digest` **(commande) :** calcule une synthèse de message pour un ou plusieurs fichiers ou pour stdin. Une synthèse permet de vérifier l'intégrité d'un fichier. SHA1 et MD5 sont des exemples de fonctions digest.
- `mac` **(commande) :** calcule un code d'authentification des messages (MAC) pour un ou plusieurs fichiers ou pour stdin. Un code MAC associe des données à un message authentifié. Un MAC permet à un destinataire de vérifier que le message provient de l'expéditeur et qu'il n'a pas été altéré. Les mécanismes `sha1_mac` et `md5_hmac` peuvent calculer un MAC.

- `encrypt` **(commande) :** chiffre des fichiers ou stdin avec un chiffrement symétrique. La commande `encrypt -l` répertorie les algorithmes disponibles. Les mécanismes répertoriés dans une bibliothèque au niveau de l'utilisateur sont disponibles pour la commande `encrypt`. La structure offre les mécanismes AES, DES, 3DES (triple DES) et ARCFOUR pour le chiffrement utilisateur.
- `decrypt` **(commande) :** déchiffre des fichiers ou stdin qui ont été chiffrés avec la commande `encrypt`. La commande `decrypt` utilise les mêmes clé et même mécanisme que ceux utilisés pour chiffrer le fichier d'origine.

Signatures binaires pour les logiciels tiers

La commande `elfsign` fournit un moyen de signer les fournisseurs à utiliser avec la structure cryptographique Oracle Solaris. En règle générale, cette commande est exécutée par le développeur d'un fournisseur.

La commande `elfsign` possède des sous-commandes pour demander un certificat auprès de Sun et signer des binaires. Une autre sous-commande vérifie la signature. Les binaires non signés ne peuvent pas être utilisés par la structure cryptographique Oracle Solaris. La signature d'un ou plusieurs fournisseurs requiert le certificat de Sun et la clé privée utilisée pour demander le certificat. Pour plus d'informations, reportez-vous à l'Annexe F, “Packaging and Signing Cryptographic Providers” du *Developer's Guide to Oracle Solaris Security*.

Plug-ins de la structure cryptographique Oracle Solaris

Des tiers peuvent inclure leurs fournisseurs dans la structure cryptographique Oracle Solaris. Un fournisseur tiers peut être l'un des objets suivants :

- Bibliothèque partagée PKCS #11
- Module de logiciel noyau chargeable, comme un algorithme de chiffrement, la fonction MAC ou la fonction digest
- Pilote de périphérique de noyau pour un accélérateur matériel

Les objets provenant d'un fournisseur doivent être signés avec un certificat de Sun. La demande de certificat se base sur une clé privée sélectionnée par le tiers et un certificat fourni par Sun. La demande de certificat est envoyée à Sun, qui enregistre le tiers, puis émet le certificat. Le tiers signe ensuite son objet fournisseur à l'aide du certificat de Sun.

Les modules de logiciels noyau chargeables et les pilotes de périphériques de noyau pour les accélérateurs matériels doivent également s'enregistrer dans le noyau. L'enregistrement s'effectue par l'intermédiaire de l'interface du fournisseur de services (SPI) de la structure cryptographique Oracle Solaris.

Pour installer le fournisseur, le tiers fournit un package qui installe l'objet signé et le certificat de Sun. Le package doit inclure le certificat et permettre à l'administrateur de placer ce certificat dans un répertoire sécurisé. Pour plus d'informations, reportez-vous à l'Annexe F, "Packaging and Signing Cryptographic Providers" du *Developer's Guide to Oracle Solaris Security*.

Services cryptographiques et zones

La zone globale et chaque zone non globale possèdent leur propre service `/system/cryptosvc`. Lorsque le service cryptographique est activé ou actualisé dans la zone globale, le démon `kcfd` démarre dans la zone globale, et la stratégie au niveau de l'utilisateur pour la zone globale et la stratégie du noyau pour le système sont définies. Lorsque le service est activé ou actualisé dans une zone non globale, le démon `kcfd` démarre dans la zone et la stratégie au niveau de l'utilisateur pour la zone est définie. La stratégie du noyau a été définie par la zone globale.

Pour plus d'informations sur les zones, reportez-vous à la Partie II, "Zones" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*. Pour plus d'informations sur l'utilitaire de gestion des services qui gère les applications persistantes, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base* et à la page de manuel `smf(5)`.

◆ ◆ ◆ CHAPITRE 14

Structure cryptographique Oracle Solaris (tâches)

Ce chapitre décrit l'utilisation de la structure cryptographique Oracle Solaris. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Utilisation de la structure cryptographique (liste des tâches)

La liste des tâches suivante fait référence à des tâches liées à l'utilisation de la structure cryptographique.

Tâche	Description	Voir
Protection de fichiers individuels ou de jeux de fichiers	Permet de s'assurer que le contenu du fichier n'a pas été altéré. Empêche les fichiers d'être lus par des intrus. Ces procédures peuvent être effectuées par des utilisateurs standard.	"Protection de fichiers avec la structure cryptographique Oracle Solaris (liste des tâches)" à la page 292
Administration de la structure	Ajoute, configure et supprime des fournisseurs de logiciels. Désactive et active des mécanismes du fournisseur de matériel. Ces procédures constituent des procédures d'administration.	"Administration de la structure cryptographique (liste des tâches)" à la page 303
Signature d'un fournisseur	Permet à un fournisseur d'être ajouté à la structure cryptographique Oracle Solaris. Ces procédures constituent les procédures de développeur.	Annexe F, "Packaging and Signing Cryptographic Providers" du *Developer's Guide to Oracle Solaris Security*.

Protection de fichiers avec la structure cryptographique Oracle Solaris (liste des tâches)

La structure cryptographique peut vous aider à protéger vos fichiers. La liste des tâches suivante présente les procédures permettant de dresser la liste des algorithmes disponibles et de protéger des fichiers par cryptographie.

Tâche	Description	Voir
Génération d'une clé symétrique	Génère une clé aléatoire à utiliser avec des algorithmes spécifiés par l'utilisateur.	"Génération d'une clé symétrique à l'aide de la commande `dd`" à la page 292
	Génère une clé de la longueur définie par l'utilisateur. Stocke éventuellement la clé dans un fichier, un keystore PKCS #11 ou un keystore NSS.	"Génération d'une clé symétrique à l'aide de la commande `pktool`" à la page 294
Calcul d'une somme de contrôle assurant l'intégrité d'un fichier	Vérifie que l'exemplaire d'un fichier reçu par le destinataire est identique au fichier qui a été envoyé.	"Procédure de calcul d'une synthèse d'un fichier" à la page 298
Protection d'un fichier avec un code d'authentification des messages (MAC)	Atteste au destinataire de votre message que vous en êtes l'expéditeur.	"Calcul du code MAC d'un fichier" à la page 299
Chiffrement d'un fichier, puis déchiffrement du fichier chiffré	Protège le contenu d'un fichier en chiffrant le fichier. Fournit les paramètres de chiffrement pour déchiffrer le fichier.	"Chiffrement et déchiffrement d'un fichier" à la page 300

Protection des fichiers avec la structure cryptographique (tâches)

Cette section décrit la génération des clés symétriques, la création des sommes de contrôle pour l'intégrité des fichiers et la protection des fichiers contre les risques d'écoute informatique. Les commandes de cette section peuvent être exécutées par des utilisateurs standard. Les développeurs peuvent écrire des scripts qui utilisent ces commandes.

▼ Génération d'une clé symétrique à l'aide de la commande `dd`

Une clé est nécessaire pour chiffrer les fichiers et générer le MAC d'un fichier. La clé doit provenir d'un pool de nombres aléatoires.

Si votre site possède un générateur de nombres aléatoires, utilisez-le. Vous pouvez également utiliser la commande dd avec le périphérique /dev/urandom d'Oracle Solaris en entrée. Pour plus d'informations, reportez-vous à la page de manuel dd(1M).

1 Déterminez la longueur de clé requise par votre algorithme.

a. Répertoriez les algorithmes disponibles.

```
% encrypt -l
Algorithm       Keysize:  Min   Max (bits)
----------------------------------------
aes                      128   128
arcfour                    8   128
des                       64    64
3des                     192   192

% mac -l
Algorithm       Keysize:  Min   Max (bits)
----------------------------------------
des_mac                   64    64
sha1_hmac                  8   512
md5_hmac                   8   512
sha256_hmac                8   512
sha384_hmac                8  1024
sha512_hmac                8  1024
```

b. Déterminez la longueur de clé en octets à transmettre à la commande dd.

Divisez les tailles de clé minimale et maximale par 8. Lorsque les tailles de clé minimale et maximale sont différentes, des tailles de clé intermédiaire sont possibles. Par exemple, la valeur 8, 16 ou 64 peut être transmise à la commande dd pour les fonctions sha1_hmac et md5_hmac.

2 Générez la clé symétrique.

```
% dd if=/dev/urandom of=keyfile bs=n count=n
```

if=*file*	Fichier d'entrée. Pour une clé aléatoire, utilisez le fichier /dev/urandom.
of=*keyfile*	Fichier de sortie contenant la clé générée.
bs=*n*	Taille de clé en octets. Pour obtenir la longueur en octets, divisez la longueur de clé en bits par 8.
count=*n*	Nombre de blocs d'entrée. Le nombre pour *n* doit être 1.

3 Stockez votre clé dans un répertoire protégé.

Le fichier de clés ne doit être lisible que par l'utilisateur.

```
% chmod 400 keyfile
```

Exemple 14–1 Création d'une clé pour l'algorithme AES

Dans l'exemple suivant, une clé secrète pour l'algorithme AES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes AES utilisent une clé de 128 bits. La clé est exprimée en tant que clé de 16 octets dans la commande `dd`.

```
% ls -al ~/keyf
drwx------   2 jdoe  staff        512 May 3 11:32 ./
% dd if=/dev/urandom of=$HOME/keyf/05.07.aes16 bs=16  count=1
% chmod 400 ~/keyf/05.07.aes16
```

Exemple 14–2 Création d'une clé pour l'algorithme DES

Dans l'exemple suivant, une clé secrète pour l'algorithme DES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes DES utilisent une clé de 64 bits. La clé est exprimée en tant que clé de 8 octets dans la commande `dd`.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.des8 bs=8  count=1
% chmod 400 ~/keyf/05.07.des8
```

Exemple 14–3 Création d'une clé pour l'algorithme 3DES

Dans l'exemple suivant, une clé secrète pour l'algorithme 3DES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes 3DES utilisent une clé de 192 bits. La clé est exprimée en tant que clé de 24 octets dans la commande `dd`.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.3des.24 bs=24 count=1
% chmod 400 ~/keyf/05.07.3des.24
```

Exemple 14–4 Création d'une clé pour l'algorithme MD5

Dans l'exemple suivant, une clé secrète pour l'algorithme MD5 est créée. La clé est également stockée pour un déchiffrement ultérieur. La clé est exprimée en tant que clé de 64 octets dans la commande `dd`.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.mack64 bs=64 count=1
% chmod 400 ~/keyf/05.07.mack64
```

▼ Génération d'une clé symétrique à l'aide de la commande `pktool`

Certaines applications exigent une clé symétrique pour le chiffrement et le déchiffrement des communications. Dans cette procédure, vous créez une clé symétrique et la stockez.

- Si votre site dispose d'un générateur de nombres aléatoires, vous pouvez l'utiliser pour créer un nombre aléatoire pour la clé. Cette procédure n'utilise pas le générateur de nombres aléatoires de votre site Web.
- Vous pouvez également utiliser la commande `dd` avec le périphérique `/dev/urandom` d'Oracle Solaris en entrée. La commande `dd` ne stocke pas la clé. Pour plus d'informations sur cette procédure, reportez-vous à la section "Génération d'une clé symétrique à l'aide de la commande dd" à la page 292.

1 (Facultatif) Si vous prévoyez d'utiliser un keystore, créez-le.

- **Pour créer et initialiser un keystore PKCS #11, reportez-vous à la section "Procédure de génération d'une phrase de passe à l'aide de la commande `pktool setpin`." à la page 324.**
- **Pour créer et initialiser une base de données NSS, reportez-vous à l'Exemple 15–5.**

2 Générez un nombre aléatoire pour l'utiliser comme clé symétrique.

Choisissez l'une des méthodes suivantes.

- **Générez une clé et stockez-la dans un fichier.**

  L'avantage d'une clé stockée dans un fichier est que vous pouvez extraire la clé de ce fichier pour l'utiliser dans le fichier de clés d'une application, tel que le fichier `/etc/inet/secret/ipseckeys` ou IPsec.

  ```
  % pktool genkey keystore=file outkey=key-fn \
  [keytype=specific-symmetric-algorithm] [keylen=size-in-bits] \
  [dir=directory] [print=n]
  ```

  `keystore`
  La valeur `file` spécifie le type de fichier dans l'emplacement de stockage de la clé.

  `outkey=`*key-fn*
  Nom de fichier lorsque `keystore=file`.

  `keytype=`*specific-symmetric-algorithm*
  Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

  `keylen=`*size-in-bits*
  Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour `des` ou `3des`.

  `dir=`*directory*
  Chemin d'accès au répertoire de *key-fn*. Par défaut, *directory* est le répertoire courant.

  `print=n`
  Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

- **Générez une clé et stockez-la dans un keystore PKCS #11.**

  L'avantage du keystore PKCS #11 est que vous pouvez extraire la clé par son étiquette. Cette méthode est utile pour les clés qui chiffrent et déchiffrent des fichiers. Vous devez effectuer l'Étape 1 avant d'utiliser cette méthode.

  ```
  % pktool genkey label=key-label \
  [keytype=specific-symmetric-algorithm] [keylen=size-in-bits] \
  [token=token] [sensitive=n] [extractable=y] [print=n]
  ```

  `label=`*key-label*
  : Étiquette spécifiée par l'utilisateur pour la clé. La clé peut être récupérée à partir du keystore par son étiquette.

  `keytype=`*specific-symmetric-algorithm*
  : Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

  `keylen=`*size-in-bits*
  : Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour `des` ou `3des`.

  `token=`*token*
  : Nom du jeton. Par défaut, le jeton est `Sun Software PKCS#11 softtoken`.

  `sensitive=n`
  : Détermine la sensibilité de la clé. Lorsque la valeur est `y`, la clé ne peut pas être imprimée à l'aide de l'argument `print=y`. Par défaut, la valeur de `sensitive` est `n`.

  `extractable=y`
  : Indique que la clé peut être extraite du keystore. Spécifiez `n` afin d'empêcher l'extraction de la clé.

  `print=n`
  : Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

- **Générez une clé et stockez-la dans un keystore NSS.**

  Vous devez effectuer l'Étape 1 avant d'utiliser cette méthode.

  ```
  % pktool keystore=nss genkey label=key-label \
  [keytype=[keytype=specific-symmetric-algorithm] [keylen=size-in-bits] [token=token] \
  [dir=directory-path] [prefix=database-prefix]
  ```

  `keystore`
  : La valeur `nss` spécifie le type NSS de l'emplacement de stockage de la clé.

  `label=`*key-label*
  : Étiquette spécifiée par l'utilisateur pour la clé. La clé peut être récupérée à partir du keystore par son étiquette.

  `keytype=`*specific-symmetric-algorithm*
  : Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

`keylen=`*size-in-bits*
Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour `des` ou `3des`.

`token=`*token*
Nom du jeton. Par défaut, le jeton est le jeton interne NSS.

`dir=`*directory*
Chemin d'accès au répertoire de la base de données NSS. Par défaut, *directory* est le répertoire courant.

`prefix=`*directory*
Préfixe de la base de données NSS. Par défaut, le champ de préfixe est vide.

`print=n`
Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

3 (Facultatif) Vérifiez que la clé existe.

Utilisez l'une des commandes suivantes, en fonction de l'endroit où vous avez stocké la clé.

- **Vérifiez la clé dans le fichier *key-fn*.**

```
% pktool list keystore=file objtype=key infile=key-fn
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Vérifiez la clé dans le keystore PKCS #11 ou NSS.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

Exemple 14–5 Création d'une clé DES à l'aide de la commande `pktool`

Dans l'exemple suivant, une clé secrète pour l'algorithme DES est créée. La clé est stockée dans un fichier local pour un déchiffrement ultérieur. La commande protège le fichier avec `400` autorisations. Si la clé est créée, l'option `print=y` affiche la clé générée dans la fenêtre de terminal.

Les mécanismes DES utilisent une clé de 64 bits. L'utilisateur propriétaire du fichier de clés récupère la clé à l'aide de la commande `od`.

```
% pktool genkey keystore=file outkey=64bit.file1 keytype=des print=y
       Key Value ="a3237b2c0a8ff9b3"
% od -x 64bit.file1
0000000 a323 7b2c 0a8f f9b3
```

▼ Procédure de calcul d'une synthèse d'un fichier

Lorsque vous calculez la synthèse d'un fichier, vous pouvez vérifier que le fichier n'a pas été altéré en comparant les résultats de la synthèse. Une synthèse n'altère pas le fichier d'origine.

1 Répertoriez les algorithmes de synthèse disponibles.

```
% digest -l
md5
sha1
sha256
sha384
sha512
```

2 Calculez la synthèse du fichier et enregistrez la liste des synthèses.

Fournissez un algorithme avec la commande `digest`.

`% digest -v -a` *algorithm input-file* `>` *digest-listing*

`-v`	Affiche la sortie au format suivant : *algorithm* `(`*input-file*`) =` *digest*
`-a` *algorithm*	Algorithme à utiliser pour calculer une synthèse du fichier. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de l'Étape 1.
input-file	Fichier d'entrée pour la commande `digest`.
digest-listing	Fichier de sortie pour la commande `digest`.

Exemple 14–6 Calcul d'une synthèse avec le mécanisme MD5

Dans l'exemple suivant, la commande `digest` utilise le mécanisme MD5 pour calculer la synthèse pour une pièce jointe d'un e-mail.

```
% digest -v -a md5 email.attach >>  $HOME/digest.emails.05.07
% cat  ~/digest.emails.05.07
md5 (email.attach) = 85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Lorsque l'option `-v` n'est pas utilisée, la synthèse est enregistrée sans informations complémentaires :

```
% digest -a md5 email.attach >>  $HOME/digest.emails.05.07
% cat  ~/digest.emails.05.07
85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Exemple 14–7 Calcul d'une synthèse avec le mécanisme SHA1

Dans l'exemple suivant, la commande `digest` utilise le mécanisme SHA1 pour fournir une liste des répertoires. Les résultats sont placés dans un fichier.

```
% digest -v -a sha1 docs/* > $HOME/digest.docs.legal.05.07
% more ~/digest.docs.legal.05.07
sha1 (docs/legal1) = 1df50e8ad219e34f0b911e097b7b588e31f9b435
sha1 (docs/legal2) = 68efa5a636291bde8f33e046eb33508c94842c38
sha1 (docs/legal3) = 085d991238d61bd0cfa2946c183be8e32cccf6c9
sha1 (docs/legal4) = f3085eae7e2c8d008816564fdf28027d10e1d983
```

▼ Calcul du code MAC d'un fichier

Un code d'authentification des messages, ou MAC, calcule la synthèse pour le fichier et utilise une clé secrète pour protéger davantage cette synthèse. Un code MAC n'altère pas le fichier d'origine.

1 Répertoriez les mécanismes disponibles.

```
% mac -l
Algorithm       Keysize:  Min   Max
---------------------------------
des_mac                  64    64
sha1_hmac                 8   512
md5_hmac                  8   512
sha256_hmac               8   512
sha384_hmac               8  1024
sha512_hmac               8  1024
```

2 Générez une clé symétrique de la longueur appropriée.

Deux options s'offrent à vous : Vous pouvez fournir une phrase de passe à partir de laquelle une clé sera générée. Ou vous pouvez fournir une clé.

- Si vous fournissez une phrase de passe, vous devez la stocker ou la mémoriser. Si vous la stockez en ligne, le fichier de la phrase de passe ne doit être lisible que par vous.
- Si vous fournissez une clé, elle doit avoir la taille correcte pour le mécanisme. Pour plus d'informations sur cette procédure, reportez-vous à la section "Génération d'une clé symétrique à l'aide de la commande dd" à la page 292.

3 Créez un MAC pour un fichier.

Fournissez une clé et utilisez un algorithme de clé symétrique avec la commande `mac`.

`% mac -v -a` *algorithm* `[ -k` *keyfile* `]` *input-file*

`-v`	Affiche la sortie au format suivant : *algorithm* `(`*input-file*`) =` *mac*
`-a` *algorithm*	Algorithme à utiliser pour calculer le code MAC. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de la commande `mac -l`.
`-k` *keyfile*	Fichier contenant une clé de longueur spécifiée par algorithme.
input-file	Fichier d'entrée pour le MAC.

Exemple 14–8 Calcul d'un MAC avec DES_MAC et une phrase de passe

Dans l'exemple suivant, la pièce jointe d'e-mail est authentifiée avec le mécanisme DES_MAC et une clé dérivée d'une phrase de passe. La liste MAC est enregistrée dans un fichier. Si la phrase de passe est stockée dans un fichier, celui-ci doit être lisible uniquement par l'utilisateur.

```
% mac -v -a des_mac email.attach
Enter passphrase:     <Type passphrase>
des_mac (email.attach) = dd27870a
% echo "des_mac (email.attach) = dd27870a" >> ~/desmac.daily.05.07
```

Exemple 14–9 Calcul d'un MAC avec MD5_HMAC et un fichier de clés

Dans l'exemple suivant, la pièce jointe d'e-mail est authentifiée avec le mécanisme MD5_HMAC et une clé secrète. La liste MAC est enregistrée dans un fichier.

```
% mac -v -a md5_hmac -k $HOME/keyf/05.07.mack64 email.attach
md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c
% echo "md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c" \
>> ~/mac.daily.05.07
```

Exemple 14–10 Calcul d'un MAC avec SHA1_HMAC et un fichier de clés

Dans l'exemple suivant, le manifeste de répertoire est authentifié avec le mécanisme SHA1_HMAC et une clé secrète. Les résultats sont placés dans un fichier.

```
% mac -v -a sha1_hmac \
-k $HOME/keyf/05.07.mack64 docs/* > $HOME/mac.docs.legal.05.07
% more ~/mac.docs.legal.05.07
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

▼ Chiffrement et déchiffrement d'un fichier

Lorsque vous chiffrez un fichier, le fichier d'origine n'est ni supprimé, ni modifié. Le fichier de sortie est chiffré.

Pour trouver des solutions aux erreurs courantes générées par la commande `encrypt`, reportez-vous à la section suivant les exemples.

1 Créez une clé symétrique de la longueur appropriée.

Deux options s'offrent à vous. Vous pouvez fournir une phrase de passe à partir de laquelle une clé sera générée. Ou vous pouvez fournir une clé.

- Si vous fournissez une phrase de passe, vous devez stocker ou mémoriser la phrase de passe. Si vous la stockez en ligne, le fichier de la phrase de passe ne doit être lisible que par vous.
- Si vous fournissez une clé, elle doit avoir la taille correcte pour le mécanisme. Pour plus d'informations sur cette procédure, reportez-vous à la section "Génération d'une clé symétrique à l'aide de la commande dd" à la page 292.

2 Chiffrez un fichier.

Fournissez une clé et utilisez un algorithme de clé symétrique avec la commande `encrypt`.

```
% encrypt -a algorithm  [ -k keyfile ] -i input-file -o output-file
```

`-a` *algorithm*	Algorithme à utiliser pour chiffrer le fichier. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de la commande `encrypt -l`.
`-k` *keyfile*	Fichier contenant une clé de longueur spécifiée par algorithme. La longueur de la clé pour chaque algorithme est répertoriée, en bits, dans la sortie de la commande `encrypt -l`.
`-i` *input-file*	Fichier d'entrée que vous voulez chiffrer. Ce fichier n'est pas modifié par la commande.
`-o` *output-file*	Fichier de sortie correspondant à la forme chiffrée du fichier d'entrée.

Exemple 14–11 Chiffrement et déchiffrement avec AES et une phrase de passe

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme AES. La clé est générée à partir de la phrase de passe. Si la phrase de passe est stockée dans un fichier, celui-ci doit être lisible uniquement par l'utilisateur.

```
% encrypt -a aes -i ticket.to.ride -o ~/enc/e.ticket.to.ride
Enter passphrase:     <Type passphrase>
Re-enter passphrase:      Type passphrase again
```

Le fichier d'entrée, `ticket.to.ride`, existe toujours sous sa forme d'origine.

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même phrase de passe et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement du fichier.

```
% decrypt -a aes -i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
Enter passphrase:     <Type passphrase>
```

Exemple 14–12 Chiffrement et déchiffrement avec AES et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme AES. Les mécanismes AES utilisent une clé de 128 bits, ou 16 octets.

```
% encrypt -a aes -k ~/keyf/05.07.aes16 \
-i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

Le fichier d'entrée, `ticket.to.ride`, existe toujours sous sa forme d'origine.

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a aes -k ~/keyf/05.07.aes16  \
-i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

Exemple 14–13 Chiffrement et déchiffrement avec ARCFOUR et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme ARCFOUR. L'algorithme ARCFOUR accepte une clé de 8 bits (1 octet), 64 bits (8 octets) ou 128 bits (16 octets).

```
% encrypt -a arcfour -i personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/enc/e.personal.txt
```

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a arcfour -i ~/enc/e.personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/personal.txt
```

Exemple 14–14 Chiffrement et déchiffrement avec 3DES et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme 3DES. L'algorithme 3DES requiert une clé de 192 bits, ou 24 octets.

```
% encrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/personal2.txt -o ~/enc/e.personal2.txt
```

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/enc/e.personal2.txt -o ~/personal2.txt
```

Erreurs fréquentes

Les messages suivants indiquent que la clé que vous avez fournie à la commande `encrypt` n'est pas autorisée par l'algorithme utilisé.

- `encrypt: unable to create key for crypto operation: CKR_ATTRIBUTE_VALUE_INVALID`
- `encrypt: failed to initialize crypto operation: CKR_KEY_SIZE_RANGE`

Si vous transmettez une clé ne répondant pas aux exigences de l'algorithme, vous devez fournir une meilleure clé.

- La première option consiste à utiliser une phrase de passe. La structure fournit ensuite une clé qui remplit les conditions requises.
- La deuxième option consiste à transmettre une taille de clé acceptée par l'algorithme. Par exemple, l'algorithme DES requiert une clé de 64 bits. L'algorithme 3DES requiert une clé de 192 bits.

Administration de la structure cryptographique (liste des tâches)

La liste des tâches suivante présente les procédures permettant d'administrer les fournisseurs de logiciels et matériels dans la structure cryptographique.

Tâche	Description	Voir
Établissement de la liste des fournisseurs dans la structure cryptographique Oracle Solaris	Répertorie les algorithmes, les bibliothèques et les périphériques matériels disponibles pour l'utilisation dans la structure cryptographique Oracle Solaris.	"Liste des fournisseurs disponibles" à la page 304
Ajout d'un fournisseur de logiciels	Ajoute une bibliothèque PKCS #11 ou un module de noyau à la structure cryptographique. Le fournisseur doit être signé.	"Ajout d'un fournisseur de logiciels" à la page 306
Interdiction d'utilisation d'un mécanisme au niveau de l'utilisateur	Empêche l'utilisation d'un mécanisme logiciel. Le mécanisme peut être activé à nouveau.	"Interdiction d'utilisation d'un mécanisme au niveau de l'utilisateur" à la page 308
Désactivation temporaire des mécanismes d'un module de noyau	Empêche temporairement l'utilisation d'un mécanisme. Généralement utilisée à des fins de test.	"Interdiction de l'utilisation d'un fournisseur de logiciels noyau" à la page 309
Désinstallation d'un fournisseur	Empêche l'utilisation d'un fournisseur de logiciels noyau.	Exemple 14–22
Établissement de la liste des fournisseurs de matériel disponibles	Affiche le matériel connecté, les mécanismes que le matériel fournit et les mécanismes activés pour utilisation.	"Liste des fournisseurs de matériel" à la page 312
Désactivation de mécanismes d'un fournisseur de matériel	Permet de s'assurer que les mécanismes sélectionnés sur un accélérateur matériel ne sont pas utilisés.	"Désactivation des mécanismes et fonctions d'un fournisseur de matériel" à la page 313
Redémarrage ou actualisation des services cryptographiques	Permet de s'assurer que les services cryptographiques sont disponibles.	"Actualisation ou redémarrage de tous les services cryptographiques" à la page 315

Administration de la structure cryptographique (tâches)

Cette section explique l'administration des fournisseurs de logiciels et des fournisseurs de matériel dans la structure cryptographique. L'utilisation de ces fournisseurs peut être empêchée lorsque cela est souhaitable. Par exemple, vous pouvez désactiver l'implémentation d'un algorithme d'un seul fournisseur de logiciels. Ensuite, vous pouvez forcer le système à utiliser l'algorithme d'un autre fournisseur de logiciels.

▼ Liste des fournisseurs disponibles

La structure cryptographique Oracle Solaris fournit des algorithmes pour plusieurs types de consommateurs :

- Les fournisseurs au niveau de l'utilisateur offrent une interface de chiffrement PKCS #11 aux applications liées à la bibliothèque `libpkcs11`.
- Les fournisseurs de logiciels noyau offrent des algorithmes pour IPsec, Kerberos et d'autres composants de noyau Oracle Solaris
- Les fournisseurs de matériel noyau offrent des algorithmes disponibles pour les consommateurs de noyau et les applications via la bibliothèque `pkcs11_kernel`.

1 Répertoriez les fournisseurs dans un format c

Remarque – Le contenu et le format de la liste de fournisseurs varient selon les versions d'Oracle Solaris. Exécutez la commande `cryptoadm list` sur votre système pour afficher les fournisseurs que votre système prend en charge.

Seuls les mécanismes au niveau de l'utilisateur sont disponibles pour les utilisateurs standard.

```
% cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa

kernel hardware providers:
    ncp/0
```

2 Répertoriez les fournisseurs et leurs mécanismes dans la structure cryptographique.

Tous les mécanismes sont répertoriés dans la sortie suivante. Cependant, certains de ces mécanismes peuvent ne pas être disponibles pour l'utilisation. Pour répertorier uniquement les mécanismes approuvés pour l'utilisation par l'administrateur, reportez-vous à l'Exemple 14–16.

La sortie est reformatée à des fins d'affichage.

```
% cryptoadm list -m
user-level providers:
=====================
/usr/lib/security/$ISA/pkcs11_kernel.so: CKM_MD5,CKM_MD5_HMAC,
CKM_MD5_HMAC_GENERAL,CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL,
...
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
kernel software providers:
==========================
des: CKM_DES_ECB,CKM_DES_CBC,CKM_DES3_ECB,CKM_DES3_CBC
aes: CKM_AES_ECB,CKM_AES_CBC
blowfish: CKM_BF_ECB,CKM_BF_CBC
arcfour: CKM_RC4
sha1: CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL
md5: CKM_MD5,CKM_MD5_HMAC,CKM_MD5_HMAC_GENERAL
rsa: CKM_RSA_PKCS,CKM_RSA_X_509,CKM_MD5_RSA_PKCS,CKM_SHA1_RSA_PKCS
swrand: No mechanisms presented.

kernel hardware providers:
==========================
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

Exemple 14–15 Recherche de mécanismes cryptographiques existants

Dans l'exemple suivant, tous les mécanismes offerts par la bibliothèque au niveau de l'utilisateur, `pkcs11_softtoken`, sont répertoriés.

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
CKM_SSL3_KEY_AND_MAC_DERIVE,CKM_TLS_KEY_AND_MAC_DERIVE
```

Exemple 14–16 Recherche de mécanismes cryptographiques disponibles

La stratégie détermine les mécanismes utilisables. L'administrateur définit la stratégie. Un administrateur peut choisir de désactiver des mécanismes à partir d'un fournisseur particulier. L'option `-p` affiche la liste des mécanismes autorisés par la stratégie définie par l'administrateur.

```
% cryptoadm list -p
user-level providers:
=====================
/usr/lib/security/$ISA/pkcs11_kernel.so: all mechanisms are enabled.
random is enabled.
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.

kernel software providers:
==========================
des: all mechanisms are enabled.
aes: all mechanisms are enabled.
blowfish: all mechanisms are enabled.
arcfour: all mechanisms are enabled.
sha1: all mechanisms are enabled.
md5: all mechanisms are enabled.
rsa: all mechanisms are enabled.
swrand: random is enabled.

kernel hardware providers:
==========================
ncp/0: all mechanisms are enabled.
```

▼ Ajout d'un fournisseur de logiciels

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Répertoriez les fournisseurs de logiciels disponibles sur le système.

```
% cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa

kernel hardware providers:
    ncp/0
```

3 Ajoutez le package d'un fournisseur en utilisant la commande pkgadd.

```
# pkgadd -d /path/to/package  pkginst
```

Le package doit inclure un logiciel signé par un certificat de Sun. Pour demander un certificat auprès de Sun et signer un fournisseur, reportez-vous à l'Annexe F, "Packaging and Signing Cryptographic Providers" du *Developer's Guide to Oracle Solaris Security*.

Le package doit avoir des scripts qui avertissent la structure cryptographique qu'un autre fournisseur doté d'un jeu de mécanismes est disponible. Pour plus d'informations sur les conditions d'empaquetage requises, reportez-vous à l'Annexe F, "Packaging and Signing Cryptographic Providers" du *Developer's Guide to Oracle Solaris Security*.

4 Actualisez les fournisseurs.

Vous devez actualiser les fournisseurs si vous avez ajouté un fournisseur de logiciels ou si vous avez ajouté un matériel et spécifié une stratégie pour ce matériel.

```
# svcadm refresh svc:/system/cryptosvc
```

5 Localisez le nouveau fournisseur dans la liste.

Dans ce cas, un nouveau fournisseur de logiciels noyau a été installé.

```
# cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
    ecc      <-- added provider
...
```

Exemple 14–17 Ajout d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, une bibliothèque PKCS 11 signée est installée.

```
# pkgadd -d /cdrom/cdrom0/SolarisNew
    Answer the prompts
# svcadm refresh system/cryptosvc
# cryptoadm list
user-level providers:
==========================
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so
    /opt/SUNWconn/lib/$ISA/libpkcs11.so.1      <-- added provider
```

Les développeurs qui testent une bibliothèque avec la structure cryptographique peuvent installer la bibliothèque manuellement.

```
# cryptoadm install provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
```

Pour plus d'informations sur l'obtention de la signature pour votre fournisseur, reportez-vous à la section "Signatures binaires pour les logiciels tiers" à la page 288.

▼ Interdiction d'utilisation d'un mécanisme au niveau de l'utilisateur

Si certains des mécanismes cryptographiques provenant d'un fournisseur de bibliothèques ne doivent pas être utilisés, vous pouvez supprimer les mécanismes sélectionnés. Cette procédure utilise les mécanismes DES de la bibliothèque `pkcs11_softtoken` comme un exemple.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle incluant le profil de droits de gestion de la cryptographie.**

Pour créer un rôle incluant le profil de droits de gestion de la cryptographie et l'assigner à un utilisateur, reportez-vous à l'Exemple 9–7.

2 **Répertoriez les mécanismes offerts par un fournisseur de logiciels particulier au niveau de l'utilisateur.**

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
```

3 **Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p
user-level providers:
=====================
...
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
...
```

4 **Désactivez les mécanismes qui ne doivent pas être utilisés.**

```
$ cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB
```

5 **Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

Exemple 14–18 Activation d'un mécanisme d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, un mécanisme DES désactivé est de nouveau rendu disponible pour l'utilisation.

```
$ cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_ECB
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

Exemple 14–19 Activation de tous les mécanismes d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, tous les mécanismes de la bibliothèque au niveau de l'utilisateur sont activés.

```
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so all
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
```

Exemple 14–20 Suppression définitive de la disponibilité d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, la bibliothèque `libpkcs11.so.1` est supprimée.

```
$ cryptoadm uninstall provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
$ cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
...
```

▼ Interdiction de l'utilisation d'un fournisseur de logiciels noyau

Si la structure cryptographique fournit plusieurs modes d'un fournisseur tel que AES, vous pouvez supprimer un mécanisme lent ou corrompu. Cette procédure utilise l'algorithme AES comme exemple.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle incluant le profil de droits de gestion de la cryptographie.**

   Pour créer un rôle incluant le profil de droits de gestion de la cryptographie et l'assigner à un utilisateur, reportez-vous à l'Exemple 9–7.

2. **Répertoriez les mécanismes qui sont offerts par un fournisseur de logiciels noyau particulier.**

```
$ cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
```

3. **Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

4. **Désactivez le mécanisme qui ne doit pas être utilisé.**

```
$ cryptoadm disable provider=aes mechanism=CKM_AES_ECB
```

5. **Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
```

Exemple 14–21 Activation d'un mécanisme d'un fournisseur de logiciels noyau

Dans l'exemple suivant, un mécanisme AES désactivé est de nouveau rendu disponible pour l'utilisation.

```
cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
$ cryptoadm enable provider=aes mechanism=CKM_AES_ECB
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

Exemple 14–22 Suppression temporaire de la disponibilité d'un fournisseur de logiciels noyau

Dans l'exemple suivant, l'utilisation du fournisseur AES est temporairement rendue impossible. La sous-commande `unload` est utile pour empêcher le chargement automatique d'un fournisseur pendant que le fournisseur est en cours de désinstallation. Par exemple, la sous-commande `unload` peut être utilisée lors de l'installation d'un patch qui affecte le fournisseur.

```
$ cryptoadm unload provider=aes

$ cryptoadm list
...
kernel software providers:
    des
```

```
    aes (inactive)
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Le fournisseur AES reste indisponible jusqu'à l'actualisation de la structure cryptographique.

```
$ svcadm refresh system/cryptosvc

$ cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Si un consommateur de noyau utilise le fournisseur de logiciels noyau, le logiciel n'est pas déchargé. Un message d'erreur s'affiche et le fournisseur continue d'être disponible pour l'utilisation.

Exemple 14–23 Suppression définitive de la disponibilité du fournisseur de logiciels

Dans l'exemple suivant, l'utilisation du fournisseur AES est définitivement rendue impossible. Une fois supprimé, le fournisseur AES n'apparaît plus dans la liste des stratégies des fournisseurs de logiciels noyau.

```
$ cryptoadm uninstall provider=aes

$ cryptoadm list
...
kernel software providers:
    des
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

Si un consommateur de noyau utilise ce fournisseur de logiciels noyau, un message d'erreur s'affiche et le fournisseur continue d'être disponible pour l'utilisation.

Exemple 14–24 Réinstallation d'un fournisseur de logiciels noyau supprimé

Dans l'exemple suivant, le fournisseur de logiciels noyau AES est réinstallé.

```
$ cryptoadm install provider=aes mechanism=CKM_AES_ECB,CKM_AES_CBC

$ cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
```

▼ Liste des fournisseurs de matériel

Les fournisseurs de matériel sont automatiquement détectés et chargés. Pour plus d'informations, reportez-vous à la page de manuel `driver.conf(4)`.

Avant de commencer

Lorsque du matériel doit être utilisé au sein de la structure cryptographique Oracle Solaris, le matériel s'enregistre sur la SPI dans le noyau. La structure vérifie que le pilote matériel est signé. Plus précisément, la structure vérifie que le fichier d'objet du pilote est signé au moyen d'un certificat émis par Sun.

Par exemple, la carte Sun Crypto Accelerator 6000 (`mca`), le pilote NCP pour l'accélérateur cryptographique sur les processeurs UltraSPARC T1 et T2 (`ncp`) et le pilote N2CP pour les processeurs UltraSPARC T2 (`n2cp`) connectent les mécanismes matériels à la structure.

Pour plus d'informations sur l'obtention de la signature pour votre fournisseur, reportez-vous à la section "Signatures binaires pour les logiciels tiers" à la page 288.

1. **Répertoriez les fournisseurs de matériel disponibles sur le système.**

```
% cryptoadm list
...
kernel hardware providers:
   ncp/0
```

2. **Répertoriez les mécanismes fournis par la puce ou la carte.**

```
% cryptoadm list -m provider=ncp/0
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

3 Répertoriez les mécanismes disponibles pour l'utilisation sur la puce ou la carte.

```
% cryptoadm list -p provider=ncp/0
ncp/0: all mechanisms are enabled.
```

▼ Désactivation des mécanismes et fonctions d'un fournisseur de matériel

Vous pouvez désactiver de façon sélective des mécanismes et la fonction de nombres aléatoires à partir d'un fournisseur de matériel. Pour les réactiver, reportez-vous à l'Exemple 14–25. Le matériel de cet exemple, la carte Sun Crypto Accelerator 1000, fournit un générateur de nombres aléatoires.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle incluant le profil de gestion de la cryptographie.

Pour créer un rôle incluant le profil de droits de gestion de la cryptographie et l'assigner à un utilisateur, reportez-vous à l'Exemple 9–7.

2 Choisissez les mécanismes ou la fonction à désactiver.

Répertoriez le fournisseur de matériel.

```
# cryptoadm list
...
Kernel hardware providers:
    dca/0
```

- **Désactivez les mécanismes sélectionnés.**

```
# cryptoadm list -m provider=dca/0
dca/0: CKM_RSA_PKCS, CKM_RSA_X_509, CKM_DSA, CKM_DES_CBC, CKM_DES3_CBC
random is enabled.
# cryptoadm disable provider=dca/0 mechanism=CKM_DES_CBC,CKM_DES3_CBC
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_CBC,CKM_DES3_CBC.
random is enabled.
```

- **Désactivez le générateur de nombres aléatoires.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

- **Désactivez tous les mécanismes. Ne désactivez pas le générateur de nombres aléatoires.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is enabled.
```

- **Désactivez toutes les fonctions et tous les mécanismes sur le matériel.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is disabled.
```

Exemple 14–25 Activation des mécanismes et fonctions sur un fournisseur de matériel

Dans les exemples suivants, les mécanismes désactivés sur un élément matériel sont activés individuellement.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB,CKM_DES3_ECB

.
random is enabled.
# cryptoadm enable provider=dca/0 mechanism=CKM_DES3_ECB
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB.
random is enabled.
```

Dans l'exemple ci-dessous, seul le générateur aléatoire est activé.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is disabled.
# cryptoadm enable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is enabled.
```

Dans l'exemple ci-dessous, seuls les mécanismes sont activés. Le générateur aléatoire reste désactivé.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,....
random is disabled.
# cryptoadm enable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

Dans l'exemple suivant, toutes les fonctions et tous les mécanismes de la carte sont activés.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_DES_ECB,CKM_DES3_ECB.
random is disabled.
# cryptoadm enable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
```

▼ Actualisation ou redémarrage de tous les services cryptographiques

Par défaut, la structure cryptographique Oracle Solaris est activée. Lorsque le démon `kcfd` échoue pour une raison quelconque, l'utilitaire de gestion des services peut être utilisé pour redémarrer les services cryptographiques. Pour plus d'informations, reportez-vous aux pages de manuel `smf(5)` et `svcadm(1M)`. Pour connaître l'effet du redémarrage des services cryptographiques sur les zones, reportez-vous à la section "Services cryptographiques et zones" à la page 289.

1 **Vérifiez l'état des services cryptographiques.**

```
% svcs cryptosvc
 STATE          STIME    FMRI
offline         Dec_09   svc:/system/cryptosvc:default
```

2 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent pour activer les services cryptographiques.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

```
# svcadm enable svc:/system/cryptosvc
```

Exemple 14–26 Actualisation des services cryptographiques

Dans l'exemple suivant, les services cryptographiques sont actualisés dans la zone globale. Par conséquent, la stratégie de cryptographie au niveau du noyau dans chaque zone non globale est également actualisée.

```
# svcadm refresh system/cryptosvc
```

◆ ◆ ◆ CHAPITRE 15

Structure de gestion des clés Oracle Solaris

Depuis la version Solaris 10 8/07, la structure de gestion des clés (KMF) fournit des outils et des interfaces de programmation pour gérer les objets de clé publique. Les objets de clé publique comprennent les certificats X.509 et les paires de clés publiques et privées. Les formats de stockage de ces objets peuvent varier. KMF offre également un outil de gestion des stratégies qui définissent l'utilisation de certificats X.509 par des applications.

Gestion des technologies à clé publique

La structure de gestion des clés (KMF) fournit une approche unifiée à la gestion des technologies à clé publique (PKI). Oracle Solaris dispose de différentes applications qui utilisent des technologies PKI. Chaque application fournit ses propres interfaces de programmation, mécanismes de stockage des clés et utilitaires d'administration. Si une application offre un mécanisme d'application de stratégie, ce mécanisme s'applique uniquement à l'application correspondante. Avec KMF, les applications utilisent un ensemble unifié d'outils d'administration, un ensemble d'interfaces de programmation et un mécanisme d'application de stratégie. Ces fonctions gèrent les besoins en PKI de toutes les applications adoptant ces interfaces.

KMF unifie la gestion des technologies à clé publique avec les interfaces suivantes :

- **Commande pktool :** cette commande gère les objets PKI, tels que les certificats, dans une variété de keystores.
- **Commande kmfcfg :** cette commande gère la base de données de stratégie PKI.

  Les décisions de stratégie PKI comprennent des opérations telles que la méthode de validation d'une opération. En outre, la stratégie PKI peut limiter l'étendue d'un certificat. Par exemple, la stratégie PKI peut affirmer qu'un certificat peut être utilisé uniquement à des fins spécifiques. Une telle stratégie peut empêcher qu'un certificat soit utilisé pour d'autres demandes.
- **Bibliothèque KMF :** Cette bibliothèque contient des interfaces de programmation qui extraient le mécanisme keystore sous-jacent.

  Les applications n'ont pas à choisir un mécanisme de keystore spécifique, ils peuvent migrer d'un seul mécanisme à un autre. Les fichiers keystore pris en charge sont PKCS #11, NSS et OpenSSL La bibliothèque comprend une structure modulable permettant l'ajout de nouveaux mécanismes keystore. Par conséquent, les applications qui utilisent les nouveaux mécanismes ne nécessitent que des modifications mineures pour utiliser un nouveau keystore.

Utilitaires de la structure de gestion des clés

KMF offre des méthodes pour la gestion du stockage des clés et fournit la stratégie globale concernant l'utilisation de ces clés. KMF gère la stratégie, les clés et les certificats pour les trois technologies à clé publique suivantes :

- Fournisseurs de jetons de PKCS #11, c'est-à-dire provenant de la structure cryptographique Oracle Solaris
- NSS, c'est-à-dire les services de sécurité réseau (Network Security Services)
- OpenSSL, un keystore basé les fichiers

L'outil `kmfcfg` peut créer, modifier ou supprimer des entrées de stratégie KMF. KMF gère les keystores par le biais de la commande `pktool`. Pour plus d'informations, reportez-vous aux pages de manuel `kmfcfg(1)` et `pktool(1)` et aux sections suivantes.

Gestion de la stratégie KMF

La stratégie KMF est enregistrée dans une base de données. Cette base de données de stratégie est accédée en interne par toutes les applications qui utilisent les interfaces de programmation KMF. La base de données peut limiter l'utilisation des clés et des certificats qui sont gérés par la bibliothèque KMF. Lorsqu'une application tente de vérifier un certificat, l'application vérifie la base de données de stratégies. La commande `kmfcfg` modifie la base de données de stratégies.

Gestion de keystore KMF

KMF gère les keystores pour les trois technologies à clé publique, PKCS #11, NSS et OpenSSL. Pour l'ensemble de ces technologies, la commande `pktool` vous permet d'effectuer les opérations suivantes :

- Génération d'un certificat autosigné
- Génération d'une demande de certificat
- Importation d'objets dans le keystore
- Liste des objets dans le keystore
- Suppression d'objets du keystore
- Téléchargement d'une CRL.

Pour les technologies PKCS #11 et NSS, la commande `pktool` vous permet également de définir un code PIN en générant une phrase de passe :

- Génération d'une phrase de passe pour le keystore.
- Génération d'une phrase de passe pour un objet dans le keystore.

Pour consulter des exemples d'utilisation de l'utilitaire `pktool`, reportez-vous à la page de manuel `pktool(1)` et à la section "Utilisation de la structure de gestion des clés (liste des tâches)" à la page 319.

Utilisation de la structure de gestion des clés (liste des tâches)

La structure de gestion des clés (KMF) vous permet de gérer de manière centralisée les technologies à clé publique.

Tâche	Description	Voir
Création d'un certificat	Crée un certificat à utiliser par PKCS #11, NSS ou SSL.	"Procédure de création d'un certificat à l'aide de la commande `pktool gencert`" à la page 320
Exportation d'un certificat	Crée un fichier avec le certificat et ses clés de prise en charge. Le fichier peut être protégé par un mot de passe.	"Procédure d'exportation d'un certificat et de la clé privée au format PKCS #12" à la page 322
Importation d'un certificat	Importe un certificat à partir d'un autre système.	"Procédure d'importation d'un certificat dans votre keystore" à la page 321
	Importe un certificat en format PKCS #12 à partir d'un autre système.	Exemple 15–2
Génération d'une phrase de passe.	Génère une phrase de passe pour l'accès à un keystore PKCS #11 ou NSS.	"Procédure de génération d'une phrase de passe à l'aide de la commande `pktool setpin`." à la page 324

Utilisation de la structure de gestion des clés (tâches)

Cette section décrit l'utilisation de la commande `pktool` pour gérer vos objets de clé publique, tels que des mots et phrases de passe, des fichiers, des keystores, des certificats et des CRL.

▼ Procédure de création d'un certificat à l'aide de la commande `pktool gencert`

Cette procédure crée un certificat autosigné et le stocke dans le keystore PKCS #11. Dans le cadre de cette opération, une paire de clés publique et privée RSA est également créée. La clé privée est stockée dans le keystore avec le certificat.

1 Générez un certificat autosigné

```
% pktool gencert [keystore=keystore] label=label-name \
subject=subject-DN serial=hex-serial-number
```

`keystore=`*keystore*	Spécifie le keystore par type d'objet de clé publique. La valeur peut être `nss`, `pkcs11` ou `ssl`. Ce mot de passe est facultatif.
`label=`*label-name*	Spécifie un nom unique donné au certificat par l'émetteur.
`subject=`*subject-DN*	Spécifie le nom distinctif du certificat.
`serial=`*hex-serial-number*	Spécifie le numéro de série au format hexadécimal. L'émetteur du certificat choisit ce nombre, comme par exemple `0x0102030405`.

2 Vérifiez le contenu du keystore.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
      ID: Fingerprint that binds certificate to private key
      Subject: subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
n. ...
```

Cette commande répertorie tous les certificats dans le keystore. Dans l'exemple suivant, le keystore ne contient qu'un seul certificat.

Exemple 15–1 Création d'un certificat autosigné à l'aide de `pktool`

Dans l'exemple suivant, un utilisateur à `My Company` crée un certificat autosigné et le stocke dans un keystore pour les objets PKCS #11. Le keystore est initialement vide. Si le keystore n'a pas été initialisé, le code PIN pour le softtoken est `changeme`.

```
% pktool gencert keystore=pkcs11 label="My Cert" \
subject="C=US, O=My Company, OU=Security Engineering Group, CN=MyCA" \
serial=0x000000001
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token

% pktool list
Found 1 certificates.
1. (X.509 certificate)
      Label: My Cert
      ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
      Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Serial: 0x01
```

▼ Procédure d'importation d'un certificat dans votre keystore

Cette procédure explique comment importer un fichier contenant des informations PKI codé avec PEM ou DER raw dans votre keystore. Pour connaître la procédure d'exportation, reportez-vous à l'Exemple 15–4.

1 Importez le certificat.

```
% pktool import keystore=keystore infile=infile-name label=label-name
```

2 Si vous importez des objets PKI privés, entrez les mots de passe lorsque vous y êtes invité.

a. À l'invite, entrez le mot de passe pour le fichier.

Si vous importez des informations PKI privées, tels qu'un fichier d'exportation au format PKCS #12, le fichier nécessite un mot de passe. Le créateur du fichier que vous importez vous fournit le mot de passe PKCS #12.

```
Enter password to use for accessing the PKCS12 file:      Type PKCS #12 password
```

b. À l'invite, entrez le mot de passe pour le keystore.

```
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
```

3 Vérifiez le contenu du keystore.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
      ID:  Fingerprint that binds certificate to private key
      Subject:  subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
2. ...
```

Exemple 15–2 Importation d'un fichier PKCS #12 dans votre keystore

Dans l'exemple suivant, l'utilisateur importe un fichier PKCS #12 d'un tiers. La commande `pktool import` extrait la clé privée et le certificat du fichier `gracedata.p12` et les stocke dans le keystore préféré de l'utilisateur.

```
% pktool import keystore=pkcs11 infile=gracedata.p12 label=GraceCert
Enter password to use for accessing the PKCS12 file:     Type PKCS #12 password
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Found 1 certificate(s) and 1 key(s) in gracedata.p12
% pktool list
Found 1 certificates.
1. (X.509 certificate)
        Label: GraceCert
        ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
        Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
        Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
        Serial: 0x01
```

Exemple 15–3 Importation d'un certificat X.509 dans votre keystore

Dans l'exemple suivant, l'utilisateur importe un certificat X.509 au format PEM dans le keystore préféré de l'utilisateur. Ce certificat public n'est pas protégé par un mot de passe. Le keystore public de l'utilisateur n'est pas protégé par un mot de passe non plus.

```
% pktool import keystore=pkcs11 infile=somecert.pem label="TheirCompany Root Cert"
% pktool list
Found 1 certificates.
1. (X.509 certificate)
        Label: TheirCompany Root Cert
        ID: 21:ae:83:98:24:d1:1f:cb:65:5b:48:75:7d:02:47:cf:98:1f:ec:a0
        Subject: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
        Issuer: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
        Serial: 0x01
```

▼ Procédure d'exportation d'un certificat et de la clé privée au format PKCS #12

Vous pouvez créer un fichier au format PKCS #12 afin d'exporter des clés privées et leur certificat X.509 associé vers d'autres systèmes. L'accès au fichier est protégé par un mot de passe.

1 Recherchez le certificat à exporter.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
      Label:  label-name
```

```
      ID: Fingerprint that binds certificate to private key
      Subject: subject-DN
      Issuer:  distinguished-name
      Serial:  hex-serial-number
2. ...
```

2 Exportez les clés et le certificat.

Utilisez le keystore et l'étiquette de la commande `pktool list`. Donnez un nom au fichier d'exportation. Si le nom contient un espace, mettez le nom entre guillemets.

```
% pktool export keystore=keystore outfile=outfile-name label=label-name
```

3 Protégez le fichier d'exportation par un mot de passe.

À l'invite, entrez le mot de passe courant du keystore. À ce stade, vous créez un mot de passe pour le fichier d'exportation. Le destinataire doit fournir ce mot de passe lors de l'importation du fichier.

```
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file:     Create PKCS #12 password
```

Astuce – Envoyez le mot de passe séparément du fichier d'exportation. Les pratiques recommandées suggèrent que vous fournissiez le mot de passe hors bande, par exemple lors d'un appel téléphonique.

Exemple 15–4 Exportation d'un certificat et de la clé privée au format PKCS #12

Dans l'exemple suivant, un utilisateur exporte les clés privées avec leur certificat X.509 associé dans un fichier PKCS #12 normal. Ce fichier peut être importé dans d'autres keystores. Le mot de passe PKCS #11 protège le keystore source. Le mot de passe PKCS #12 est utilisé pour protéger des données privées dans le fichier PKCS #12. Ce mot de passe est requis pour importer le fichier.

```
% pktool list
Found 1 certificates.
1. (X.509 certificate)
      Label: My Cert
      ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
      Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
      Serial: 0x01

% pktool export keystore=pkcs11 outfile=mydata.p12 label="My Cert"
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file:     Create PKCS #12 password
```

L'utilisateur appelle ensuite le destinataire par téléphone pour lui fournir le mot de passe PKCS #12.

▼ Procédure de génération d'une phrase de passe à l'aide de la commande `pktool setpin`.

Vous pouvez générer une phrase de passe pour un objet dans un keystore et pour le keystore lui-même. La phrase de passe est nécessaire pour accéder à l'objet ou au keystore. Pour un exemple de génération d'une phrase de passe pour un objet dans un keystore, reportez-vous à l'Exemple 15–4.

1 Générez une phrase de passe pour accéder à un keystore.

```
% pktool setpin keystore=nss|pkcs11 dir=directory
```

2 Répondez aux invites.

Si aucun mot de passe n'est encore défini pour le keystore, appuyez sur la touche Entrée pour créer le mot de passe.

```
Enter current token passphrase:      Press the Return key
Create new passphrase:      Type the passphrase that you want to use
Re-enter new passphrase:      Retype the passphrase
Passphrase changed.
```

Le keystore est maintenant protégé par une *passphrase*. Si vous perdez la phrase de passe, vous perdez l'accès aux objets dans le keystore.

Exemple 15–5 Protection d'un keystore par une phrase de passe

L'exemple suivant montre comment définir la phrase de passe pour une base de données NSS. Comme aucune phrase de passe n'a été créée, l'utilisateur appuie sur la touche Entrée à la première invite.

```
% pktool setpin keystore=nss dir=/var/nss
Enter current token passphrase:     Press the Return key
Create new passphrase:    has8n0NdaH
Re-enter new passphrase:  has8n0NdaH
Passphrase changed.
```

PARTIE V

Services d'authentification et communication sécurisée

Cette section décrit les services d'authentification pouvant être configurés sur un système autonome ou entre deux systèmes.

Pour configurer un réseau d'utilisateurs et de systèmes authentifiés, reportez-vous à la section Partie VI.

◆ ◆ ◆ CHAPITRE 16

Utilisation des services d'authentification (tâches)

Ce chapitre fournit des informations sur la façon d'utiliser le RPC (appel de procédure à distance) sécurisé pour authentifier un hôte et un utilisateur sur un montage NFS. Voici la liste des sujets abordés dans ce chapitre :

Présentation du RPC sécurisé

Le RPC sécurisé protège les procédures distantes par le biais d'un mécanisme d'authentification. Le mécanisme d'authentification Diffie-Hellman authentifie à la fois l'hôte et l'utilisateur à l'origine d'une demande de service. Le mécanisme d'authentification utilise le chiffrement Data Encryption Standard (DES). Les applications utilisant le RPC sécurisé incluent NFS et les services de nommage, NIS et NIS+.

Services NFS et sécurisé

NFS permet à plusieurs hôtes de partager des fichiers sur le réseau. Dans le cadre du service NFS, un serveur contient les données et les ressources pour plusieurs clients. Les clients ont accès aux systèmes de fichiers que le serveur partage avec les clients. Les utilisateurs connectés aux systèmes client peuvent accéder aux systèmes de fichiers en montant les systèmes de fichiers à partir du serveur. Pour l'utilisateur sur le système client, il s'affiche comme si les fichiers étaient des fichiers locaux pour le client. L'une des utilisations les plus courantes de NFS permet aux systèmes d'être installés dans les bureaux, tout en stockant tous les fichiers utilisateur dans un emplacement central. Certaines fonctions du service NFS, telles que l'option `-nosuid` de la commande `mount` peuvent être utilisées pour interdire l'ouverture des périphériques et systèmes de fichiers par des utilisateurs non autorisés.

Le service NFS utilise le RPC sécurisé afin d'authentifier les utilisateurs adressant des demandes sur le réseau. Ce processus est appelé *NFS sécurisé*. Le mécanisme d'authentification Diffie-Hellman `AUTH_DH` utilise des fonctions de chiffrement DES pour garantir un accès autorisé. Le mécanisme `AUTH_DH` est également appelé `AUTH_DES`. Pour plus d'informations, reportez-vous aux références suivantes :

- Pour configurer et administrer le service NFS sécurisé, reportez-vous à la section "Administration du système Secure NFS" du *Guide d'administration système : Services réseau*.
- Pour configurer les tables NIS+ et entrer des noms dans la table `cred`, reportez-vous à la section *System Administration Guide: Naming and Directory Services (NIS+)* .
- Pour une présentation des transactions impliquées dans l'authentification RPC, reportez-vous à la section "Mise en œuvre de l'authentification Diffie-Hellman " à la page 329.

Chiffrement DES avec NFS sécurisé

Les fonctions de chiffrement Data Encryption Standard (DES) utilisent une clé 56 bits pour chiffrer les données. Si deux utilisateurs identifiés ou principaux disposent de la même clé DES, ils peuvent communiquer en privé à l'aide de la clé pour chiffrer et déchiffrer du texte. DES est un mécanisme de chiffrement relativement rapide. Une puce DES accélère encore le chiffrement. Toutefois, si la puce est absente, elle est remplacée par une mise en œuvre logicielle.

Le risque lié à l'utilisation de la clé DES uniquement est qu'un intrus puisse recueillir suffisamment de messages texte chiffrés avec la même clé pour être en mesure de découvrir la clé et déchiffrer les messages. C'est pour cette raison que les systèmes de sécurité tels que NFS sécurisé doivent changer de clés fréquemment.

Authentification Kerberos

Kerberos est un système d'authentification développé au MIT. Une partie du chiffrement dans Kerberos est basée sur DES. La prise en charge de Kerberos V4 n'est plus assurée dans le cadre du RPC sécurisé. Cependant, une mise en œuvre côté client et côté serveur de Kerberos V5, qui utilise RPCSEC_GSS, est incluse dans cette version. Pour plus d'informations, reportez-vous au Chapitre 21, "Introduction au service Kerberos".

Authentification Diffie-Hellman et RPC sécurisé

La méthode Diffie-Hellman (DH) d'authentification des utilisateurs se révèle très difficile à déchiffrer pour un intrus. Le client et le serveur disposent chacun de leur clé privée, qu'ils

utilisent avec la clé publique pour créer une clé commune. La clé privée est également appelée *clé secrète*. Le client et le serveur utilisent la clé commune pour communiquer l'un avec l'autre. La clé commune est chiffrée à l'aide d'une fonction de chiffrement convenue, comme par exemple la méthode DES.

L'authentification est basée sur la capacité du système émetteur à utiliser la clé commune pour chiffrer l'heure actuelle. Le système récepteur peut ensuite la déchiffrer et la vérifier par rapport à son heure actuelle. L'heure du client et l'heure du serveur doivent être synchronisées. Pour plus d'informations, reportez-vous à la section "Gestion du protocole NTP (tâches)" du *Guide d'administration système : Services réseau*.

Les clés publiques et privées sont conservées dans une base de données NIS ou NIS+. NIS stocke les clés dans la carte `publickey`. NIS+ stocke les clés dans la table `cred` . Ces fichiers contiennent la clé publique et la clé privée pour tous les utilisateurs potentiels.

L'administrateur système est responsable du paramétrage des cartes NIS ou tables NIS+ et de la génération d'une clé publique et d'une clé privée pour chaque utilisateur. La clé privée est stockée sous forme chiffrée avec le mot de passe de l'utilisateur. Du fait de ce processus, la clé privée n'est connue que de l'utilisateur.

Mise en œuvre de l'authentification Diffie-Hellman

Cette section décrit la série de transactions dans une session client-serveur utilisant la méthode d'authentification Diffie-Hellman (`AUTH__DH`).

Génération de clés publiques et de clés secrètes pour le RPC sécurisé

Avant une transaction, l'administrateur exécute la commande `newkey` ou `nisaddcred` pour générer une clé publique et une clé secrète. . Chaque utilisateur dispose de ses propres clé publique et clé secrète. La clé publique est stockée dans une base de données publique. La clé secrète est stockée sous forme chiffrée dans la même base de données. La commande `chkey` modifie la paire de clés.

Exécution de la commande keylogin pour le RPC sécurisé

Normalement, le mot de passe de connexion est identique au mot de passe du RPC sécurisé. Dans ce cas, la commande `keylogin` n'est pas requise. Toutefois, si les mots de passe sont différents, les utilisateurs doivent se connecter, puis exécuter la commande `keylogin`.

La commande `keylogin` invite l'utilisateur à indiquer son mot de passe de RPC sécurisé. La commande utilise ensuite le mot de passe pour déchiffrer la clé secrète. La commande `keylogin` transmet ensuite la clé secrète déchiffrée au programme du *serveur de clés*. Le serveur de clés est un service RPC avec une instance locale sur chaque ordinateur. Le serveur de clés enregistre la clé secrète déchiffrée et attend que l'utilisateur lance une transaction de RPC sécurisé avec un serveur.

Si le mot de passe de connexion et le mot de passe RPC sont identiques, le processus de connexion transmet la clé secrète au serveur de clés. Si les mots de passe doivent être différents, l'utilisateur doit toujours exécuter la commande `keylogin`. Lorsque la commande `keylogin` est incluse dans le fichier de configuration d'environnement de l'utilisateur, tels que le fichier `~/.login`, `~/.cshrc` ou `~/.profile`, la commande `keylogin` s'exécute automatiquement chaque fois que l'utilisateur se connecte.

Génération de la clé de conversation pour le RPC sécurisé

Lorsque l'utilisateur lance une transaction avec un serveur, les événements suivants se produisent :

1. Le serveur de clés génère une clé de conversation de manière aléatoire.
2. Le noyau utilise la clé de conversation, ainsi que d'autres matériaux, pour chiffrer l'horodatage du client.
3. Le serveur de clés recherche la clé publique du serveur dans la base de données des clés publiques. Pour plus d'informations, reportez-vous à la page de manuel `publickey(4)`.
4. Le serveur de clés utilise la clé secrète du client et la clé publique du serveur pour générer une clé commune.
5. Le serveur de clés chiffre la clé de conversation avec la clé commune.

Connexion initiale au serveur dans le RPC sécurisé

La transmission, qui inclut l'horodatage chiffré et la clé de conversation chiffrée, est ensuite envoyée au serveur. La transmission comprend également des informations d'identification et un vérificateur. L'information d'identification contient trois composants :

- Le nom de réseau du client
- La clé de conversation chiffrée à l'aide de la clé commune
- Une "fenêtre" chiffrée à l'aide de la clé de conversation

La fenêtre correspond à la différence de temps qui doit être autorisée selon le client entre l'horloge du serveur et l'horodatage du client. Si la différence entre l'horloge du serveur et l'horodatage est supérieure à la fenêtre, le serveur rejette la demande du client. Dans des circonstances normales, ce rejet ne se produit pas, car le client se synchronise d'abord avec le serveur avant de commencer la session RPC.

Le vérificateur du client contient les éléments suivants :

- L'horodatage chiffré
- Un vérificateur chiffré de la fenêtre spécifiée, décrémenté de 1.

Le vérificateur de fenêtre est requis au cas où quelqu'un tenterait d'usurper l'identité d'un utilisateur. L'usurpateur peut écrire un programme qui, au lieu de remplir les champs chiffrés avec les informations d'identification et le vérificateur, insère simplement des bits aléatoires. Le

serveur déchiffre la clé de conversation dans une clé aléatoire. Le serveur utilise ensuite la clé pour tenter de déchiffrer la fenêtre et l'horodatage. Il en résulte des nombres aléatoires. Cependant, après quelques milliers d'essais, la paire fenêtre/horodatage aléatoire est susceptible de passer le système d'authentification. Le vérificateur de fenêtre réduit les risques que des informations d'identification fausses puissent être authentifiées.

Déchiffrement de la clé de conversation dans le RPC sécurisé

Lorsque le serveur reçoit la transmission du client, les événements suivants se produisent :

1. Le serveur de clés qui est local pour le serveur recherche la clé publique du client dans la base de données de clés publiques.
2. Le serveur de clés utilise la clé publique du client et la clé secrète du serveur pour en déduire la clé commune. La clé commune est identique à celle calculée par le client. Seul le serveur et le client peuvent calculer la clé commune car le calcul nécessite de connaître l'une des clés secrètes.
3. Le noyau utilise la clé commune pour déchiffrer la clé de conversation.
4. Le noyau appelle le serveur de clés pour déchiffrer l'horodatage du client à l'aide de la clé de conversation déchiffrée.

Stockage d'informations sur le serveur dans le RPC sécurisé

Une fois l'horodatage du client déchiffré par le serveur, ce dernier enregistre quatre éléments d'informations dans une table des informations d'identification :

- Le nom d'ordinateur du client
- La clé de conversation
- La fenêtre
- L'horodatage du client

Le serveur enregistre les trois premiers éléments pour une utilisation ultérieure. Le serveur enregistre l'horodatage du client pour empêcher toute rediffusion. Le serveur accepte uniquement les horodatages qui sont postérieurs au dernier horodatage vu. Par conséquent, les transactions rediffusées sont garanties d'être rejetées.

Remarque – Dans ces transactions, le nom de l'appelant, qui doit être authentifié d'une manière ou d'une autre, est implicite. Le serveur de clés ne peut pas utiliser l'authentification DES afin d'authentifier l'appelant car l'utilisation de DES par le serveur de clés pourrait générer un interblocage. Pour éviter tout interblocage, le serveur de clés stocke les clés secrètes par ID utilisateur (UID) et attribue des requêtes uniquement aux processus `root` locaux.

Renvoi du vérificateur au client dans le RPC sécurisé

Le serveur renvoie un vérificateur au client incluant les éléments suivants :

- L'ID d'index, qui est enregistré par le serveur dans son cache des informations d'identification
- L'horodatage du client moins 1, qui est chiffré à l'aide de la clé de conversation

La soustraction de 1 à l'horodatage du client permet de garantir que l'horodatage est obsolète Un horodatage obsolète ne peut pas être réutilisé comme vérificateur de client.

Authentification du serveur dans le RPC sécurisé

Le client reçoit le vérificateur et authentifie le serveur. Le client sait que seul le serveur peut avoir envoyé le vérificateur car le serveur est le seul à connaître l'horodatage envoyé par le client.

Traitement des transactions dans le RPC sécurisé

Avec chaque transaction survenant après la première transaction, le client renvoie l'ID d'index au serveur dans sa prochaine transaction. Le client envoie également un autre horodatage chiffré. Le serveur renvoie l'horodatage du client moins 1, chiffré par la clé de conversation.

Administration du RPC sécurisé (liste des tâches)

La liste des tâches suivante présente les procédures de configuration du RPC sécurisé pour NIS, NIS+ et NFS.

Tâche	Description	Voir
1. Démarrage du serveur de clés.	Permet de s'assurer que des clés peuvent être créées, de sorte que les utilisateurs peuvent être authentifiés.	“Redémarrage du serveur de clé RPC sécurisé” à la page 333
2. Définition des informations d'identification sur un hôte NIS+.	Permet de s'assurer que l'utilisateur `root` sur un hôte peut être authentifié dans un environnement NIS+.	“Configuration d'une clé Diffie-Hellman pour un hôte NIS+ ” à la page 333
3. Attribution d'une clé à un utilisateur NIS+.	Permet à un utilisateur d'être authentifié dans un environnement NIS+.	“Configuration d'une clé Diffie-Hellman Key pour un utilisateur NIS+ ” à la page 335
4. Définition des informations d'identification sur un hôte NIS.	Permet de s'assurer que l'utilisateur `root` sur un hôte peut être authentifié dans un environnement NIS.	“Configuration d'une clé Diffie-Hellman pour un hôte NIS” à la page 336

Tâche	Description	Voir
5. Attribution d'une clé à un utilisateur NIS.	Permet à un utilisateur d'être authentifié dans un environnement NIS.	“Configuration d'une clé Diffie-Hellman Key pour un utilisateur NIS ” à la page 336
6. Partage de fichiers NFS avec authentification.	Permet à un serveur NFS de protéger en toute sécurité des systèmes de fichiers partagés à l'aide de l'authentification.	“Partage de fichiers NFS avec l'authentification Diffie-Hellman ” à la page 338

Administration de l'authentification avec le RPC sécurisé (tâches)

En requérant l'authentification pour l'utilisation des systèmes de fichiers NFS montés, vous augmentez la sécurité de votre réseau.

▼ Redémarrage du serveur de clé RPC sécurisé

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Vérifiez que le démon `keyserv` est en cours d'exécution.**

```
# svcs \*keyserv\*
STATE    STIME   FMRI
disabled Dec_14  svc:/network/rpc/keyserv
```

3 **Activez le service du serveur de clés si le service n'est pas en ligne.**

```
# svcadm enable network/rpc/keyserv
```

▼ Configuration d'une clé Diffie-Hellman pour un hôte NIS+

Cette procédure doit être effectuée sur chaque hôte du domaine NIS+. Une fois que `root` a exécuté la commande `keylogin`, le serveur dispose d'informations d'identification de l'accepteur GSS-API pour `mech_dh` et le client dispose d'informations d'identification de l'initiateur GSS-API.

Pour une description détaillée de la sécurité NIS+, reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)*.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Activez la table `publickey` dans le service de nommage.**

   Ajoutez la ligne suivante au fichier `/etc/nsswitch.conf` :

   ```
   publickey: nisplus
   ```

3. **Initialisez le client NIS+.**

   ```
   # nisinit -cH hostname
   ```

   où *hostname* est le nom d'un serveur NIS+ de confiance qui contient une entrée dans ses tables pour le système client.

4. **Ajoutez le client à la table `cred`.**

   Saisissez les commandes suivantes :

   ```
   # nisaddcred local
   # nisaddcred des
   ```

5. **Vérifiez la configuration à l'aide de la commande `keylogin`.**

   Si vous êtes invité à saisir un mot de passe, la procédure s'est correctement exécutée.

   ```
   # keylogin
   Password:
   ```

Exemple 16–1 Configuration d'une nouvelle clé pour `root` sur un client NIS+

L'exemple suivant utilise l'hôte `pluto` pour configurer `earth` en tant que client NIS+. Vous pouvez ignorer les avertissements. La commande `keylogin` est acceptée, la vérification que `earth` est correctement configuré en tant que client NIS+ sécurisé est en cours.

```
# nisinit -cH pluto
NIS Server/Client setup utility.
This system is in the example.com. directory.
Setting up NIS+ client ...
All done.
# nisaddcred local
# nisaddcred des
DES principal name : unix.earth@example.com
Adding new key for unix.earth@example.com (earth.example.com.)
Network password:    <Type password>
Warning, password differs from login password.
Retype password:     <Retype password>
# keylogin
Password:            <Type password>
#
```

▼ Configuration d'une clé Diffie-Hellman Key pour un utilisateur NIS+

Cette procédure doit être effectuée sur chaque utilisateur du domaine NIS+.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Ajoutez des utilisateurs à la table `cred` sur un serveur maître root.**

   Saisissez la commande suivante :

   `# nisaddcred -p unix.`*UID*`@`*domain-name* **`-P`** *username*`.`*domain-name*`.` **`des`**

   Notez que, dans ce cas, *username.domain-name* doit se terminer par un point (.).

3. **Vérifiez la configuration en vous connectant en tant que client et en saisissant la commande `keylogin`.**

Exemple 16–2 Configuration d'une nouvelle clé pour un utilisateur NIS+

Dans l'exemple suivant, une clé pour l'authentification Diffie-Hellman est attribuée à l'utilisateur `jdoe`.

```
# nisaddcred -p unix.1234@example.com -P jdoe.example.com. des
DES principal name : unix.1234@example.com
Adding new key for unix.1234@example.com (jdoe.example.com.)
Password:           <Type password>
Retype password:    <Retype password>
# rlogin rootmaster -l jdoe
% keylogin
Password:           <Type password>
%
```

▼ Configuration d'une clé Diffie-Hellman pour un hôte NIS

Cette procédure doit être effectuée sur chaque hôte du domaine NIS.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Activez la carte `publickey` dans le service de nommage.**

Ajoutez la ligne suivante au fichier `/etc/nsswitch.conf` :

```
publickey: nis
```

3 **Créez une nouvelle paire de clés à l'aide de la commande `newkey`.**

```
# newkey -h hostname
```

où *hostname* est le nom du client.

Exemple 16–3 Configuration d'une nouvelle clé pour `root` sur un client NIS

Dans l'exemple ci-dessous, `earth` est configuré en tant que client NIS sécurisé.

```
# newkey -h earth
Adding new key for unix.earth@example.com
New Password:       <Type password>
Retype password:    <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

▼ Configuration d'une clé Diffie-Hellman Key pour un utilisateur NIS

Cette procédure doit être effectuée sur chaque utilisateur du domaine NIS.

Avant de commencer Seuls les administrateurs système, lorsqu'ils sont connectés au serveur maître NIS, peuvent générer une nouvelle clé pour un utilisateur.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Créez une nouvelle clé pour un utilisateur.**

   ```
   # newkey -u username
   ```

   où *username* correspond au nom de l' utilisateur. Le système vous invite à saisir un mot de passe. Vous pouvez saisir un mot de passe générique. La clé privée est stockée sous forme chiffrée à l'aide du mot de passe générique.

3. **Indiquez à l'utilisateur de se connecter et de saisir la commande `chkey -p`.**

   Cette commande permet aux utilisateurs de re-chiffrer leurs clés privées avec un mot de passe uniquement connu de l'utilisateur.

Remarque – La commande `chkey` peut être utilisée pour créer une nouvelle paire de clés pour un utilisateur.

Exemple 16–4 Configuration et chiffrement d'une nouvelle clé utilisateur dans NIS

Dans cet exemple, le superutilisateur définit la clé.

```
# newkey -u jdoe
Adding new key for unix.12345@example.com
New Password:       <Type password>
Retype password:    <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

L'utilisateur `jdoe` re-chiffre la clé à l'aide d'un mot de passe privé.

```
% chkey -p
Updating nis publickey database.
Reencrypting key for unix.12345@example.com
Please enter the Secure-RPC password for jdoe:    <Type password>
Please enter the login password for jdoe:         <Type password>
Sending key change request to centralexample...
```

▼ Partage de fichiers NFS avec l'authentification Diffie-Hellman

Cette procédure protège les systèmes de fichiers partagés sur un serveur NFS en requérant l'authentification pour l'accès.

Avant de commencer

L'authentification par clé publique Diffie-Hellman doit être activée sur le réseau. Pour activer l'authentification sur le réseau, effectuez l'une des opérations suivantes :

- “Configuration d'une clé Diffie-Hellman pour un hôte NIS+ ” à la page 333
- “Configuration d'une clé Diffie-Hellman pour un hôte NIS” à la page 336

1 Connectez-vous en tant que superutilisateur ou prenez un rôle incluant le profil de gestion du système de fichiers.

Le rôle d'administrateur système inclut le profil de gestion du système de fichiers. Pour créer le rôle et l'attribuer à un utilisateur, reportez-vous à la section “Configuration de RBAC (liste des tâches)” à la page 208.

2 Sur le serveur NFS, partagez un système de fichiers avec l'authentification Diffie-Hellman..

```
# share -F nfs -o sec=dh /filesystem
```

où *filesystem* est le système de fichiers partagé.

L'option `-o sec=dh` signifie que l'authentification `AUTH_DH` est désormais requise pour accéder au système de fichiers.

3 Sur un client NFS, montez un système de fichiers avec l'authentification Diffie-Hellman.

```
# mount -F nfs -o sec=dh server:filesystem mount-point
```

server	Nom du système qui partage *filesystem*
filesystem	Nom du système de fichiers partagé, tel que `opt`
mount-point	Nom du point de montage, tel que `/opt`

L'option `-o sec=dh` permet de monter le système de fichiers avec l'authentification `AUTH_DH`.

◆ ◆ ◆ CHAPITRE 17

Utilisation de PAM

Ce chapitre traite de la structure PAM (Pluggable Authentication Module, module d'authentification enfichable). PAM fournit une méthode pour "enficher" des services d'authentification dans le SE Oracle Solaris. PAM permet la prise en charge de plusieurs services d'authentification lors de l'accès à un système.

PAM (présentation)

La structure PAM (Pluggable Authentication Module, module d'authentification enfichable) permet "d'enficher" de nouveaux services d'authentification sans modifier les services de saisie système tels que `login`, `ftp` et `telnet`. Vous pouvez également utiliser PAM pour intégrer la connexion UNIX à d'autres mécanismes de sécurité tels que Kerberos. Des mécanismes de compte, d'informations d'identification, de session et de gestion des mots de passe peuvent également être "enfichés" grâce à cette structure.

Avantages de l'utilisation de PAM

La structure PAM permet de configurer l'utilisation des services de saisie système (tels que `ftp`, `login`, `telnet` ou `rsh`) pour authentifier l'utilisateur. La liste ci-dessous répertorie les avantages principaux de PAM :

- Flexibilité de la stratégie de configuration
  - Stratégie d'authentification par application
  - Possibilité de choisir un mécanisme d'authentification par défaut
  - Possibilité de demander plusieurs autorisations sur les systèmes haute sécurité
- Facilité d'utilisation pour l'utilisateur final

  - Pas de nouvelle saisie des mots de passe s'ils ne varient pas d'un service d'authentification à l'autre
  - Possibilité d'inviter l'utilisateur à saisir des mots de passe pour plusieurs services d'authentification sans qu'il ait à taper plusieurs commandes
- Possibilité de transmettre des options facultatives aux services d'authentification des utilisateurs
- Possibilité de mettre en place une stratégie de sécurité spécifique au site sans avoir à modifier les services de saisie système

Présentation de la structure PAM

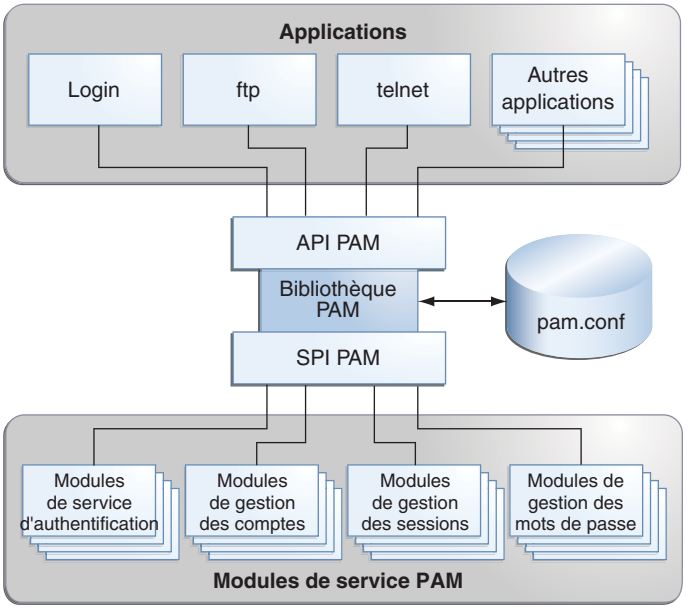
La structure PAM s'organise autour de quatre composants :

- Consommateurs PAM
- Bibliothèque PAM
- Fichier de configuration `pam.conf(4)`
- Modules de service PAM, également appelés fournisseurs

La structure permet d'uniformiser les activités liées à l'authentification. Cette approche permet aux développeurs d'applications d'utiliser les services PAM sans connaissance préalable de la sémantique de la stratégie. Les algorithmes sont fournis de manière centralisée. Ils peuvent être modifiés indépendamment de chaque application. Grâce à PAM, les administrateurs peuvent adapter le processus d'authentification aux besoins d'un système particulier sans avoir à modifier aucune application. Les ajustements sont effectués par le biais du fichier de configuration PAM `pam.conf`.

La figure ci-dessous illustre l'architecture PAM. Les applications communiquent avec la bibliothèque PAM par l'intermédiaire de l'API (Application Programming Interface, interface de programmation d'application) PAM. Les modules PAM communiquent avec la bibliothèque PAM par l'intermédiaire de la SPI (Service Provider Interface, interface de fournisseur de services) PAM. Ainsi, la bibliothèque PAM permet aux applications et modules de communiquer entre eux.

FIGURE 17–1 Architecture PAM



Modifications apportées à PAM pour la version de Solaris10

La version Solaris10 inclut les modifications apportées à la structure PAM (Pluggable Authentication Module, module d'authentification enfichable) :

- Le module `pam_authtok_check` permet maintenant une vérification stricte des mots de passe à l'aide de nouveaux paramètres réglables dans le fichier `/etc/default/passwd`. Les nouveaux paramètres définissent les éléments suivants :
  - une liste de fichiers dictionnaire dont les valeurs sont séparées par des virgules, utilisée pour vérifier les noms communs dans un mot de passe ;
  - les différences minimales requises entre un nouveau mot de passe et un ancien ;
  - le nombre minimal de caractères alphabétiques ou non alphabétiques devant être employés dans un nouveau mot de passe ;
  - le nombre minimal de lettres majuscules et minuscules devant être utilisées dans un nouveau mot de passe ;
  - le nombre de caractères répétés de manière consécutive autorisés ;

- Le module `pam_unix_auth` met en œuvre le verrouillage des comptes pour les utilisateurs locaux. Le verrouillage des comptes est activé par le paramètre `LOCK_AFTER_RETRIES` dans le fichier `/etc/security/policy.conf` et par la clé `lock_after-retries` dans le fichier `/etc/user_attr`. Pour plus d'informations, reportez-vous aux pages de manuel `policy.conf(4)` et `user_attr(4)`.
- Un nouvel indicateur de contrôle `binding` a été défini. Cet indicateur de contrôle est décrit dans la page de manuel `pam.conf(4)` et à la section "Fonctionnement de la superposition PAM" à la page 347.
- Le module `pam_unix` a été supprimé et remplacé par un ensemble de modules de service de fonctionnalité équivalente ou supérieure. Un grand nombre de ces modules ont été introduits dans la version Solaris 9. En voici la liste :
  - `pam_authtok_check`
  - `pam_authtok_get`
  - `pam_authtok_store`
  - `pam_dhkeys`
  - `pam_passwd_auth`
  - `pam_unix_account`
  - `pam_unix_auth`
  - `pam_unix_cred`
  - `pam_unix_session`
- La fonctionnalité du module `pam_unix_auth` a été répartie en deux modules. Le module `pam_unix_auth` vérifie maintenant l'exactitude du mot de passe de l'utilisateur. Le nouveau module `pam_unix_cred` fournit les fonctions qui permettent de définir les informations d'identification de l'utilisateur.
- Des ajouts ont été apportés au module `pam_krb5` pour gérer le cache des informations d'identification de Kerberos à l'aide de la structure PAM.
- Le nouveau module `pam_deny` a été ajouté. Il permet de refuser l'accès à des services. Par défaut, le module `pam_deny` n'est pas utilisé. Pour plus d'informations, reportez-vous à la page de manuel `pam_deny(5)`.

PAM (tâches)

Cette section examine certaines tâches qui peuvent être nécessaires pour que la structure PAM utilise une stratégie de sécurité spécifique. Sachez que certains problèmes de sécurité sont associés au fichier de configuration PAM. Pour plus d'informations sur les problèmes de sécurité, reportez-vous à la section "Planification de la mise en œuvre PAM " à la page 343.

PAM (liste des tâches)

Tâche	Description	Voir
Planification de l'installation PAM	Avant de procéder à la configuration du logiciel, vous devez examiner les problèmes qu'elle risque de poser et prendre les décisions qui s'imposent.	"Planification de la mise en œuvre PAM " à la page 343
Ajout de nouveaux modules PAM	Parfois, des modules spécifiques au site doivent être écrits et installés en fonction d'exigences qui ne relèvent pas du logiciel générique. Cette procédure explique comment installer ces nouveaux modules PAM.	"Ajout d'un module PAM" à la page 344
Blocage de l'accès via `~/.rhosts`	Renforcez la sécurité en interdisant l'accès via `~/.rhosts` .	"Comment empêcher l'accès rhost à partir de systèmes distants avec PAM" à la page 345
Initialisation de la journalisation des erreurs	Démarrez la journalisation des messages d'erreur PAM via `syslog`.	"Journalisation de rapports d'erreur PAM" à la page 345

Planification de la mise en œuvre PAM

Tel qu'il est livré, le fichier de configuration `pam.conf` met en œuvre la stratégie de sécurité standard. Cette stratégie doit fonctionner dans de nombreuses situations. Si vous avez besoin d'appliquer une stratégie de sécurité différente, prenez en compte les points suivants :

- Identifiez vos besoins, en particulier les modules de service PAM que vous devez sélectionner.
- Identifiez les services qui nécessitent une configuration spéciale. Utilisez `other`, si nécessaire.
- Décidez de l'ordre d'exécution des modules.
- Sélectionnez l'indicateur de contrôle pour chaque module. Pour plus d'informations sur tous les indicateurs de contrôle, reportez-vous à la section "Fonctionnement de la superposition PAM" à la page 347.
- Choisissez les options nécessaires pour chaque module. La page de manuel pour chaque module doit répertorier toutes les options spéciales.

Voici quelques suggestions à prendre en compte avant de modifier le fichier de configuration PAM :

- Utilisez les entrées `other` pour chaque type de module afin de ne pas devoir inclure chaque application dans le fichier `/etc/pam.conf`.
- Veillez à prendre en compte les implications en matière de sécurité des indicateurs de contrôle `bind`, `sufficient` et `optional`.

- Prenez connaissance des pages de manuel associées aux modules. Elles peuvent vous aider à mieux comprendre le fonctionnement de chaque module, la disponibilité des options et les interactions entre modules empilés.

Attention – Si le fichier de configuration PAM est mal configuré ou corrompu, aucun utilisateur n'est en mesure de se connecter. Étant donné que la commande `sulogin` n'utilise pas PAM, le mot de passe root est alors nécessaire pour initialiser la machine en mode monoutilisateur et résoudre le problème.

Une fois le fichier `/etc/pam.conf` modifié, révisez-le autant que possible tant que votre accès au système vous permet de résoudre les problèmes. Testez toutes les commandes sur lesquelles vos modifications ont peut-être eu une incidence. Si vous ajoutez par exemple un module au service `telnet`, vous devez utiliser la commande `telnet` et vérifier que le service se comporte comme attendu, suite à vos modifications.

▼ Ajout d'un module PAM

Cette procédure indique comment ajouter un nouveau module PAM. Vous pouvez créer des modules pour prendre en charge des applications tierces ou des stratégies de sécurité spécifiques à votre site.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2. **Déterminez les indicateurs de contrôle et les autres options à utiliser.**

   Pour plus d'informations sur les indicateurs de contrôle, reportez-vous à la section "Fonctionnement de la superposition PAM" à la page 347.

3. **Assurez-vous que la propriété et les autorisations sont définies de telle sorte que le fichier de module appartienne à `root` et les droits soient `555`.**

4. **Modifiez le fichier de configuration PAM, `/etc/pam.conf` , et ajoutez ce module aux services appropriés.**

5. **Vérifiez que le module a été ajouté correctement.**

   Vous devez réaliser le test *avant* la réinitialisation du système au cas où le fichier de configuration serait mal configuré. Connectez-vous à l'aide d'un service direct, tel que `ssh`, et exécutez la commande `su` avant de redémarrer le système. Le service peut être un démon généré dynamiquement une seule fois lors de l'initialisation du système. Vous devez ensuite redémarrer le système avant de vérifier l'ajout du module.

▼ Comment empêcher l'accès rhost à partir de systèmes distants avec PAM

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 **Supprimez toutes les lignes comportant `rhosts_auth.so.1` dans le fichier de configuration PAM.**

Cette étape permet d'éviter la lecture des fichiers `~/.rhosts` au cours d'une session `rlogin`. Par conséquent, elle permet d'empêcher l'accès non authentifié au système local à partir de systèmes distants. Tous les accès `rlogin` requièrent un mot de passe, indépendamment de la présence ou du contenu des fichiers `~/.rhosts` ou `/etc/hosts.equiv` .

3 **Désactivez le service `rsh`.**

Pour empêcher d'autres accès non authentifiés aux fichiers `~/.rhosts`, n'oubliez pas de désactiver le service `rsh`.

```
# svcadm disable network/shell
```

▼ Journalisation de rapports d'erreur PAM

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 **Configurez le fichier `/etc/syslog.conf` en fonction du niveau de journalisation dont vous avez besoin.**

Pour plus d'informations sur les niveaux de journalisation, reportez-vous à `syslog.conf(4)`.

3 **Actualisez les informations de configuration pour le démon `syslog`.**

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

Configuration PAM (référence)

Le fichier de configuration PAM, `pam.conf(4)`, permet de configurer les modules du service PAM pour les services de système `login`, `rlogin`, `su` et `cron`. Il incombe à l'administrateur système de gérer ce fichier. Un ordre d'entrée incorrect dans le fichier `pam.conf` peut entraîner des effets secondaires imprévus. Par exemple, un fichier `pam.conf` mal configuré peut verrouiller les utilisateurs, de manière que le mode monoutilisateur s'impose pour effectuer des réparations. La section "Fonctionnement de la superposition PAM" à la page 347 décrit comment définir l'ordre.

Syntaxe du fichier de configuration PAM

Le format des entrées du fichier de configuration est le suivant :

service-name module-type control-flag module-path module-options

service-name — Nom du service, par exemple, `ftp`, `login` ou `passwd`. Une application peut utiliser différents noms pour les services offerts par l'application. Par exemple, le démon shell sécurisé Oracle Solaris utilise les noms de services suivants : `sshd-none`, `sshd-password`, `sshd-kbdint`, `sshd-pubkey` et `sshd-hostbased`. Le nom de service *other* est un nom prédéfini, utilisé comme nom de service générique. Si aucun nom de service spécifique n'est trouvé dans le fichier de configuration, la configuration pour *other* est utilisée.

module-type — Type du service, c'est-à-dire `auth`, `account`, `session` ou `password`.

control-flag — Rôle du module dans la détermination de la valeur intégrée de réussite ou d'échec pour le service. Les indicateurs de contrôle valides sont `binding`, `include`, `optional`, `required`, `requisite` et `sufficient`. Pour plus d'informations sur l'utilisation de ces indicateurs, reportez-vous à la section "Fonctionnement de la superposition PAM" à la page 347.

module-path — Chemin d'accès à l'objet de bibliothèque qui met en œuvre le service. S'il n'est pas absolu, on suppose qu'il est relatif à `/usr/lib/security/$ISA/`. Utilisez la macro dépendante de l'architecture $ISA pour que `libpam` recherche l'architecture spécifique de l'application dans le répertoire.

module-options — Options transmises aux modules de service. Une page de manuel du module décrit les options acceptées par ce module. `nowarn` et `debug` sont deux options de module typiques.

Fonctionnement de la superposition PAM

Lorsqu'une application appelle les fonctions suivantes, `libpam` lit le fichier de configuration `/etc/pam.conf` pour identifier les modules qui participent à l'opération pour ce service :

- `pam_authenticate`(3PAM)
- `pam_acct_mgmt`(3PAM)
- `pam_setcred`(3PAM)
- `pam_open_session`(3PAM)
- `pam_close_session`(3PAM)
- `pam_chauthtok`(3PAM)

Si `/etc/pam.conf` ne contient qu'un seul module pour une opération pour ce service (authentification ou gestion de compte, par exemple), le résultat de ce module détermine celui de l'opération. Par exemple, l'opération d'authentification par défaut pour l'application `passwd` contient un module, `pam_passwd_auth.so.1` :

```
passwd  auth required           pam_passwd_auth.so.1
```

D'autre part, si plusieurs modules sont définis pour l'opération du service, on parle de modules *empilés* et d'une *pile PAM* pour ce service. Par exemple, prenons le cas où `pam.conf` contient les entrées suivantes :

```
login   auth requisite          pam_authtok_get.so.1
login   auth required           pam_dhkeys.so.1
login   auth required           pam_unix_cred.so.1
login   auth required           pam_unix_auth.so.1
login   auth required           pam_dial_auth.so.1
```

Ces entrées représentent un exemple de pile `auth` pour le service `login`. Pour déterminer le résultat de cette pile, les codes de résultat de chaque module requièrent un *processus d'intégration*. Dans le processus d'intégration, les modules sont exécutés dans l'ordre indiqué par `/etc/pam.conf`. Chaque code de réussite ou d'échec est intégré dans le résultat global en fonction de l'indicateur de contrôle du module. L'indicateur de contrôle peut entraîner la fin anticipée de la pile. Par exemple, un module `requisite` peut échouer, ou un module `sufficient` ou `binding` peut réussir. Une fois la pile traitée, tous les résultats sont regroupés en un résultat global unique, qui est transmis à l'application.

L'indicateur de contrôle précise le rôle joué par le module PAM pour déterminer l'accès au service. Les indicateurs de contrôle ont les effets suivants :

- **Binding** : lorsque les exigences d'un module binding (obligatoire) sont satisfaites, la réussite est immédiatement renvoyée à l'application si aucun module required précédent n'a échoué. Si ces conditions sont vérifiées, aucun autre module n'est exécuté. En cas d'échec, un échec required est enregistré et le traitement des modules se poursuit.
- **Include** : ajoute des lignes d'un autre fichier de configuration PAM à utiliser à ce stade de la pile PAM. Cet indicateur ne contrôle pas les comportements de réussite ni d'échec. Lorsqu'un nouveau fichier est lu, la pile include (inclure) PAM est incrémentée. Au terme de la vérification de la pile dans le nouveau fichier, la valeur de la pile include est décrémentée. Une fois la fin du fichier atteinte et la valeur de la pile include PAM définie sur 0, le traitement de la pile prend fin. La valeur maximale pour la pile include PAM est 32.
- **Optional** : il n'est pas nécessaire que les exigences d'un module optional (facultatif) soient satisfaites pour que le service puisse être utilisé. En cas d'échec, un échec optional est enregistré.
- **Required** : les exigences d'un module required (requis) doivent être satisfaites pour que le service puisse être utilisé. Un échec entraîne le renvoi d'une erreur après l'exécution des modules restants pour ce service. La réussite finale du service n'est renvoyée que si aucun module binding ou required n'a signalé d'échec.
- **Requisite** : les exigences d'un module requisite (indispensable) doivent être satisfaites pour que le service puisse être utilisé. Un échec entraîne le renvoi immédiat d'une erreur et l'arrêt de l'exécution des modules. Tous les modules requisite pour un service doivent renvoyer un résultat positif pour que la fonction puisse renvoyer une réussite à l'application.
- **Sufficient** : si aucun échec required précédent ne s'est produit, la réussite dans un module sufficient (suffisant) renvoie immédiatement un résultat positif à l'application et aucun autre module n'est exécuté. En cas d'échec, un échec optional est enregistré.

Les deux diagrammes suivants indiquent comment l'accès est déterminé lors du processus d'intégration. Le premier diagramme indique comment la réussite ou l'échec sont enregistrés pour chaque type d'indicateur de contrôle. Le second diagramme indique comment la valeur intégrée est déterminée.

FIGURE 17–2 Superposition PAM : effet des indicateurs de contrôle

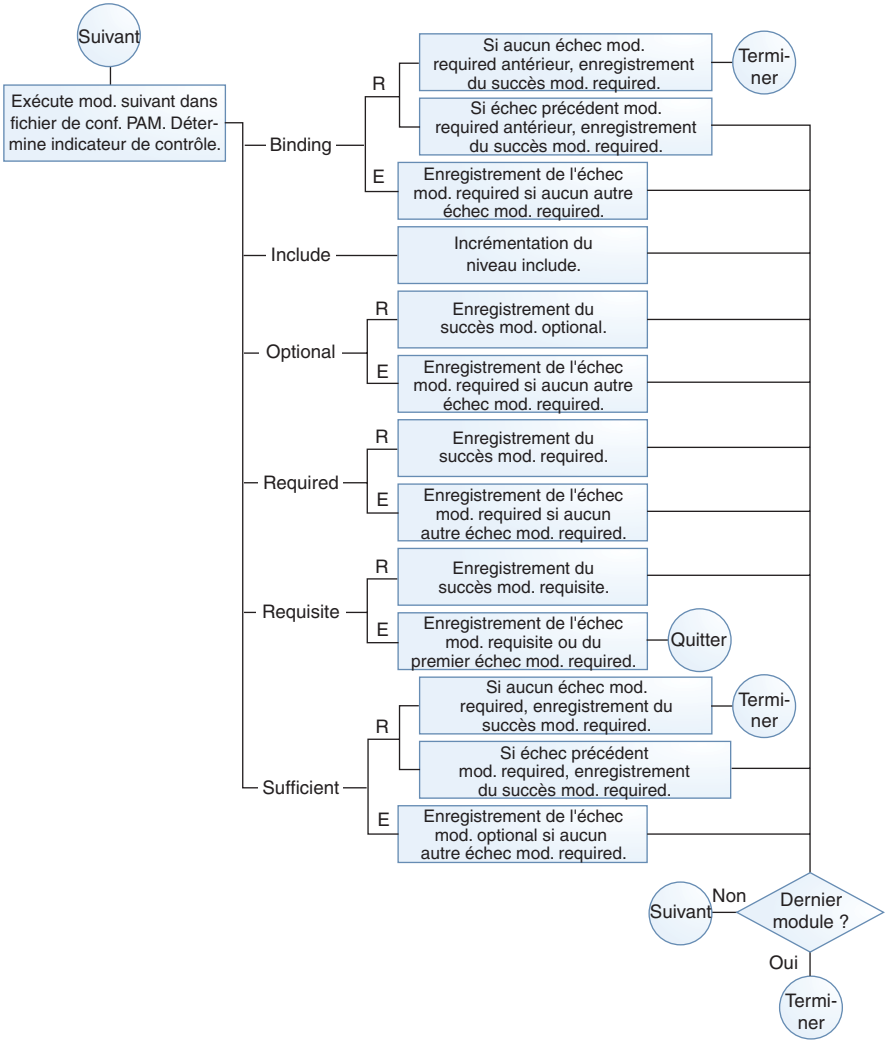
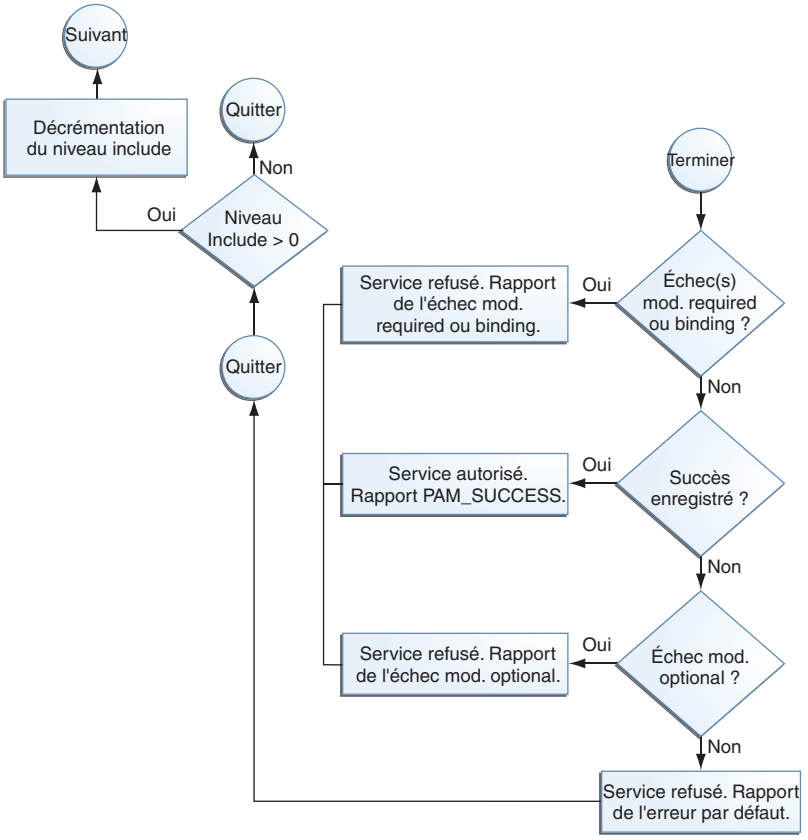


FIGURE 17–3 Superposition PAM : détermination de la valeur intégrée



Exemple de superposition PAM

Examinez l'exemple suivant d'un service `rlogin` qui demande une authentification.

EXEMPLE 17–1 Contenu partiel d'un fichier de configuration PAM standard

Le fichier `pam.conf` dans cet exemple comporte les éléments suivants pour les services `rlogin` :

```
# Authentication management
...
# rlogin service
rlogin  auth sufficient         pam_rhosts_auth.so.1
rlogin  auth requisite          pam_authtok_get.so.1
rlogin  auth required           pam_dhkeys.so.1
rlogin  auth required           pam_unix_auth.so.1
...
```

EXEMPLE 17–1 Contenu partiel d'un fichier de configuration PAM standard *(Suite)*

Lorsque le service `rlogin` demande une authentification, `libpam` exécute d'abord le module `pam_rhosts_auth(5)`. L'indicateur de contrôle est défini sur `sufficient` pour le module `pam_rhosts_auth`. Si le module `pam_rhosts_auth` est en mesure d'authentifier l'utilisateur, le traitement s'arrête et la réussite est renvoyée à l'application.

Si le module `pam_rhosts_auth` n'est pas en mesure d'authentifier l'utilisateur, le module PAM suivant, `pam_authtok_get(5)` est exécuté. L'indicateur de contrôle de ce module est défini sur `requisite`. Si `pam_authtok_get` échoue, le processus d'authentification se termine et l'échec est renvoyé à `rlogin`.

Si `pam_authtok_get` réussit, les deux modules suivants, `pam_dhkeys(5)` et `pam_unix_auth(5)`, sont exécutés. Les indicateurs de contrôle associés des deux modules sont définis sur `required` de sorte que le processus se poursuit même si un échec individuel est renvoyé. Une fois `pam_unix_auth` exécuté, il ne reste plus de modules pour l'authentification `rlogin`. À ce stade, si `pam_dhkeys` ou `pam_unix_auth` a renvoyé un échec, l'accès via `rlogin` est refusé à l'utilisateur.

◆ ◆ ◆ CHAPITRE 18

Utilisation de SASL

Ce chapitre contient des informations sur SASL (Simple Authentication and Security Layer, couche d'authentification et de sécurité simple).

SASL (présentation)

La couche SASL (Simple Authentication and Security Layer) est une structure fournissant des services d'authentification et de sécurité facultatifs aux protocoles réseau. Une application appelle la bibliothèque SASL, `/usr/lib/libsasl.so`, qui fournit une couche de collage entre l'application et les divers mécanismes SASL. Les mécanismes sont utilisés dans le processus d'authentification et lors de la fourniture de services de sécurité facultatifs. La version de SASL est dérivée de la couche Cyrus SASL avec quelques changements.

SASL fournit les services suivants :

- Chargement de plug-ins
- Détermination des options de sécurité nécessaires dans l'application afin de faciliter le choix d'un mécanisme de sécurité
- Liste des plug-ins disponibles pour l'application
- Choix du meilleur mécanisme dans une liste des mécanismes disponibles pour une tentative d'authentification particulière
- Routage des données d'authentification entre l'application et le mécanisme sélectionné
- Renvoi des informations sur la négociation SASL à l'application

SASL (référence)

La section suivante fournit des informations sur l'implémentation de SASL.

Plug-ins SASL

Les plug-ins SASL assurent la prise en charge des mécanismes de sécurité, la normalisation utilisateur et la récupération des propriétés auxiliaires. Par défaut, les plug-ins 32 bits chargés de manière dynamique sont installés dans `/usr/lib/sasl` et les plug-ins 64 bits sont installés dans `/usr/lib/sasl/` *$ISA*. Les plug-ins de mécanismes de sécurité suivants sont fournis :

`crammd5.so.1`	CRAM-MD5, qui prend en charge l'authentification uniquement, et non l'autorisation.
`digestmd5.so.1`	DIGEST-MD5, qui prend en charge l'authentification, l'intégrité et la confidentialité, ainsi que l'autorisation.
`gssapi.so.1`	GSSAPI, qui prend en charge l'authentification, l'intégrité et la confidentialité, ainsi que l'autorisation. Le mécanisme de sécurité GSSAPI requiert une infrastructure Kerberos en état de fonctionnement.
`plain.so.1`	PLAIN, qui prend en charge l'authentification et l'autorisation.

En outre, les plug-ins de mécanismes de sécurité EXTERNES et les plug-ins de normalisation utilisateur INTERNE sont créés dans `libsasl.so.1`. Le mécanisme EXTERNE prend en charge l'authentification et l'autorisation. Le mécanisme prend en charge l'intégrité et la confidentialité si la source de sécurité externe les fournit. Le plug-in INTERNE ajoute le nom de domaine si nécessaire pour le nom d'utilisateur.

Actuellement, la version d'Oracle Solaris ne fournit aucun plug-in `auxprop`. Pour que les plug-ins de mécanismes CRAM-MD5 et DIGEST-MD5 soient entièrement opérationnels côté serveur, l'utilisateur doit fournir un plug-in `auxprop` pour récupérer des mots de passe en clair. Le plug-in PLAIN (en clair) requiert une prise en charge supplémentaire pour vérifier le mot de passe. La prise en charge de la vérification du mot de passe peut se faire à travers l'un des éléments suivants : un rappel à l'application de serveur, un plug-in `auxprop`, `saslauthd` ou `pwcheck`. Les démons `salauthd` et `pwcheck` ne sont pas fournis dans les versions Oracle Solaris. Pour une meilleure interopérabilité, limitez les applications de serveur aux mécanismes qui sont entièrement opérationnel en utilisant l'option SASL `mech_list`.

Variable d'environnement SASL

Par défaut, le nom d'authentification client est défini sur `getenv("LOGNAME")`. Cette variable peut être réinitialisée par le client ou par le plug-in.

Options SASL

Le comportement de `libsasl` et les plug-ins peuvent être modifiés côté serveur à l'aide d'options pouvant être définies dans le fichier `/etc/sasl/`*app*`.conf`. La variable *app* est le nom défini côté serveur pour l'application. La documentation du serveur *app* doit indiquer le nom de l'application.

Les options suivantes sont prises en charge :

`auto_transition`	Effectue la transition automatique de l'utilisateur vers d'autres mécanismes lorsque celui-ci réalise une authentification en texte simple réussie.
`auxprop_login`	Dresse la liste des noms de plug-ins de propriétés auxiliaires à utiliser.
`canon_user_plugin`	Sélectionne le plug-in canon_user à utiliser.
`mech_list`	Dresse la liste des mécanismes autorisés à être utilisés par l'application de serveur.
`pwcheck_method`	Dresse la liste des mécanismes utilisés pour vérifier les mots de passe. Actuellement, `auxprop` est la seule valeur autorisée.
`reauth_timeout`	Définit la durée, en minutes, pendant laquelle les informations d'authentification sont mises en mémoire cache pour une réauthentification rapide. Cette option est utilisée par le plug-in DIGEST-MD5. La définition de cette option sur la valeur 0 désactive la réauthentification.

Les options suivantes ne sont pas prises en charge :

`plugin_list`	Dresse la liste des mécanismes disponibles. Non utilisé, car l'option modifie le comportement de chargement dynamique des plug-ins.
`saslauthd_path`	Définit l'emplacement de la porte saslauthd, qui est utilisée pour la communication avec le démon `saslauthd`. Le démon `saslauthd` n'est pas inclus dans la version Oracle Solaris. Par conséquent, cette option n'est pas incluse non plus.
`keytab`	Définit l'emplacement du fichier `keytab` utilisé par le plug-in GSSAPI. Utilisez à la place la variable d'environnement `KRB5_KTNAME` pour définir l'emplacement `keytab` par défaut.

Les options suivantes ne figurent pas dans Cyrus SASL. Cependant, elles ont été ajoutées dans la version Oracle Solaris :

`use_authid`	Permet d'obtenir les informations d'identification du client plutôt que d'utiliser les informations d'identification par défaut lors de la création du contexte de sécurité client GSS. Par défaut, l'identité Kerberos du client est utilisée.

`log_level` Définit le niveau souhaité de journalisation d'un serveur.

◆ ◆ ◆ CHAPITRE 19

Utilisation d'Oracle Solaris Secure Shell (tâches)

La fonction Secure Shell fournit un accès sécurisé à un hôte distant sur un réseau non sécurisé. Le shell fournit des commandes pour une connexion à distance et le transfert de fichier distant. Vous trouverez ci-après une liste des sujets abordés dans ce chapitre.

Pour obtenir des informations de référence, reportez-vous au Chapitre 20, "Oracle Solaris Secure Shell (référence)". Pour plus d'informations sur la relation entre Oracle Solaris Secure Shell et le projet OpenSSH, reportez-vous à la section "Oracle Solaris Secure Shell et le projet OpenSSH" à la page 360.

Oracle Solaris Secure Shell (présentation)

Avec Secure Shell, l'authentification s'effectue via l'utilisation de mots de passe et/ou de clés publiques. Tout le trafic réseau est chiffré. Par conséquent, Secure Shell empêche tout intrus potentiel de lire une communication interceptée. Secure Shell empêche également un adversaire de mystifier le système.

Secure Shell peut également être utilisé comme un VPN à la demande. Un VPN peut transmettre le trafic système X Window ou connecter des numéros de port individuels compris entre les machines locales et distantes via un lien réseau crypté.

Avec Secure Shell, vous pouvez effectuer les actions suivantes :

- Se connecter de manière sécurisée à un autre hôte sur un réseau non sécurisé.
- Copier des fichiers en toute sécurité entre les deux hôtes.
- Exécuter des commandes en toute sécurité sur l'hôte distant.

Secure Shell prend en charge deux versions du protocole Secure Shell. La version 1 est la version d'origine de ce protocole. La version 2 est plus sécurisée, et règle certaines failles de sécurité de base de la version 1. La version 1 est fournie uniquement pour aider les utilisateurs qui effectuent une migration vers la version 2. Il est vivement déconseillé aux utilisateurs d'utiliser la version 1.

Remarque – Ci-après dans ce texte, v1 est utilisé pour représenter la version 1, et v2 est utilisé pour représenter la version 2.

Authentification Oracle Solaris Secure Shell

Secure Shell fournit des méthodes de clé publique et mot de passe pour l'authentification de la connexion à l'hôte distant. L'authentification avec clé publique est un mécanisme d'authentification plus fiable que l'authentification par mot de passe, car la clé privée ne se déplace pas sur le réseau.

Les méthodes d'authentification sont tentées dans l'ordre suivant. Lorsque la configuration ne satisfait pas à une méthode d'authentification, la méthode suivante est tentée.

- **GSS-API :** utilise les informations d'authentification des mécanismes GSS-API tels que `mech_krb5` (Kerberos V) et `mech_dh` (AUTH_DH) pour authentifier les clients et serveurs. Pour plus d'informations sur GSS-API, reportez-vous à la rubrique "Introduction to GSS-API" du *Developer's Guide to Oracle Solaris Security*.
- **Authentification basée sur l'hôte :** utilise les clés d'hôte et les fichiers rhosts. Utilise les clés d'hôte privées/publiques RSA et DSA du client pour authentifier ce dernier. Utilise les fichiers rhosts pour autoriser les clients à des utilisateurs.
- **Authentification avec clé publique :** authentifie les utilisateurs avec leurs clés publiques et privées RSA et DSA.
- **Authentification du mot de passe :** utilise PAM pour authentifier les utilisateurs. La méthode d'authentification du clavier dans v2 permet l'invitation arbitraire par PAM. Pour plus d'informations, reportez-vous à la section `SECURITY` de la page de manuel `sshd(1M)`.

Le tableau suivant répertorie les conditions requises pour l'authentification d'un utilisateur essayant de se connecter à un hôte distant. L'utilisateur est sur l'hôte local, le client. L'hôte distant, le serveur, exécute le démon `sshd`. Le tableau présente les méthodes d'authentification Secure Shell, les versions de protocole compatibles et les exigences de l'hôte.

TABLEAU 19–1 Méthodes d'authentification pour Secure Shell

Méthode d'authentification (version du protocole)	Exigences de l'hôte local (client)	Exigences de l'hôte distant (serveur)
GSS-API (v2)	Informations d'identification de l'initiateur pour le mécanisme GSS.	Informations d'identification de l'accepteur pour le mécanisme GSS. Pour plus d'informations, reportez-vous à la section "Acquisition d'informations d'identification GSS dans Secure Shell" à la page 381.

Basée sur l'hôte (v2)	Compte utilisateur
	Clé privée de l'hôte local dans `/etc/ssh/ssh_host_rsa_key` ou `/etc/ssh/ssh_host_dsa_key`
	`HostbasedAuthentication yes` dans `/etc/ssh/ssh_config`
		Compte utilisateur
		Clé privée de l'hôte local dans `/etc/ssh/known_hosts` ou `~/.ssh/known_hosts`
		`HostbasedAuthentication yes` dans `/etc/ssh/sshd_config`
		`IgnoreRhosts no` dans `/etc/ssh/sshd_config`
		Entrée d'hôte local dans `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.rhosts` ou `~/.shosts`

Clé publique RSA ou DSA (v2)	Compte utilisateur Clé privée dans `~/.ssh/id_rsa` ou `~/.ssh/id_dsa` Clé publique d'utilisateur dans `~/.ssh/id_rsa.pub` ou `~/.ssh/id_dsa.pub`	Compte utilisateur Clé publique d'utilisateur en `~/.ssh/authorized_keys`
Clé publique RSA (v1)	Compte utilisateur Clé privée dans `~/.ssh/identity` Clé publique d'utilisateur en `~/.ssh/identity.pub`	Compte utilisateur Clé publique d'utilisateur en `~/.ssh/authorized_keys`
Interactive avec clavier (v2)	Compte utilisateur	Compte utilisateur Prend en charge PAM, y compris l'invite arbitraire et le changement de mot de passe lorsque le vieillissement du mot de passe est déclenché.
Basée sur mot de passe (v1 ou v2)	Compte utilisateur	Compte utilisateur Prend en charge PAM.
`.rhosts` uniquement (v1)	Compte utilisateur	Compte utilisateur `IgnoreRhosts no` dans `/etc/ssh/sshd_config` Entrée d'hôte local dans `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.shosts` ou `~/.rhosts`

TABLEAU 19–1 Méthodes d'authentification pour Secure Shell *(Suite)*

Méthode d'authentification (version du protocole)	Exigences de l'hôte local (client)	Exigences de l'hôte distant (serveur)
`.rhosts` avec RSA (v1) sur le serveur uniquement	Compte utilisateur Clé publique de l'hôte local dans `/etc/ssh/ssh_host_rsa1_key`	Compte utilisateur Clé publique de l'hôte local dans `/etc/ssh/ssh_known_hosts` ou `~/.ssh/known_hosts` `IgnoreRhosts no` dans `/etc/ssh/sshd_config` Entrée d'hôte local dans `/etc/ssh/shosts.equiv`, `/etc/hosts.equiv`, `~/.shosts` ou `~/.rhosts`

Secure Shell dans l'entreprise

Pour obtenir des informations complètes sur la fonction Secure Shell sur un système Oracle Solaris, reportez-vous à l'ouvrage *Secure Shell in the Enterprise*, de Jason Reid, ISBN 0-13-142900-0, Juin 2003. Ce manuel fait partie de la série Sun BluePrints publiée par Sun Microsystems Press.

Oracle Solaris Secure Shell et le projet OpenSSH

La fonction Oracle Solaris Secure Shell est un fork du projet OpenSSH (`http://www.openssh.com`). Les correctifs de sécurité pour la correction des vulnérabilités découvertes dans les versions ultérieures d'OpenSSH sont intégrés à Oracle Solaris Secure Shell, tout comme des corrections de bogues et des fonctions. Le développement interne se poursuit sur le fork Oracle Solaris Secure Shell.

En plus des corrections de bogues dans le projet, les ingénieurs Oracle Solaris ont également intégré les fonctionnalités suivantes dans le fork Oracle Solaris de Secure Shell :

- PAM - Oracle Solaris Secure Shell utilise PAM. L'option de configuration `UsePAM` OpenSSH n'est pas prise en charge.
- Séparation des privilèges : Oracle Solaris Secure Shell n'utilise pas le code de séparation des privilèges du projet OpenSSH. Oracle Solaris Secure Shell sépare le traitement de l'audit, de la conservation des enregistrements et de la re-saisie du traitement des protocoles de session.

  Le code de séparation des privilèges Oracle Solaris Secure Shell est toujours actif et ne peut pas être désactivé. L'option OpenSSH `UsePrivilegeSeparation` n'est pas prise en charge.
- Environnement linguistique : Oracle Solaris Secure Shell prend entièrement en charge les langues négociées dans RFC 4253, *Secure Shell Transfer Protocol*. Une fois que l'utilisateur se connecte, le shell de connexion de l'utilisateur peut remplacer les paramètres régionaux négociés avec Secure Shell.

- Audit : Oracle Solaris Secure Shell est totalement intégré au sous-système d'audit Oracle Solaris. Pour plus d'informations sur l'audit, reportez-vous à la Partie VII.
- Prise en charge GSS-API : GSS-API peut être utilisé pour l'authentification des utilisateurs *et* pour l'échange de clé initiale. La fonction GSS-API est définie dans RFC4462, *Generic Security Service Application Program Interface*.
- Commandes proxy : Oracle Solaris Secure Shell fournit les commandes de proxy pour les protocoles SOCKS5 et HTTP. Pour consulter un exemple, reportez-vous à la section "Définition des connexions aux hôtes en dehors du pare-feu " à la page 376.

Depuis la version Solaris 9, les modifications spécifiques suivantes ont été introduites dans Oracle Solaris Secure Shell :

- La fonction Oracle Solaris Secure Shell est clonée d'OpenSSH 3.5p1.
- La valeur par défaut `X11Forwarding` est `yes` dans le fichier `/etc/ssh/sshd_config`.
- Les mots-clés suivants ont été introduits :
  - `GSSAPIAuthentication`
  - `GSSAPIKeyExchange`
  - `GSSAPIDelegateCredentials`
  - `GSSAPIStoreDelegatedCredentials`
  - `KbdInteractiveAuthentication`

  Les mots-clés `GSSAPI` activent Oracle Solaris Secure Shell pour utiliser les informations d'identification GSS pour l'authentification. Le mot-clé `KbdInteractiveAuthentication` prend en charge l'invitation arbitraire et la modification du mot de passe dans PAM. Pour obtenir une liste complète des mots-clés et de leurs valeurs par défaut, reportez-vous à la section "Mots-clés dans Secure Shell" à la page 383.
- Les chiffrements ARCFOUR et AES128-CTR sont désormais disponibles. ARCFOUR est également appelé RC4. Le chiffrement AES est AES en mode de compteur.
- Le démon `sshd` utilise les variables du fichier `/etc/default/login` et la commande `login`. Les variables `etc/default/login` peuvent être remplacées par d'autres valeurs dans le fichier `sshd_config`. Pour plus d'informations, reportez-vous à la section "Secure Shell et les variables d'environnement de connexion" à la page 387 et à la page de manuel `sshd_config(4)`.
- L'option `ChrootDirectory` sur le serveur permet au serveur, une fois que la connexion est authentifiée, d'exécuter `chroot` sur les clients connectés au répertoire spécifié par l'option. Cette option prend en charge un serveur SFTP dans le processus, c'est-à-dire, un SFTP interne, dont les configurations sont simplifiées par l'utilisation de l'option `ChrootDirectory`.

Oracle Solaris Secure Shell (liste des tâches)

La liste des tâches suivante présente les tâches de configuration Secure Shell et d'utilisation de la fonction Secure Shell dans Oracle Solaris.

Tâche	Description	Voir
Configuration de Secure Shell	Guide les administrateurs tout au long de la configuration de Secure Shell pour les utilisateurs.	"Configuration d'Oracle Solaris Secure Shell (liste des tâches) " à la page 362
Utilisez Secure Shell	Aide les utilisateurs à utiliser Secure Shell.	"Utilisation d'Oracle Solaris Secure Shell (liste des tâches) " à la page 367

Configuration d'Oracle Solaris Secure Shell (liste des tâches)

La liste des tâches suivante présente les procédures de configuration de Secure Shell.

Tâche	Description	Voir
Configuration de l'authentification basée sur l'hôte	Configure l'authentification basée sur l'hôte sur le serveur et sur le client.	"Configuration de l'authentification basée sur l'hôte pour Secure Shell " à la page 362
Configuration d'un hôte pour qu'il utilise v1 et v2	Crée des fichiers de clé publique pour les hôtes qui utilisent les protocoles v1 et v2.	"Activation de Secure Shell v1" à la page 365
Configuration du transfert de port	Permet aux utilisateurs d'utiliser le transfert de port.	"Configuration du transfert de port dans Secure Shell " à la page 366

Configuration d'Oracle Solaris Secure Shell (tâches)

Par défaut, l'authentification basée sur l'hôte et l'utilisation des deux protocoles ne sont pas activées dans Secure Shell. La modification de ces valeurs par défaut nécessite une intervention de l'administrateur. L'administrateur doit également intervenir pour que le transfert de port de fonctionne.

▼ Configuration de l'authentification basée sur l'hôte pour Secure Shell

La procédure suivante définit un système de clé publique où la clé publique du client est utilisée pour l'authentification sur le serveur. L'utilisateur doit également créer une paire de clés publiques ou privées.

Dans cette procédure, les termes *client* et *hôte local* désignent la machine sur laquelle un utilisateur saisit la commande `ssh`. Les termes *serveur* et *hôte distant* désignent la machine que le client tente d'atteindre.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Sur le client, activez l'authentification basée sur l'hôte.**

Dans le fichier de configuration du client, `/etc/ssh/ssh_config`, tapez l'entrée suivante :

```
HostbasedAuthentication yes
```

Pour connaître la syntaxe du fichier de configuration, reportez-vous à la page de manuel `ssh_config`(4)

3 **Sur le serveur, activez l'authentification basée sur l'hôte.**

Dans le fichier de configuration du serveur, `/etc/ssh/sshd_config`, saisissez la même entrée :

```
HostbasedAuthentication yes
```

Pour connaître la syntaxe du fichier de configuration, reportez-vous à la page de manuel `sshd_config`(4)

4 **Sur le serveur, vous devez configurer un fichier qui permet au client d'être reconnu en tant qu'hôte de confiance.**

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

- **Ajoutez le client sous la forme d'une entrée pour le fichier `/etc/ssh/shosts.equiv` du serveur.**

  client-host

- **Ou bien, vous pouvez demander aux utilisateurs d'ajouter une entrée pour le client dans leur fichier `~/.shosts` sur le serveur.**

  client-host

5 **Sur le serveur, vérifiez que le démon `sshd` peut accéder à la liste des hôtes de confiance.**

Définissez `IgnoreRhosts` sur `no` dans le fichier `/etc/ssh/sshd_config`.

```
## sshd_config
IgnoreRhosts no
```

6 **Assurez-vous que les utilisateurs de Secure Shell sur votre site possèdent des comptes sur les deux hôtes.**

7 Procédez de l'une des manières suivantes pour placer la clé publique du client sur le serveur.

- **Modifiez le fichier `sshd_config` sur le serveur, puis demandez à vos utilisateurs d'ajouter les clés d'hôte publiques du client à leur fichier `~/.ssh/known_hosts`.**

  ```
  ## sshd_config
  IgnoreUserKnownHosts no
  ```

  Pour des instructions d'utilisation, reportez-vous à la section "Génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell " à la page 367.

- **Copiez la clé publique du client sur le serveur.**

  Les clés d'hôte sont stockées dans le répertoire `/etc/ssh`. Ces clés sont généralement générées par le démon `sshd` au premier démarrage.

  a. **Ajoutez la clé au fichier `/etc/ssh/ssh_known_hosts` sur le serveur.**

     Sur le client, saisissez la commande sur une seule ligne, sans barre oblique inverse.

     ```
     # cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
     'cat >> /etc/ssh/ssh_known_hosts && echo "Host key copied"'
     ```

  b. **Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.**

     Lorsque le fichier est copié, le message "Host key copied" (Clé d'hôte copiée) s'affiche.

     Chaque ligne du fichier `/etc/ssh/ssh_known_hosts` se compose de champs séparés par des espaces :

     hostnames algorithm-name publickey comment

  c. **Modifiez le fichier `/etc/ssh/ssh_known_hosts` et ajoutez *RemoteHost* comme premier champ de l'entrée copiée.**

     ```
     ## /etc/ssh/ssh_known_hosts File
     RemoteHost  <copied entry>
     ```

Exemple 19–1 Configuration de l'authentification basée sur l'hôte

Dans l'exemple ci-dessous, chaque hôte est configuré en tant que serveur et en tant que client. Un utilisateur de l'un ou l'autre hôte peut lancer une connexion `ssh` à l'autre hôte. La configuration suivante convertit chaque hôte en serveur et client :

- Sur chaque hôte, les fichiers de configuration Secure Shell contiennent les entrées suivantes :

  ```
  ## /etc/ssh/ssh_config
  HostBasedAuthentication yes
  #
  ## /etc/ssh/sshd_config
  HostBasedAuthentication yes
  IgnoreRhosts no
  ```

- Sur chaque hôte, le fichier `shosts.equiv` contient une entrée pour l'autre hôte :

```
## /etc/ssh/shosts.equiv on machine2
machine1

## /etc/ssh/shosts.equiv on machine1
machine2
```

- La clé publique pour chaque hôte est dans le fichier `/etc/ssh/ssh_known_hosts` sur l'autre hôte :

```
## /etc/ssh/ssh_known_hosts on machine2
... machine1

## /etc/ssh/ssh_known_hosts on machine1
... machine2
```

- Les utilisateurs ont un compte sur les deux hôtes :

```
## /etc/passwd on machine1
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh

## /etc/passwd on machine2
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh
```

▼ Activation de Secure Shell v1

Cette procédure est utile lorsqu'un hôte interagit avec les hôtes qui exécutent v1 et v2.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Configurez l'hôte pour qu'il utilise les deux protocoles Secure Shell.

Modifier le fichier `/etc/ssh/sshd_config`.

```
# Protocol 2
Protocol 2,1
```

3 Fournissez un fichier distinct pour la clé d'hôte du protocole v1.

Ajouter une entrée `HostKey` au fichier `/etc/ssh/sshd_config`.

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_rsa1_key
```

4 Générez une clé d'hôte pour v1.

```
# ssh-keygen -t rsa1 -f /etc/ssh/ssh_host_rsa1_key -N ''
```

`-t rsa1` Indique l'algorithme RSA pour v1.

`-f` Indique le fichier qui contient la clé d'hôte.

`-N ''` Indique qu'aucune phrase de passe n'est requise.

5 **Redémarrez le démon `sshd`.**

```
# svcadm restart network/ssh:default
```

Vous pouvez également redémarrer le système.

▼ Configuration du transfert de port dans Secure Shell

Le transfert de port permet à un port local d'être transmis à un hôte distant. En réalité, un socket est alloué pour écouter le port côté local. De la même façon, un port peut être spécifié côté distant.

Remarque – Le transfert de port Secure Shell doit utiliser des connexions TCP. Secure Shell ne prend pas en charge les connexions UDP pour le transfert de port.

---

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Configurez une définition Secure Shell sur le serveur distant pour autoriser le transfert de port.**

Définissez la valeur de `AllowTcpForwarding` sur `yes` dans le fichier `/etc/ssh/sshd_config`.

```
# Port forwarding
AllowTcpForwarding yes
```

3 **Redémarrez le service Secure Shell.**

```
remoteHost# svcadm restart network/ssh:default
```

Pour plus d'informations sur la gestion des services persistants, reportez-vous au Chapitre 18, “Gestion des services (présentation) ” du *Guide d'administration système : administration de base* et à la page de manuel `svcadm`(1M).

4 **Vérifiez que le transfert de port peut être utilisé.**

```
remoteHost# /usr/bin/pgrep -lf sshd
 1296 ssh -L 2001:remoteHost:23 remoteHost
```

Utilisation d'Oracle Solaris Secure Shell (liste des tâches)

La liste des tâches suivante présente les procédures d'utilisation de Secure Shell.

Tâche	Description	Voir
Création d'une paire de clés publique/privée	Permet l'accès à Secure Shell pour des sites qui nécessitent une authentification avec clé publique.	"Génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell " à la page 367
Changement de phrase de passe	Change la phrase qui authentifie votre clé privée.	"Modification de la phrase de passe pour une clé privée Secure Shell" à la page 370
Connexion par le biais de Secure Shell	Permet la communication chiffrée Secure Shell lors d'une connexion à distance. Le processus est similaire à l'utilisation de la commande `rsh`.	"Connexion à un hôte distant avec Secure Shell " à la page 370
Connexion à Secure Shell sans mot de passe	Permet la connexion par le biais d'un agent qui fournit votre mot de passe à Secure Shell.	"Réduction des invites de mot de passe dans Secure Shell " à la page 371
		"Configuration de la commande `ssh-agent` pour qu'elle s'exécute automatiquement dans le CDE " à la page 373
Utilisation du transfert de port dans Secure Shell	Spécifie un port local ou un port distant à utiliser pour les connexions Secure Shell via TCP.	"Utilisation du transfert de port dans Secure Shell " à la page 374
Copie de fichiers avec Secure Shell	Copie les fichiers d'un hôte à l'autre en toute sécurité.	"Copie de fichiers avec Secure Shell " à la page 375
Connexion sécurisée à partir d'un hôte à l'intérieur d'un pare-feu sur un hôte à l'extérieur du pare-feu	Utilise les commandes Secure Shell compatibles avec le protocole HTTP ou SOCKS5 pour connecter les hôtes séparés par un pare-feu.	"Définition des connexions aux hôtes en dehors du pare-feu " à la page 376

Utilisation d'Oracle Solaris Secure Shell (tâches)

Secure Shell fournit un accès sécurisé entre un shell local et un shell distant. Pour plus d'informations, reportez-vous aux pages de manuel `ssh_config`(4) et `ssh`(1).

▼ Génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell

Les utilisateurs doivent générer une paire de clés publiques ou privées lorsque leur site met en œuvre l'authentification basée sur l'hôte ou l'authentification avec clé publique de l'utilisateur. Pour plus d'options, reportez-vous à la page de manuel `ssh-keygen`(1).

Avant de commencer Vérifiez auprès de votre administrateur système si l'authentification basée sur l'hôte est configurée.

1 Démarrez le programme de génération de clés.

```
myLocalHost% ssh-keygen -t rsa
Generating public/private rsa key pair.
...
```

Où `-t` est le type d'algorithme, `rsa`, `dsa`, ou `rsa1`.

2 Spécifiez le chemin vers le fichier qui contiendra la clé.

Par défaut, le nom de fichier `id_rsa`, qui représente une clé RSA v2, s'affiche entre parenthèses. Vous pouvez sélectionner ce fichier en appuyant sur la touche Retour. Ou bien, vous pouvez taper un autre nom de fichier.

```
Enter file in which to save the key (/home/jdoe/.ssh/id_rsa):     <Press Return>
```

Le nom de fichier de la clé publique est créé automatiquement par l'ajout de la chaîne `.pub` au nom du fichier de clés privées.

3 Entrez une phrase de passe pour utiliser votre clé.

Cette phrase de passe est utilisée pour chiffrer votre clé privée. Une entrée nulle est *fortement déconseillée*. Notez que la phrase de passe ne s'affiche pas lorsque vous la saisissez.

```
Enter passphrase (empty for no passphrase):     <Type passphrase>
```

4 Entrez de nouveau la phrase de passe pour la confirmer.

```
Enter same passphrase again:     <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/id_rsa.
Your public key has been saved in /home/jdoe/.ssh/id_rsa.pub.
The key fingerprint is:
0e:fb:3d:57:71:73:bf:58:b8:eb:f3:a3:aa:df:e0:d1 jdoe@myLocalHost
```

5 Vérifiez les résultats.

Vérifiez que le chemin d'accès au fichier de la clé est correct.

```
% ls ~/.ssh
id_rsa
id_rsa.pub
```

À ce stade, vous avez créé une paire de clés publiques ou privées.

6 Choisissez l'option appropriée :

- **Si votre administrateur a configuré l'authentification basée sur l'hôte, vous pouvez être amené à copier la clé publique de l'hôte local sur l'hôte distant.**

  Vous pouvez maintenant vous connecter à l'hôte distant. Pour plus de détails, reportez-vous à la section "Connexion à un hôte distant avec Secure Shell " à la page 370.

  a. Saisissez la commande sur une seule ligne, sans barre oblique inverse.

  ```
  % cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
  'cat >> ~./ssh/known_hosts && echo "Host key copied"'
  ```

  b. Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.

  ```
  Enter password:      <Type password>
  Host key copied
  %
  ```

- **Si votre site utilise l'authentification de l'utilisateur avec les clés publiques, remplissez votre fichier `authorized_keys` sur l'hôte distant.**

  a. Copiez votre clé publique sur l'hôte distant.

  Saisissez la commande sur une seule ligne, sans barre oblique inverse.

  ```
  myLocalHost% cat $HOME/.ssh/id_rsa.pub | ssh myRemoteHost \
  'cat >> .ssh/authorized_keys && echo "Key copied"'
  ```

  b. Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.

  Lorsque le fichier est copié, le message "Key copied" (Clé copiée) s'affiche.

  ```
  Enter password:      Type login password
  Key copied
  myLocalHost%
  ```

7 (Facultatif) Réduisez le nombre d'invites de phrases de passe.

Pour connaître la procédure, reportez-vous à la section "Réduction des invites de mot de passe dans Secure Shell " à la page 371. Pour plus d'informations, reportez-vous aux pages de manuel `ssh-agent(1)` et `ssh-add(1)`.

Exemple 19–2 Définition d'une clé RSA v1 pour un utilisateur

Dans l'exemple ci-dessous, l'utilisateur peut contacter les hôtes qui exécutent la version 1 du protocole Secure Shell. Afin d'être authentifié par les hôtes v1, l'utilisateur crée une clé v1 et copie la portion de clé publique sur l'hôte distant.

```
myLocalHost% ssh-keygen -t rsa1 -f /home/jdoe/.ssh/identity
Generating public/private rsa key pair.
...
```

```
Enter passphrase (empty for no passphrase):     <Type passphrase>
Enter same passphrase again:     <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/identity.
Your public key has been saved in /home/jdoe/.ssh/identity.pub.
The key fingerprint is:
...
myLocalHost% ls ~/.ssh
id_rsa
id_rsa.pub
identity
identity.pub
myLocalHost% cat $HOME/.ssh/identity.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

▼ Modification de la phrase de passe pour une clé privée Secure Shell

La procédure suivante ne change pas la clé privée. La procédure modifie le mécanisme d'authentification pour la clé privée, la phrase de passe. Pour plus d'informations, reportez-vous à la page de manuel `ssh-keygen(1)`.

- **Modifiez votre phrase de passe.**

  Tapez la commande `ssh-keygen` avec l'option `-p`, et répondez aux invites.

  ```
  myLocalHost% ssh-keygen -p
  Enter file which contains the private key (/home/jdoe/.ssh/id_rsa):     <Press Return>
  Enter passphrase (empty for no passphrase):     <Type passphrase>
  Enter same passphrase again:     <Type passphrase>
  ```

  Où `-p` demande la modification de la phrase de passe d'un fichier de clés privées.

▼ Connexion à un hôte distant avec Secure Shell

1. **Démarrez une session Secure Shell.**

   Tapez la commande `ssh` et spécifiez le nom de l'hôte distant.

   ```
   myLocalHost% ssh myRemoteHost
   ```

   Une invite met en doute l'authenticité de l'hôte distant :

   ```
   The authenticity of host 'myRemoteHost' can't be established.
   RSA key fingerprint in md5 is: 04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26
   Are you sure you want to continue connecting(yes/no)?
   ```

   Cette invite est normale pour les connexions initiales sur des hôtes distants.

2 À l'invite, vérifiez l'authenticité de la clé de l'hôte distant.

- **Si vous ne pouvez pas confirmer l'authenticité de l'hôte distant, saisissez `no` et contactez votre administrateur système.**

  ```
  Are you sure you want to continue connecting(yes/no)? no
  ```

  L'administrateur est responsable de la mise à jour du fichier `/etc/ssh/ssh_known_hosts` global. Un fichier `ssh_known_hosts` mis à jour empêche l'affichage de cette invite.

- **Si vous confirmez l'authenticité de l'hôte distant, répondez à l'invite et passez à l'étape suivante.**

  ```
  Are you sure you want to continue connecting(yes/no)? yes
  ```

3 Authentifiez-vous sur Secure Shell.

a. Lorsque vous y êtes invité, saisissez votre phrase de passe.

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':      <Type passphrase>
```

b. Lorsque vous y êtes invité, saisissez votre mot de passe de compte.

```
jdoe@myRemoteHost's password:      <Type password>
Last login: Fri Jul 20 14:24:10 2001 from myLocalHost
myRemoteHost%
```

4 Effectuez des transactions sur l'hôte distant.

Les commandes que vous envoyez sont chiffrées. Les réponses que vous recevez sont chiffrées.

5 Arrêtez la connexion Secure Shell.

Lorsque vous avez terminé, saisissez **`exit`** ou utilisez votre méthode habituelle pour quitter votre shell.

```
myRemoteHost% exit
myRemoteHost% logout
Connection to myRemoteHost closed
myLocalHost%
```

▼ Réduction des invites de mot de passe dans Secure Shell

Si vous ne voulez pas saisir votre phrase de passe et votre mot de passe pour utiliser Secure Shell, vous pouvez utiliser le démon de l'agent. Démarrez ce démon au début de la session. Ensuite, stockez vos clés privées avec le démon de l'agent à l'aide de la commande `ssh-add`. Si vous avez des comptes différents sur différents hôtes, ajoutez les clés dont vous avez besoin pour la session.

Vous pouvez démarrer le démon de l'agent manuellement lorsque vous en avez besoin, comme décrit dans la procédure suivante. Ou bien, vous pouvez définir le démon de l'agent pour qu'il s'exécute automatiquement au début de chaque session comme décrit dans la section "Configuration de la commande `ssh-agent` pour qu'elle s'exécute automatiquement dans le CDE " à la page 373.

1 Démarrez le démon de l'agent.

```
myLocalHost% eval 'ssh-agent'
Agent pid 9892
```

2 Vérifiez que le démon de l'agent a été démarré.

```
myLocalHost% pgrep ssh-agent
9892
```

3 Ajoutez votre clé privée au démon de l'agent.

Saisissez la commande `ssh-add`.

```
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost%
```

4 Démarrez une session Secure Shell.

```
myLocalHost% ssh myRemoteHost
```

Vous n'êtes pas invité à saisir une phrase de passe.

Exemple 19–3 Utilisation des options `ssh-add`

Dans cet exemple, `jdoe` ajoute deux clés pour le démon de l'agent. L'option `-l` sert à répertorier toutes les clés stockées dans le démon. À la fin de la session, l'option `-D` sert à supprimer toutes les clés du démon de l'agent.

```
myLocalHost% ssh-agent
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost% ssh-add /home/jdoe/.ssh/id_dsa
Enter passphrase for /home/jdoe/.ssh/id_dsa:      <Type passphrase>
Identity added:
/home/jdoe/.ssh/id_dsa(/home/jdoe/.ssh/id_dsa)

myLocalHost% ssh-add -l
md5 1024 0e:fb:3d:53:71:77:bf:57:b8:eb:f7:a7:aa:df:e0:d1
/home/jdoe/.ssh/id_rsa(RSA)
md5 1024 c1:d3:21:5e:40:60:c5:73:d8:87:09:3a:fa:5f:32:53
/home/jdoe/.ssh/id_dsa(DSA)
```

User conducts Oracle Solaris Secure Shell transactions

```
myLocalHost% ssh-add -D
Identity removed:
/home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa.pub)
/home/jdoe/.ssh/id_dsa(DSA)
```

Configuration de la commande `ssh-agent` pour qu'elle s'exécute automatiquement dans le CDE

Avec le CDE, vous pouvez éviter d'avoir à fournir votre phrase de passe et votre mot de passe à chaque utilisation de Secure Shell en démarrant automatiquement un démon d'agent, `ssh-agent`. Vous pouvez démarrer le démon de l'agent du script `.dtprofile`. Pour ajouter la phrase de passe et un mot de passe au démon de l'agent, reportez-vous à l'Exemple 19–3.

Attention – Si vous utilisez Sun Java Desktop System (Java DS), ne configurez pas la commande `ssh-agent` pour qu'elle s'exécute automatiquement. Étant donné que l'interruption forcée du processus `ssh-agent` est contrôlée par une interface CDE, lorsque vous quittez le Java DS, le démon continue de s'exécuter. Par exemple, si vous lancez le démon dans une session CDE, passez à une session Java DS, puis déconnectez-vous, le démon continue de s'exécuter.

Un démon en cours d'exécution utilise les ressources système. Le fait que le démon `ssh-agent` continue de s'exécuter ne pose pas de problème en soi, par contre, son mot de passe vous expose à un risque de sécurité.

1. **Démarrez le démon de l'agent automatiquement dans un script de démarrage utilisateur.**

   Ajoutez les lignes suivantes à la fin du script `$HOME/.dtprofile` :

   ```
   if [ "$SSH_AUTH_SOCK" = "" -a -x /usr/bin/ssh-agent ]; then
                   eval `/usr/bin/ssh-agent`
   fi
   ```

2. **Arrêtez le démon de l'agent lorsque vous quittez la session CDE.**

   Ajoutez les lignes suivantes au script `$HOME/.dt/sessions/sessionexit` :

   ```
   if [ "$SSH_AGENT_PID" != "" -a -x /usr/bin/ssh-agent ]; then
                   /usr/bin/ssh-agent -k
   fi
   ```

   Cette entrée garantit que personne ne peut utiliser l'agent Secure Shell après la fermeture d'une session CDE. Étant donné que le script utilise une interface spécifique à CDE, `sessionexit`, cette procédure n'interrompt pas le démon de l'agent dans une session Sun Java Desktop System.

▼ Utilisation du transfert de port dans Secure Shell

Vous pouvez spécifier qu'un port local est transmis à un hôte distant. En réalité, un socket est alloué pour écouter le port côté local. La connexion sur l'hôte distant à partir de ce port est effectuée par le biais d'un canal sécurisé. Par exemple, vous pouvez spécifier un port 143 afin de recevoir votre courrier à distance avec IMAP4. De la même façon, un port peut être spécifié côté distant.

Avant de commencer Pour utiliser le transfert de port, l'administrateur doit avoir activé le transfert de port sur le serveur Secure Shell distant. Pour plus de détails, reportez-vous à la section "Configuration du transfert de port dans Secure Shell " à la page 366.

- **Pour utiliser le transfert de port sécurisé, choisissez l'une des options suivantes :**

  - **Pour définir un port local pour recevoir une communication sécurisée à partir d'un port distant, spécifiez les deux ports.**

    Spécifiez le port local à l'écoute de la communication à distance. De même, indiquez l'hôte distant et le port distant qui transfèrent la communication.

    ```
    myLocalHost% ssh -L localPort:remoteHost:remotePort
    ```

  - **Pour définir un port distant de manière à ce qu'il reçoive une connexion sécurisée d'un port local, spécifiez les deux ports.**

    Spécifiez le port distant à l'écoute de la communication à distance. De même, indiquez l'hôte local et le port local qui transfèrent la communication.

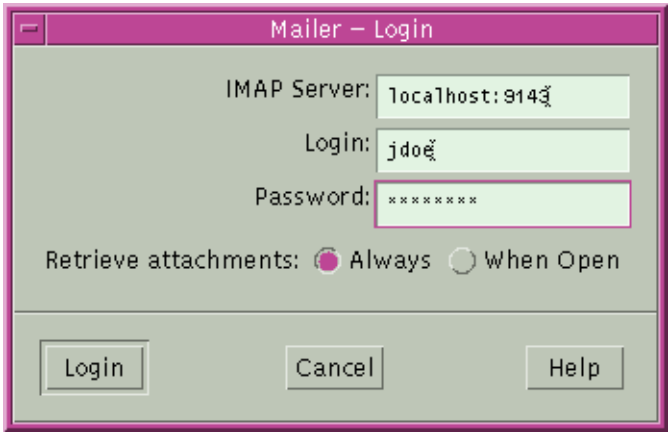
    ```
    myLocalHost% ssh -R remotePort:localhost:localPort
    ```

Exemple 19–4 Utilisation du transfert de port local pour recevoir du courrier

L'exemple suivant illustre l'utilisation du transfert du port local pour recevoir du courrier en toute sécurité à partir d'un serveur distant.

```
myLocalHost% ssh -L 9143:myRemoteHost:143 myRemoteHost
```

Cette commande transmet les connexions à partir du port 9143 sur myLocalHost au port 143. Port 143 est le port du serveur IMAP v2 sur myRemoteHost. Lorsque l'utilisateur lance une application de messagerie, celui-ci doit spécifier le numéro de port local, comme indiqué dans la boîte de dialogue suivante.



Il ne faut pas confondre `localhost`, dans cette boîte de dialogue, avec `myLocalHost`. `myLocalHost` est un nom d'hôte hypothétique. `localhost` est un mot-clé qui identifie votre système local.

Exemple 19–5 Utilisation du transfert de port distant pour communiquer à l'extérieur d'un pare-feu

Cet exemple montre comment l'utilisateur, dans un environnement d'entreprise, peut transférer vers un hôte à l'intérieur d'un pare-feu d'entreprise des connexions d'un hôte sur un réseau externe.

```
myLocalHost% ssh -R 9022:myLocalHost:22 myOutsideHost
```

Cette commande transmet les connexions à partir du port `9022` sur `myOutsideHost` au port `22`, le serveur `sshd`, sur l'hôte local.

```
myOutsideHost% ssh -p 9022 localhost
myLocalHost%
```

▼ Copie de fichiers avec Secure Shell

La procédure suivante décrit la façon dont la commande `scp` copie les fichiers chiffrés entre les hôtes. Vous pouvez copier les fichiers chiffrés entre un hôte local et un hôte distant, ou entre deux hôtes distants. Cette commande fonctionne de manière similaire à la commande `rcp`, à l'exception près que `scp` invite à s'authentifier. Pour plus d'informations, reportez-vous à la page de manuel `scp(1)`.

Vous pouvez également utiliser la commande `sftp`, une forme plus sécurisée de la commande `ftp`. Pour plus d'informations, reportez-vous à la page de manuel `sftp(1)`. Voir l'Exemple 19–6.

1 **Démarrez le programme de copie sécurisée.**

Spécifier le fichier source, le nom d'utilisateur au niveau de la destination distante et le répertoire de destination.

```
myLocalHost% scp myfile.1 jdoe@myRemoteHost:~
```

2 **Indiquez votre phrase de passe lorsque vous y êtes invité.**

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':      <Type passphrase>
myfile.1       25% |*******                      |    640 KB  0:20 ETA
myfile.1
```

Une fois que vous avez saisi la phrase de passe, un indicateur de progression s'affiche. Reportez-vous à la seconde ligne de la sortie ci-dessus. L'indicateur de progression affiche les données suivantes :

- Le nom de fichier
- Le pourcentage du fichier qui a été transféré
- Une série d'astérisques qui indiquent le pourcentage du fichier qui a été transmis
- La quantité de données transférées
- L'heure d'arrivée prévue de la totalité du fichier (c'est-à-dire, le temps restant)

Exemple 19–6 Spécification d'un port à l'aide de la commande `sftp`

Dans cet exemple, l'utilisateur souhaite que la commande `sftp` utilise un port spécifique. L'utilisateur utilise l'option `-o` pour spécifier le port.

```
% sftp -o port=2222 guest@RemoteFileServer
```

▼ Définition des connexions aux hôtes en dehors du pare-feu

Vous pouvez utiliser Secure Shell pour établir une connexion entre un hôte à l'intérieur d'un pare-feu et un hôte à l'extérieur du pare-feu. Cette tâche s'effectue en spécifiant une commande proxy pour `ssh` dans un fichier de configuration ou sous forme d'option dans la ligne de commande. Pour l'option de ligne de commande, reportez-vous à l'Exemple 19–7.

En général, vous pouvez personnaliser vos interactions `ssh` par le biais d'un fichier de configuration.

- Vous pouvez personnaliser votre propre fichier personnel dans `~/.ssh/config`.
- Ou bien, vous pouvez utiliser les paramètres dans le fichier de configuration administrative, `/etc/ssh/ssh_config`.

Les fichiers peuvent être personnalisés avec deux types de commandes proxy. Une commande proxy sert aux connexions HTTP. L'autre commande proxy sert aux connexions SOCKS5. Pour plus d'informations, reportez-vous à la page de manuel `ssh_config(4)`.

1 Spécifiez les commandes proxy et les hôtes dans un fichier de configuration.

Utilisez la syntaxe suivante pour ajouter autant de lignes qu'il est nécessaire :

```
[Host outside-host]
ProxyCommand proxy-command [-h proxy-server] \
[-p proxy-port] outside-host|%h outside-port|%p
```

`Hôte` *outside-host*
: Limite la spécification de la commande proxy aux instances lorsqu'un nom d'hôte distant est spécifié dans la ligne de commande. Si vous utilisez un caractère générique pour *outside-host*, vous appliquez la spécification de la commande proxy à un ensemble d'hôtes.

proxy-command
: Spécifie la commande proxy.

  La commande peut avoir l'une des formes suivantes :

  - `/usr/lib/ssh/ssh-http-proxy-connect` pour les connexions HTTP
  - `/usr/lib/ssh/ssh-socks5-proxy-connect` pour les connexions SOCKS5

`-h` *proxy-server* et `-p` *proxy-port*
: Ces options spécifient respectivement un serveur proxy et un port proxy. Si des proxys sont présents, ils remplacent toutes les variables d'environnement qui spécifient les serveurs et ports proxy, tel que `HTTPPROXY`, `HTTPPROXYPORT`, `SOCKS5_PORT`, `SOCKS5_SERVER` et `http_proxy`. La variable `http_proxy` spécifie une adresse URL. Si ces options ne sont pas utilisées, les variables d'environnement doivent être définies. Pour plus d'informations, reportez-vous aux pages de manuel `ssh-socks5-proxy-connect(1)` et `ssh-http-proxy-connect(1)`.

outside-host
: Désigne un hôte spécifique pour la connexion. Utilisez l'argument de substitution `%h` pour spécifier l'hôte sur la ligne de commande.

outside-port
: Désigne un port spécifique pour la connexion. Utilisez l'argument de substitution `%p` pour spécifier le port sur la ligne de commande. En spécifiant `%h` et `%p` sans utiliser l'option `Host` *outside-host*, la commande proxy est appliquée à l'argument de l'hôte chaque fois que la commande `ssh` est appelée.

2 Exécutez Secure Shell en indiquant l'hôte externe.

Par exemple, tapez la commande suivante :

```
myLocalHost% ssh myOutsideHost
```

Cette commande recherche une spécification de commande proxy pour `myOutsideHost` dans votre fichier de configuration. Si la spécification est introuvable, la commande recherche dans le fichier de configuration du système, `/etc/ssh/ssh_config`. La commande proxy remplace la commande `ssh`.

Exemple 19–7 Connexion à des hôtes en dehors du pare-feu à partir de la ligne de commande

La section "Définition des connexions aux hôtes en dehors du pare-feu " à la page 376 décrit la procédure de spécification d'une commande proxy dans un fichier de configuration. Dans cet exemple, une commande proxy est spécifiée sur la ligne de commande `ssh`.

```
% ssh -o'Proxycommand=/usr/lib/ssh/ssh-http-proxy-connect \
-h myProxyServer -p 8080 myOutsideHost 22' myOutsideHost
```

L'option `-o` de la commande `ssh` fournit une méthode de ligne de commande pour spécifier une commande proxy. Cet exemple de commande effectue les opérations suivantes :

- La commande proxy HTTP remplace `ssh`
- Le port `8080` est utilisé et `myProxyServer` défini en tant que serveur proxy
- La connexion a lieu sur le port `22` de `myOutsideHost`

◆ ◆ ◆ CHAPITRE 20

Oracle Solaris Secure Shell (référence)

Ce chapitre décrit les options de configuration de la fonction Secure Shell d'Oracle Solaris. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre.

Pour plus d'informations sur les procédures de configuration de Secure Shell, reportez-vous au Chapitre 19, "Utilisation d'Oracle Solaris Secure Shell (tâches)".

Session Secure Shell standard

Le démon Secure Shell (`sshd`) est démarré normalement au moment de l'initialisation lorsque les services réseau sont démarrés. Le démon détecte les connexions des clients. Une session Secure Shell commence lorsque l'utilisateur exécute une commande `ssh`, `scp` ou `sftp`. Un nouveau démon `sshd` est cloné pour chaque connexion entrante. Le démon cloné gère l'échange de clés, le chiffrement, l'authentification, l'exécution des commandes et l'échange de données avec le client. Ces caractéristiques de session sont déterminées par les fichiers de configuration côté client et côté serveur. Les arguments de la ligne de commande peuvent remplacer les paramètres des fichiers de configuration.

Le client doit s'authentifier auprès du serveur et vice-versa. Après la réussite de l'authentification, l'utilisateur peut exécuter des commandes à distance et copier des données entre les hôtes.

Caractéristiques des sessions dans Secure Shell

Le comportement côté serveur du démon `sshd` est contrôlé par les paramètres de mot-clé dans le fichier `/etc/ssh/sshd_config`. Par exemple, le fichier `sshd_config` détermine les types d'authentification qui sont autorisés pour l'accès au serveur. Le comportement côté serveur peut également être contrôlé par les options de la ligne de commande lorsque le démon `sshd` est démarré.

Le comportement côté client est contrôlé par les mots-clés Secure Shell dans l'ordre de priorité suivant :

- Options de ligne de commande
- Fichier de configuration de l'utilisateur, `~/.ssh/config`
- Fichier de configuration à l'échelle du système, `/etc/ssh/ssh_config`

Par exemple, un utilisateur peut remplacer un paramètre `Ciphers` de configuration à l'échelle du système qui préfère `aes128-cen` en spécifiant `-c aes256-cen,aes128-cen,arcfour` sur la ligne de commande. Le premier chiffre, `aes256-cen`, est désormais préféré.

Authentification et échange de clés dans Secure Shell

Les protocoles Secure Shell, v1 et v2, prennent en charge l'authentification de l'utilisateur/hôte client et l'authentification de l'hôte serveur. Les deux protocoles impliquent l'échange de clés cryptographiques de session pour la protection des sessions Secure Shell. Chaque protocole fournit plusieurs méthodes pour l'authentification et l'échange de clés. Certaines de ces méthodes sont facultatives. Secure Shell prend en charge un certain nombre de mécanismes d'authentification client, tel qu'illustré dans le Tableau 19–1. Les serveurs sont authentifiés à l'aide de clés publiques d'hôte connu.

Pour le protocole v1, Secure Shell prend en charge l'authentification de l'utilisateur avec des mots de passe. Le protocole prend également en charge les clés publiques utilisateur et l'authentification avec des clés publiques d'hôte de confiance. L'authentification du serveur est effectuée avec une clé publique d'hôte. Pour le protocole v1, toutes les clés publiques sont des clés RSA. Les échanges de clé de session impliquent l'utilisation d'une clé de serveur éphémère qui est régulièrement regénérée.

Pour le protocole v2, Secure Shell prend en charge l'authentification de l'utilisateur et l'authentification interactive générique, qui implique généralement des mots de passe. Le protocole prend également en charge l'authentification avec des clés publiques utilisateur et des clés publiques d'hôte de confiance. Il peut s'agir de clés RSA ou DSA. Les échanges de clés de session sont des échanges de clés éphémères Diffie-Hellman qui sont signées à l'étape d'authentification du serveur. En outre, Secure Shell peut utiliser des informations d'identification GSS pour l'authentification.

Acquisition d'informations d'identification GSS dans Secure Shell

Pour utiliser GSS-API pour l'authentification dans Secure Shell, le serveur doit disposer des informations d'identification de l'accepteur GSS-API et le client doit disposer des informations d'identification de l'initiateur GSS-API. La prise en charge est disponible pour `mech_dh` et pour `mech_krb5`.

Pour `mech_dh`, le serveur dispose des informations d'identification de l'accepteur GSS-API si `root` a exécuté la commande `keylogin`.

Pour `mech_krb5`, le serveur dispose des informations d'identification de GSS-API lorsque l'hôte principal qui correspond au serveur possède une valeur correcte dans `/etc/krb5/krb5.keytab`.

Le client dispose des informations d'identification de l'initiateur pour `mech_dh` si l'une des actions ci-après a été effectuée :

- La commande `keylogin` a été exécutée.
- Le module `pam_dhkeys` est utilisé dans le fichier `pam.conf`.

Le client dispose des informations d'identification de l'initiateur pour `mech_krb5` si l'une des actions ci-après a été effectuée :

- La commande `kinit` a été exécutée.
- Le module `pam_krb5` est utilisé dans le fichier `pam.conf`.

Pour l'utilisation de `mech_dh` dans le RPC sécurisé, reportez-vous au Chapitre 16, “Utilisation des services d'authentification (tâches) ”. Pour l'utilisation de `mech_krb5`, reportez-vous au Chapitre 21, “Introduction au service Kerberos”. Pour plus d'informations sur les mécanismes, reportez-vous aux pages de manuel `mech(4)` et `mech_spnego(5)`.

Exécution des commandes et transmission de données dans Secure Shell

Une fois l'authentification terminée, l'utilisateur peut utiliser Secure Shell, généralement en demandant un shell ou en exécutant une commande. Par l'intermédiaire des options de commande `ssh`, l'utilisateur peut effectuer des demandes. Les demandes peuvent inclure l'allocation d'un pseudo-tty, la transmission des connexions X11 ou TCP/IP, ou l'activation d'un programme d'authentification `ssh-agent` via une connexion sécurisée.

Les composants de base d'une session utilisateur sont les suivants :

1. L'utilisateur demande un shell ou l'exécution d'une commande, ce qui lance le mode de session.

   Dans ce mode, les données sont envoyées ou reçues par le biais du terminal sur le côté client. Sur le côté serveur, les données sont envoyées par l'intermédiaire du shell ou d'une commande.

2. Lorsque la transmission des données est terminée, le programme utilisateur s'arrête.
3. L'ensemble de la transmission X11 et de la transmission TCP/IP est arrêté, sauf pour les connexions qui existent déjà. Les connexions X11 et TCP/IP existantes restent ouvertes.
4. Le serveur envoie un message d'état de sortie au client. Lorsque toutes les connexions sont fermées, telles que les ports transmis qui étaient restés ouverts, le client ferme la connexion au serveur. Ensuite, le client se ferme.

Configuration des clients et des serveurs dans Secure Shell

Les caractéristiques d'une session Secure Shell sont contrôlées par les fichiers de configuration. Les fichiers de configuration peuvent être remplacés dans une certaine mesure par des options de la ligne de commande.

Configuration des clients dans Secure Shell

Dans la plupart des cas, les caractéristiques côté client d'une session Secure Shell sont régies par le fichier de configuration à l'échelle du système, `/etc/ssh/ssh_config`. Les paramètres dans le fichier `ssh_config` peuvent être remplacés par le fichier de configuration de l'utilisateur, `~/.ssh/config`. En outre, l'utilisateur peut remplacer les deux fichiers de configuration sur la ligne de commande.

Les paramètres du fichier `/etc/ssh/sshd_config` du serveur déterminent quelles demandes client sont autorisées par le serveur. Pour obtenir la liste des paramètres de configuration de serveur, reportez-vous à la section "Mots-clés dans Secure Shell" à la page 383. Pour plus d'informations, reportez-vous à la page de manuel `sshd_config(4)`.

Les mots-clés du fichier de configuration du client sont répertoriés dans la section "Mots-clés dans Secure Shell" à la page 383. Si le mot-clé a une valeur par défaut, la valeur est donnée. Ces mots-clés sont décrits en détails dans les pages de manuel `ssh(1)`, `scp(1)`, `sftp(1)` et `ssh_config(4)`. Pour obtenir la liste des mots-clés dans l'ordre alphabétique et leurs substituts de ligne de commande équivalents, reportez-vous au Tableau 20–8.

Configuration du serveur dans Secure Shell

Les caractéristiques côté serveur d'une session Secure Shell sont régies par le fichier `/etc/ssh/sshd_config`. Les mots-clés dans le fichier de configuration du serveur sont répertoriés dans "Mots-clés dans Secure Shell" à la page 383. Si le mot-clé a une valeur par défaut, la valeur est donnée. Pour une description complète des mots-clés, reportez-vous à la page de manuel `sshd_config(4)`.

Mots-clés dans Secure Shell

Les tableaux ci-dessous répertorient les mots-clés et leurs valeurs par défaut, le cas échéant. Les mots-clés sont dans l'ordre alphabétique. L'emplacement des mots-clés sur le client est le fichier `ssh_config`. Les mots-clés qui s'appliquent au serveur sont dans le fichier `sshd_config`. Certains mots-clés sont définis dans les deux fichiers. Si le mot-clé ne s'applique qu'à une version du protocole, la version est répertoriée.

TABLEAU 20–1 Mots-clés des fichiers de configuration Secure Shell (A à Echap)

Mot-clé	Valeur par défaut	Emplacement	Protocole
`AllowGroups`	Pas de valeur par défaut.	Serveur	
`AllowTcpForwarding`	`yes`	Serveur	
`AllowUsers`	Pas de valeur par défaut.	Serveur	
`AuthorizedKeysFile`	`~/.ssh/authorized_keys`	Serveur	
`Banner`	`/etc/issue`	Serveur	
`Batchmode`	`no`	Client	
`BindAddress`	Pas de valeur par défaut.	Client	
`CheckHostIP`	`yes`	Client	
`ChrootDirectory`	`no`	Serveur	v2
`Cipher`	`blowfish`, `3des`	Client	v1
`Ciphers`	`aes128-ctr, aes128-cbc, 3des-cbc, blowfish-cbc, arcfour`	Les deux	v2
`ClearAllForwardings`	`no`	Client	
`ClientAliveCountMax`	`3`	Serveur	v2
`ClientAliveInterval`	`0`	Serveur	v2
`Compression`	`no`	Les deux	
`CompressionLevel`	Pas de valeur par défaut.	Client	v1
`ConnectionAttempts`	`1`	Client	
`DenyGroups`	Pas de valeur par défaut	Serveur	
`DenyUsers`	Pas de valeur par défaut	Serveur	
`DynamicForward`	Pas de valeur par défaut.	Client	
`EscapeChar`	`~`	Client	

TABLEAU 20–2 Mots-clés dans les fichiers de configuration Secure Shell (Fall à Local)

Mot-clé	Valeur par défaut	Emplacement	Protocole
`FallBackToRsh`	`no`	Client	
`ForwardAgent`	`no`	Client	
`ForwardX11`	`no`	Client	
`GatewayPorts`	`no`	Les deux	
`GlobalKnownHostsFile`	`/etc/ssh/ssh_known_hosts`	Client	
`GSSAPIAuthentication`	`yes`	Les deux	v2
`GSSAPIDelegateCredentials`	`no`	Client	v2
`GSSAPIKeyExchange`	`yes`	Les deux	v2
`GSSAPIStoreDelegateCredentials`	`yes`	Serveur	v2
`Host`	* Pour plus d'informations, reportez-vous à la section "Paramètres spécifiques à l'hôte dans Secure Shell" à la page 386.	Client	
`HostbasedAuthentication`	`no`	Les deux	v2
`HostbasedUsesNameFromPacketOnly`	`no`	Serveur	v2
`HostKey`	`/etc/ssh/ssh_host_key`	Serveur	v1
`HostKey`	`/etc/ssh/host_rsa_key`, `/etc/ssh/host_dsa_key`	Serveur	v2
`HostKeyAlgorithms`	`ssh-rsa, ssh-dss`	Client	v2
`HostKeyAlias`	Pas de valeur par défaut.	Client	v2
`HostName`	Pas de valeur par défaut.	Client	v2
`IdentityFile`	`~/.ssh/identity`	Client	v1
`IdentityFile`	`~/.ssh/id_dsa, ~/.ssh/id_rsa`	Client	v2
`IgnoreRhosts`	`yes`	Serveur	
`IgnoreUserKnownHosts`	`yes`	Serveur	
`KbdInteractiveAuthentication`	`yes`	Les deux	
`KeepAlive`	`yes`	Les deux	
`KeyRegenerationInterval`	`3600` (secondes)	Serveur	
`ListenAddress`	Pas de valeur par défaut.	Serveur	

TABLEAU 20–2 Mots-clés dans les fichiers de configuration Secure Shell (Fall à Local) *(Suite)*

Mot-clé	Valeur par défaut	Emplacement	Protocole
`LocalForward`	Pas de valeur par défaut.	Client	

TABLEAU 20–3 Mots-clés dans les fichiers de configuration Secure Shell (Login à R)

Mot-clé	Valeur par défaut	Emplacement	Protocole
`LoginGraceTime`	`600` (secondes)	Serveur	
`LogLevel`	`info`	Les deux	
`LookupClientHostnames`	`yes`	Serveur	
`MACs`	`hmac-sha1,hmac-md5`	Les deux	v2
`MaxAuthTries`	`6`	Serveur	
`MaxAuthTriesLog`	3	Serveur	
`MaxStartups`	`10:30:60`	Serveur	
`NoHostAuthenticationForLocalHost`	`no`	Client	
`NumberOfPasswordPrompts`	`3`	Client	
`PAMAuthenticationViaKBDInt`	`yes`	Serveur	v2
`PasswordAuthentication`	`yes`	Les deux	Les deux
`PermitEmptyPasswords`	`no`	Serveur	
`PermitRootLogin`	`no`	Serveur	
`PermitUserEnvironment`	`no`	Serveur	
`PidFile`	`/var/run/sshd.pid`	Serveur	
`Port`	`22`	Les deux	
`PreferredAuthentications`	`hostbased,publickey,keyboard-interactive,passwor`	Client	v2
`PrintLastLog`	`yes`	Serveur	v2
`PrintMotd`	`no`	Serveur	
`Protocol`	`2,1`	Les deux	
`ProxyCommand`	Pas de valeur par défaut.	Client	
`PubkeyAuthentication`	`yes`	Les deux	v2
`RemoteForward`	Pas de valeur par défaut.	Client	

TABLEAU 20–3 Mots-clés dans les fichiers de configuration Secure Shell (Login à R) *(Suite)*

Mot-clé	Valeur par défaut	Emplacement	Protocole
`RhostsAuthentication`	`no`	Les deux	v1
`RhostsRSAAuthentication`	`no`	Les deux	v1
`RSAAuthentication`	`no`	Les deux	v1

TABLEAU 20–4 Mots-clés dans les fichiers de configuration Secure Shell (S à X)

Mot-clé	Valeur par défaut	Emplacement	Protocole
`StrictHostKeyChecking`	`ask`	Client	
`StrictModes`	`yes`	Serveur	
`Subsystem`	`sftp /usr/lib/ssh/sftp-server`	Serveur	
`SyslogFacility`	`auth`	Serveur	
`UseLogin`	`no` Désapprouvé et ignoré.	Serveur	
`UseOpenSSLEngine`	`yes`	Les deux	v2
`UsePrivilegedPort`	`no`	Les deux	v2
`User`	Pas de valeur par défaut	Client	
`UserKnownHostsFile`	`~/.ssh/known_hosts`	Client	
`UseRsh`	`no`	Client	
`VerifyReverseMapping`	`no`	Serveur	
`X11DisplayOffset`	`10`	Serveur	
`X11Forwarding`	`yes`	Serveur	
`X11UseLocalHost`	`yes`	Serveur	
`XAuthLocation`	`/usr/openwin/bin/xauth`	Les deux	

Paramètres spécifiques à l'hôte dans Secure Shell

S'il est utile de disposer de différentes caractéristiques Secure Shell pour différents hôtes locaux, l'administrateur peut définir différents ensembles de paramètres dans le fichier `/etc/ssh/ssh_config` à appliquer en fonction de l'hôte ou d'une expression régulière. Cette tâche s'effectue en regroupant les entrées dans le fichier par le mot-clé `Host`. Si le mot-clé `Host` n'est pas utilisé, les entrées dans le fichier de configuration du client s'appliquent à n'importe lequel des hôtes locaux sur lesquels un utilisateur travaille.

Secure Shell et les variables d'environnement de connexion

Si les mots-clés Secure Shell suivants ne sont pas définis dans le fichier `sshd_config`, ils obtiennent leur valeur des entrées équivalentes à partir du fichier `/etc/default/login` :

Entrée dans `/etc/default/login`	Mot-clé et valeur dans `sshd_config`
`CONSOLE=*`	`PermitRootLogin=without-password`
`#CONSOLE=*`	`PermitRootLogin=yes`
`PASSREQ=YES`	`PermitEmptyPasswords=no`
`PASSREQ=NO`	`PermitEmptyPasswords=yes`
`#PASSREQ`	`PermitEmptyPasswords=no`
`TIMEOUT=`*secs*	`LoginGraceTime=`*secs*
`#TIMEOUT`	`LoginGraceTime=300`
`RETRIES` et `SYSLOG_FAILED_LOGINS`	S'appliquent uniquement aux méthodes d'authentification `password` et `keyboard-interactive`.

Lorsque les variables suivantes sont définies par les scripts d'initialisation du shell de connexion de l'utilisateur, le démon `sshd` utilise ces valeurs. Lorsque les variables ne sont pas définies, le démon utilise la valeur par défaut.

`TIMEZONE` Contrôle la définition de la variable d'environnement `TZ`. Lorsque cette variable n'est pas définie, le démon `sshd` utilise la valeur de `TZ` telle qu'elle était au moment de son démarrage.

`ALTSHELL` Contrôle la définition de la variable d'environnement `SHELL`. La valeur par défaut est `ALTSHELL=YES`, où le démon `sshd` utilise la valeur de shell de l'utilisateur. Quand `ALTSHELL=NO`, la valeur de `SHELL` n'est pas définie.

`PATH` Contrôle la définition de la variable d'environnement `PATH`. Lorsque la valeur n'est pas définie, le chemin d'accès par défaut est `/usr/bin`.

`SUPATH` Contrôle la définition de la variable d'environnement `PATH` pour `root`. Lorsque la valeur n'est pas définie, le chemin d'accès par défaut est `/usr/sbin:/usr/bin`.

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

Mise à jour des hôtes connus dans Secure Shell

Chaque hôte qui doit communiquer de manière sécurisée avec un autre hôte doit avoir la clé publique du serveur stockée dans le fichier `/etc/ssh/les` de l'hôte local. Bien qu'un script puisse être utilisé pour mettre à jour les fichiers `/etc/ssh/ssh_known_hosts`, une telle pratique est fortement déconseillée parce qu'un script crée une grande vulnérabilité de la sécurité.

Le fichier `/etc/ssh/ssh_known_hosts` doit uniquement être distribué par un mécanisme sécurisé comme suit :

- Via une connexion sécurisée, comme par exemple Secure Shell, IPsec, ou `ftp` utilisant Kerberos à partir d'une machine connue et de confiance.
- Au moment de l'installation

Pour éviter toute possibilité qu'un intrus obtienne l'accès en insérant de fausses clés publiques dans un fichier `known_hosts`, vous devez utiliser un serveur JumpStart en tant que source connue et de confiance du fichier `ssh_known_hosts`. Le fichier `ssh_known_hosts` peut être distribué au cours de l'installation. Plus tard, les scripts utilisant la commande `scp` peuvent être utilisés pour récupérer la version la plus récente. Cette approche est sécurisée car chaque hôte possède déjà la clé publique du serveur JumpStart.

Packages Secure Shell et initialisation

Secure Shell dépend des packages Solaris de base et des packages suivants :

- `SUNWgss` : contient le logiciel Generic Security Service (GSS)
- `SUNWtcpd` : contient les wrappers TCP
- `SUNWopenssl-libraries` : contient les bibliothèques OpenSSL
- `SUNWzlib` : contient la bibliothèque de compression zip

Les packages suivants installent Secure Shell :

- `SUNWsshr` : contient les fichiers client et les utilitaires pour le répertoire root (`/`)
- `SUNWsshdr` : contient les fichiers de serveur et utilitaires correspondant au répertoire (`/`) root
- `SUNWsshcu` : contient les fichiers source communs pour le répertoire `/usr`
- `SUNWsshdu` : contient les fichiers du serveur pour le répertoire `/usr`
- `SUNWsshu` : contient les fichiers client et utilitaires pour le répertoire `/usr`

Lors du redémarrage après installation, le démon `sshd` est en cours d'exécution. Le démon crée des raccourcis clavier sur le système. Un système Oracle Solaris qui exécute le démon `sshd` est un serveur Secure Shell.

Fichier Secure Shell

Le tableau suivant montre les fichiers Secure Shell importants et les autorisations de fichier suggérées.

TABLEAU 20–5 Fichier Secure Shell

Nom du fichier	Description	Autorisations suggérées et propriétaire
`/etc/ssh/sshd_config`	Contient des données de configuration pour `sshd`, le démon Secure Shell.	`-rw-r--r-- root`
`/etc/ssh/ssh_host_key`	Contient la clé privée de l'hôte (v1).	`-rw------- root`
`/etc/ssh/ssh_host_dsa_key` ou `/etc/ssh/ssh_host_rsa_key`	Contient la clé privée de l'hôte (v2).	`-rw------- root`
host-private-key `.pub`	Contient la clé publique de l'hôte, par exemple, `/etc/ssh/ssh_host_rsa_key.pub`. Est utilisé pour copier la clé d'hôte dans le fichier `known_hosts` local.	`-rw-r--r-- root`
`/var/run/sshd.pid`	Contient l'ID de processus du démon Secure Shell, `sshd`. Si plusieurs démons sont en cours d'exécution, le fichier contient la dernier démon qui a été démarré.	`-rw-r--r-- root`
`~/.ssh/authorized_keys`	Contient les clés publiques de l'utilisateur qui est autorisé à se connecter au compte utilisateur.	`-rw-r--r--` *username*
`/etc/ssh/ssh_known_hosts`	Contient les clés publiques pour tous les hôtes avec lesquels le client peut communiquer de manière sécurisée. Le fichier est renseigné par l'administrateur.	`-rw-r--r-- root`
`~/.ssh/known_hosts`	Contient les clés publiques pour tous les hôtes avec lesquels le client peut communiquer de manière sécurisée. Le fichier est mis à jour automatiquement. Chaque fois que l'utilisateur se connecte à l'aide d'un hôte inconnu, la clé de l'hôte distant est ajoutée au fichier.	`-rw-r--r--` *username*
`/etc/default/login`	Fournit les valeurs par défaut pour le démon `sshd` lorsque les paramètres `sshd_config` correspondants ne sont pas définis.	`-r--r--r-- root`
`/etc/nologin`	Si ce fichier existe, le démon `sshd` n'autorise que `root` à se connecter. Le contenu de ce fichier est affiché pour les utilisateurs qui tentent de se connecter.	`-rw-r--r-- root`
`~/.rhosts`	Contient les paires de noms hôte-utilisateur qui permettent d'indiquer les hôtes auxquels l'utilisateur peut se connecter sans mot de passe. Ce fichier est également utilisé par les démons `rlogind` et `rshd`.	`-rw-r--r--` *username*

TABLEAU 20–5 Fichier Secure Shell *(Suite)*

Nom du fichier	Description	Autorisations suggérées et propriétaire
`~/.shosts`	Contient les paires de noms hôte-utilisateur qui permettent d'indiquer les hôtes auxquels l'utilisateur peut se connecter sans mot de passe. Ce fichier n'est utilisé par aucun autre utilitaire. Pour plus d'informations, reportez-vous à la page de manuel `sshd(1M)` dans la section `FILES`.	`-rw-r--r--` *username*
`/etc/hosts.equiv`	Contient les hôtes qui sont utilisés dans l'authentification `.rhosts`. Ce fichier est également utilisé par les démons `rlogind` et `rshd`.	`-rw-r--r-- root`
`/etc/ssh/shosts.equiv`	Contient les hôtes qui sont utilisés dans l'authentification basée sur les hôtes. Ce fichier n'est utilisé par aucun autre utilitaire.	`-rw-r--r-- root`
`~/.ssh/environment`	Contient les affectations initiales au moment de la connexion. Par défaut, ce fichier n'est pas lu. Le mot-clé `PermitUserEnvironment` du fichier `sshd_config` doit être défini sur `yes` pour que ce fichier soit lu.	`-rw-r--r--` *username*
`~/.ssh/rc`	Contient les routines d'initialisation qui sont exécutées avant que le shell utilisateur ne démarre. Pour un échantillon de routine d'initialisation, reportez-vous à la page de manuel `sshd(1M)`.	`-rw-r--r--` *username*
`/etc/ssh/crsh`	Contient les routines d'initialisation spécifiques à un hôte qui sont spécifiées par un administrateur.	`-rw-r--r-- root`
`/etc/ssh/ssh_config`	Configure les paramètres système sur le système client.	`-rw-r--r-- root`
`~/.ssh/config`	Permet de configurer les paramètres de l'utilisateur. Remplace les paramètres système.	`-rw-r--r--` *username*

Le tableau ci-dessous répertorie les fichiers Secure Shell qui peuvent être remplacés par des mots-clés ou des options de commande.

TABLEAU 20–6 Remplacement pour l'emplacement des fichiers Secure Shell

Nom du fichier	Remplacement par mot-clé	Remplacement via la ligne de commande
`/etc/ssh/ssh_config`		`ssh -F` *config-file* `scp -F` *config-file*
`~/.ssh/config`		`ssh -F` *config-file*
`/etc/ssh/host_rsa_key` `/etc/ssh/host_dsa_key`	`HostKey`	

TABLEAU 20–6 Remplacement pour l'emplacement des fichiers Secure Shell *(Suite)*

Nom du fichier	Remplacement par mot-clé	Remplacement via la ligne de commande
`~/.ssh/identity`	`IdentityFile`	`ssh -i` *id-file*
`~/.ssh/id_dsa`, `~/.ssh/id_rsa`		`scp -i` *id-file*
`~/.ssh/authorized_keys`	`AuthorizedKeysFile`	
`/etc/ssh/ssh_known_hosts`	`GlobalKnownHostsFile`	
`~/.ssh/known_hosts`	`UserKnownHostsFile`	
	`IgnoreUserKnownHosts`	

Commandes Secure Shell

Le tableau suivant récapitule les principales commandes Secure Shell.

TABLEAU 20–7 Commandes Secure Shell

Commande	Description	Page de manuel
`ssh`	Connecte un utilisateur à une machine distante et exécute de manière sécurisée les commandes sur une machine distante. Cette commande est le remplacement Secure Shell des commandes `rlogin` et `rsh`. La commande `ssh` permet de protéger les communications chiffrées entre deux hôtes non autorisés sur un réseau non sécurisé. Les connexions X11 et les ports TCP/IP arbitraires peuvent également être transmis via le canal sécurisé.	`ssh(1)`
`sshd`	Est le démon pour Secure Shell. Le démon détecte les connexions des clients et sécurise les communications chiffrées entre deux hôtes non autorisés sur un réseau non sécurisé.	`sshd(1M)`
`ssh-add`	Ajoute des identités RSA ou DSA à l'agent d'authentification, `ssh-agent`. Les identités sont également appelées *clés*.	`ssh-add(1)`
`ssh-agent`	Contient les clés privées qui sont utilisées pour l'authentification avec clé publique. Le programme `ssh-agent` est lancé au début d'une session X ou d'une session de connexion. Toutes les autres fenêtres et les autres programmes sont lancés en tant que clients du programme `ssh-agent`. Par le biais de l'utilisation de variables d'environnement, l'agent peut être localisé et utilisé pour l'authentification lorsque les utilisateurs utilisent la commande `ssh` pour se connecter à d'autres systèmes.	`ssh-agent(1)`
`ssh-keygen`	Génère et gère des clés d'authentification pour Secure Shell.	`ssh-keygen(1)`
`ssh-keyscan`	Regroupe les clés publiques d'un certain nombre d'hôtes Secure Shell. Facilite la création et la vérification des fichiers `ssh_known_hosts`.	`ssh-keyscan(1)`
`ssh-keysign`	Est utilisé par les commandes `ssh` pour accéder aux clés d'hôte sur l'hôte local. Génère la signature numérique requise pendant l'authentification basée sur l'hôte avec Secure Shell v2. La commande est appelée par la commande `ssh`, et non par l'utilisateur.	`ssh-keysign(1M)`

TABLEAU 20–7 Commandes Secure Shell *(Suite)*

Commande	Description	Page de manuel
`scp`	Copie les fichiers de manière sécurisée entre les hôtes d'un réseau via un transport `ssh` chiffré. Contrairement à la commande `rcp`, la commande `scp` demande à saisir les mots de passe ou les phrases de passe, si des informations de mot de passe sont nécessaires pour l'authentification.	`scp`(1)
`sftp`	Est un programme de transmission de fichier interactif similaire à la commande `ftp`. Contrairement à la commande `ftp`, la commande `sftp` effectue toutes les opérations sur un transport `ssh` chiffré. La commande établit la connexion, se connecte au nom d'hôte spécifié, puis entre en mode de commande interactif.	`sftp`(1)

Le tableau suivant répertorie les options de commande qui remplacent les mots-clés Secure Shell. Les mots-clés sont spécifiés dans les fichiers `ssh_config` et `sshd_config`.

TABLEAU 20–8 Équivalents de la ligne de commande pour les mots-clés Secure Shell

Mot-clé	`ssh` Remplacement de ligne de commande	`scp` Remplacement de ligne de commande
`BatchMode`		`scp -B`
`BindAddress`	`ssh -b` *bind-addr*	`scp -a` *bind-addr*
`Cipher`	`ssh -c` *cipher*	`scp -c` *cipher*
`Ciphers`	`ssh -c` *cipher-spec*	`scp -c` *cipher-spec*
`Compression`	`ssh -C`	`scp -C`
`DynamicForward`	`ssh -D` *SOCKS4-port*	
`EscapeChar`	`ssh -e` *escape-char*	
`ForwardAgent`	`ssh -A` pour activer `ssh -a` pour désactiver	
`ForwardX11`	`ssh -X` pour activer `ssh -x` pour désactiver	
`GatewayPorts`	`ssh -g`	
`IPv4`	`ssh -4`	`scp -4`
`IPv6`	`ssh -6`	`scp -6`
`LocalForward`	`ssh -L` *localport:remotehost:remoteport*	
`MACS`	`ssh -m` *mac-spec*	
`Port`	`ssh -p` *port*	`scp -P` *port*

TABLEAU 20–8 Équivalents de la ligne de commande pour les mots-clés Secure Shell *(Suite)*

Mot-clé	ssh Remplacement de ligne de commande	scp Remplacement de ligne de commande
`Protocol`	`ssh -1` pour v1 uniquement `ssh -2` pour v2 uniquement	
`RemoteForward`	`ssh -R` *remoteport:localhost:localport*	

PARTIE VI

Service Kerberos

Cette section fournit des informations sur la configuration, la gestion et l'utilisation du service Kerberos dans les chapitres suivants :

◆ ◆ ◆ CHAPITRE 21

Introduction au service Kerberos

Ce chapitre présente le service Kerberos. Vous trouverez ci-après une liste des informations de présentation contenues dans ce chapitre.

Description du service Kerberos

Le *service Kerberos* est une architecture client-serveur qui fournit des transactions sécurisées entre des réseaux. Le service assure l'authentification utilisateur fiable, ainsi que l'intégrité et la confidentialité. L'*authentification* garantit que l'identité de l'expéditeur et du destinataire d'une transaction réseau sont toutes deux réelles. Le service peut également vérifier la validité des données transmises (*intégrité*) et le chiffrement des données lors de la transmission (*confidentialité*). À l'aide du service Kerberos, vous pouvez vous connecter à d'autres machines, exécuter des commandes, échanger des données et transférer des fichiers en toute sécurité. En outre, ce service offre des services d'*autorisation*, ce qui permet aux administrateurs de limiter l'accès aux services et aux machines. Par ailleurs, en tant qu'utilisateur Kerberos, vous pouvez réguler l'accès d'autres personnes à votre compte.

Le service Kerberos est un système à *connexion unique*, ce qui signifie que vous ne devez vous authentifier auprès du service qu'une fois par session et toutes les transactions ultérieures au cours de la session sont automatiquement protégées. Une fois authentifié par le service, vous n'avez plus besoin de vous authentifier à chaque utilisation d'une commande basée sur Kerberos, comme `ftp` ou `rsh`, ou pour accéder à des données sur un système de fichiers NFS. Par conséquent, vous n'avez pas à envoyer votre mot de passe sur le réseau, où il peut être intercepté à chaque fois que vous utilisez ces services.

Le service Kerberos d'Oracle Solaris est basé sur le protocole d'authentification réseau Kerberos V5 développé au Massachusetts Institute of Technology (MIT). Les utilisateurs du produit

Kerberos V5 devraient donc trouver la version Oracle Solaris très familière. Le protocole Kerberos V5 étant une norme *de facto* de l'industrie en matière de réseau, la version d'Oracle Solaris favorise l'interopérabilité avec d'autres systèmes. En d'autres termes, puisque le service Kerberos d'Oracle Solaris fonctionne avec les systèmes utilisant le protocole Kerberos V5, ce service permet de sécuriser les transactions même sur des réseaux hétérogènes. En outre, le service assure l'authentification et la sécurité entre les domaines et au sein d'un domaine unique.

Le service Kerberos offre une plus grande flexibilité dans l'exécution des applications Oracle Solaris. Vous pouvez configurer ce service pour autoriser les demandes de services réseau Kerberos et non-Kerberos, notamment les services NFS, `telnet` et `ftp`. Par conséquent, les applications actuelles fonctionnent toujours, même si elles sont en cours d'exécution sur des systèmes sur lesquels le service Kerberos n'est pas activé. Bien entendu, vous pouvez également configurer le service Kerberos pour n'autoriser que les requêtes de réseau Kerberos.

Le service Kerberos fournit un mécanisme de sécurité permettant d'utiliser Kerberos pour l'authentification, l'intégrité et la confidentialité lors de l'utilisation d'applications ayant recours à GSS-API (API générique de services de sécurité). Toutefois, il n'est pas nécessaire que les applications restent dédiées au service Kerberos si d'autres mécanismes de sécurité sont développés. Étant donné que le service est conçu pour s'intégrer de façon modulaire à GSS-API, les applications qui l'utilisent peuvent utiliser le mécanisme de sécurité le plus adapté à leurs besoins.

Fonctionnement du service Kerberos

Vous trouverez ci-dessous une présentation de l'authentification Kerberos. Pour une description plus détaillée, reportez-vous à la section "Fonctionnement du système d'authentification Kerberos" à la page 580.

Du point de vue de l'utilisateur, le service Kerberos est pratiquement invisible une fois la session Kerberos démarrée. Les commandes telles que `rsh` ou `ftp` fonctionnent de la même manière. L'initialisation d'une session Kerberos n'implique souvent rien de plus que la connexion et l'indication du mot de passe Kerberos.

Le système Kerberos est basé sur le concept de *ticket*. Un ticket est un ensemble d'informations électroniques qui identifient un utilisateur ou un service tel que le service NFS. Tout comme votre permis de conduire vous identifie et indique les privilèges de conduite dont vous disposez, un ticket vous identifie ainsi que vos privilèges d'accès au réseau. Lorsque vous effectuez une transaction basée sur Kerberos (par exemple, si vous vous connectez à distance à une autre machine), vous envoyez de façon transparente une demande de ticket à un *KDC* (Key Distribution Center, centre de distribution des clés). Le KDC accède à une base de données pour authentifier votre identité et renvoie un ticket qui vous autorise à accéder à l'autre machine. "De façon transparente" signifie que vous n'avez pas à demander explicitement un

ticket. La demande s'effectue dans le cadre de la commande `rlogin`. Puisque seul un client authentifié peut obtenir un ticket d'un service particulier, un autre client ne peut pas utiliser `rlogin` sous une fausse identité.

Certains attributs sont associés aux tickets. Par exemple, un ticket peut être *transmissible*, ce qui signifie qu'il peut être utilisé sur un autre ordinateur sans nouveau processus d'authentification. Un ticket peut également être *postdaté*, ce qui signifie qu'il n'est pas valide avant une heure spécifiée. Les utilisations des tickets, par exemple, pour spécifier quels utilisateurs sont autorisés à obtenir quels types de ticket, sont définies par des *stratégies*. Les stratégies sont déterminées lors de l'installation ou de l'administration de Kerberos.

Remarque – Vous rencontrerez fréquemment les termes *informations d'identification* et *ticket*. Dans l'univers Kerberos, ils sont souvent utilisés de façon interchangeable. D'un point de vue technique, cependant, les informations d'identification correspondent à un ticket et à la *clé de session* pour cette session. Cette différence est expliquée plus en détail à la section "Obtention de l'accès à un service à l'aide de Kerberos" à la page 581.

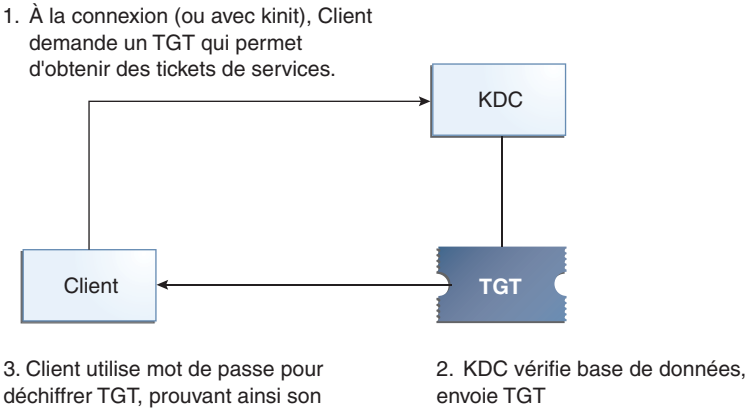
Les sections suivantes expliquent davantage les processus d'authentification Kerberos.

Authentification initiale : le TGT

L'authentification Kerberos comprend deux phases : une authentification initiale qui autorise toutes les authentifications, puis les authentifications suivantes.

La figure ci-dessous illustre la manière dont l'authentification initiale a lieu.

FIGURE 21–1 Authentification Kerberos initiale pour une session



1. Un client (un utilisateur, ou un service comme NFS) commence une session Kerberos en demandant un *TGT* (ticket d'octroi de tickets) dans le KDC (centre de distribution de clés). Cette demande est souvent effectuée automatiquement à la connexion.

   Un TGT est nécessaire pour obtenir d'autres tickets pour des services spécifiques. Considérez le TGT comme étant semblable à un passeport. Comme un passeport, le TGT vous identifie et vous permet d'obtenir de nombreux "visas", où les "visas" (tickets) ne sont pas des pays étrangers mais des machines distantes ou des services réseau. Comme les passeports et les visas, le TGT et les autres différents tickets ont une durée de vie limitée. La seule différence réside dans le fait que les commandes Kerberos voient que vous avez un passeport et qu'elles obtiennent les visas pour vous. Vous n'avez pas à effectuer les transactions vous-même.

   Une autre analogie pour le TGT est celle du passe de ski de trois jours valable dans quatre différentes stations. Vous pouvez montrer le passe dans la station de votre choix et vous recevez un ticket pour les pistes correspondantes, tant que le passe n'a pas expiré. Une fois que vous avez accès aux pistes, vous pouvez skier autant que vous le voulez dans cette station. Si vous passez à une autre station le jour suivant, vous devez montrer votre passe à nouveau, et vous obtenez l'accès aux pistes de la nouvelle station. La différence réside dans le fait que les commandes Kerberos voient que vous avez un passe de ski de trois jours, et qu'elles obtiennent l'accès aux pistes pour vous. Ainsi, vous n'avez pas à effectuer les opérations vous-même.

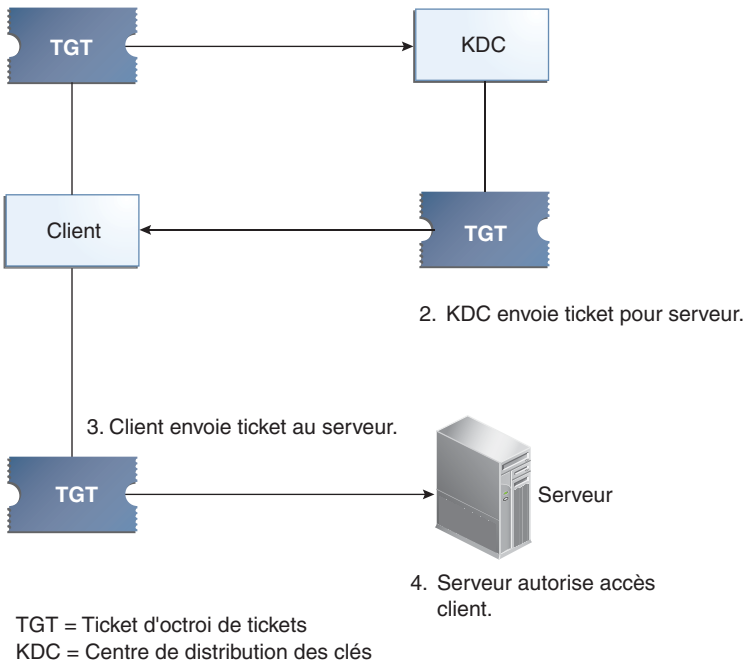
2. Le KDC crée un TGT qu'il renvoie, sous forme chiffrée, au client. Le client déchiffre le TGT en utilisant le mot de passe du client.

3. Maintenant en possession d'un TGT en cours de validité, le client peut demander des tickets pour toutes sortes d'opérations réseau, telles que `rlogin` ou `telnet`, aussi longtemps que le TGT est valide. Ce ticket dure généralement quelques heures. À chaque fois que le client effectue une opération réseau unique, il demande un ticket pour cette opération au KDC.

Authentifications Kerberos suivantes

Une fois que le client a reçu l'authentification initiale, chaque nouvelle authentification suit le modèle indiqué dans la figure ci-dessous.

FIGURE 21–2 Obtention de l'accès à un service à l'aide de l'authentification Kerberos



1. Le client demande un ticket au KDC pour un service particulier, par exemple, pour se connecter à distance à une autre machine, en envoyant au KDC son TGT comme preuve d'identité.
2. Le KDC envoie le ticket pour le service spécifique au client.

Par exemple, si l'utilisateur `joe` demande l'accès à un système de fichiers NFS qui a été partagé avec `krb5`, l'authentification est nécessaire. Puisqu'il est déjà authentifié (c'est-à-dire, qu'il possède déjà un TGT), lorsqu'il tente d'accéder aux fichiers, le système client NFS obtient automatiquement et de façon transparente un ticket du KDC pour le service NFS.

Par exemple, supposons que l'utilisateur `joe` utilise `rlogin` sur le serveur `boston`. Comme il est déjà authentifié, c'est-à-dire qu'il a déjà un TGT, il obtient automatiquement et de façon transparente un ticket en tant que partie de la commande `rlogin`. Ce ticket lui permet de se connecter à distance à `boston` aussi souvent qu'il le souhaite jusqu'à expiration du ticket. Si `joe` veut se connecter à distance à la machine `denver`, il obtient un autre ticket, comme à l'étape 1.

3. Le client envoie le ticket au serveur.

   Lors de l'utilisation du service NFS, le client NFS envoie le ticket automatiquement et de manière transparente au service NFS pour le serveur NFS.

4. Le serveur autorise l'accès au client.

Ces étapes montrent que le serveur ne communique pas toujours avec le KDC. Cependant, le serveur s'enregistre auprès du KDC, tout comme le premier client. À des fins de simplification, cette partie a été omise.

Applications distantes Kerberos

Les commandes basées sur Kerberos disponibles pour un utilisateur comme `joe` sont les suivantes :

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Ces applications sont les mêmes que les applications Solaris du même nom. Cependant, elles ont été étendues pour utiliser les principaux Kerberos pour authentifier les transactions, afin que vous disposiez d'une sécurité Kerberos. Pour plus d'informations sur les principaux, reportez-vous à la section “Principaux Kerberos” à la page 403

Ces commandes sont traitées plus en détail à la section “Commandes utilisateur Kerberos ” à la page 564.

Principaux Kerberos

Un client dans le service Kerberos est identifié par son *principal*. Un principal est une identité unique à laquelle le KDC peut affecter les tickets. Un principal peut être un utilisateur, comme `joe`, ou un service, tel que `nfs` ou `telnet`.

Par convention, un nom de principal est divisé en trois composants : le *primaire*, l'*instance* et le *domaine*. Un principal Kerberos type peut être, par exemple, `joe/admin@ENG.EXAMPLE.COM`. Dans cet exemple :

- `joe` est le primaire. Le primaire peut être un nom d'utilisateur, comme ici, ou un service, comme `nfs`. Le primaire peut également être l'`hôte`, ce qui signifie que ce principal est un principal de service qui est configuré afin de fournir divers services réseau, `ftp`, `rcp`, `rlogin` etc.
- `admin` est l'instance. Une instance est facultative dans le cas de principaux d' utilisateur, mais elle est nécessaire pour les principaux de service. Par exemple, si l'utilisateur `joe` agit parfois en tant qu'administrateur système, il peut utiliser `joe/admin` pour se distinguer dans son identité d'utilisateur habituelle. De même, si `joe` a des comptes sur deux hôtes différents, il peut utiliser deux noms de principal avec différentes instances, par exemple, `joe/denver.example.com` et `joe/boston.example.com`. Notez que le service Kerberos traite `joe` et `joe/admin` comme deux identités totalement différentes.

  Dans le cas d'un principal de service, l'instance est le nom d'hôte complet. `bigmachine.eng.example.com` est un exemple d'une telle instance. Le principal ou l'instance pour cet exemple pourrait être `ftp/bigmachine.eng.example.com` ou `host/bigmachine.eng.example.com`.
- `ENG.EXAMPLE.COM` est le domaine Kerberos. Les domaines sont abordés dans “Domaines Kerberos” à la page 403.

Les éléments suivants sont tous les noms de principaux valides :

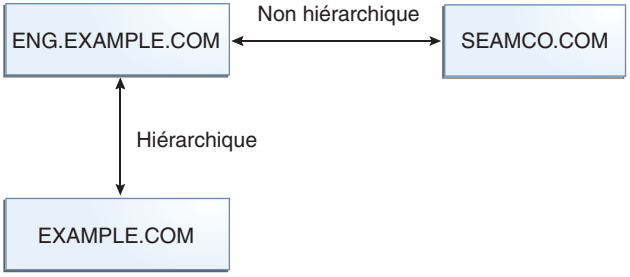
- `joe`
- `joe/admin`
- `joe/admin@ENG.EXAMPLE.COM`
- `nfs/host.eng.example.com@ENG.EXAMPLE.COM`
- `host/eng.example.com@ENG.EXAMPLE.COM`

Domaines Kerberos

Un *domaine* est un réseau logique qui définit un groupe de systèmes sous le même *KDC maître*. La Figure 21–3 montre comment les domaines peuvent se rapporter les uns aux autres. Certains domaines sont hiérarchiques, où un domaine est un surensemble de l'autre domaine. Dans le cas contraire, les domaines sont non hiérarchiques (ou "directs") et le mappage entre les deux domaines doit être défini. Une fonction du service Kerberos est d'autoriser l'authentification au

sein des domaines. Chaque domaine a seulement besoin de disposer d'une entrée de principal pour l'autre domaine dans son KDC. Cette fonction Kerberos est appelée *authentification inter-domaine*.

FIGURE 21–3 Domaines Kerberos



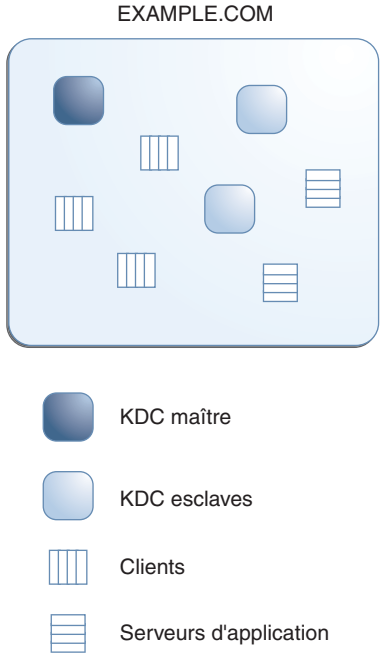
Serveurs Kerberos

Chaque domaine doit inclure un serveur qui gère la copie principale de la base de données du principal. Ce serveur est appelé le *serveur KDC maître*. En outre, chaque domaine doit contenir au moins un *serveur KDC esclave*, qui contient des copies de la base de données du principal. Le serveur KDC maître et le serveur KDC esclave créent tous deux des tickets utilisés pour établir l'authentification.

Le domaine peut également inclure un *serveur d'application* Kerberos. Ce serveur permet d'accéder aux services utilisant Kerberos (tels que `ftp`, `telnet`, `rsh` et NFS). Si vous avez installé SEAM 1.0 ou 1.0.1, le domaine peut inclure un serveur d'application de réseau Kerberos, mais ce logiciel n'a pas été inclus avec ces versions.

La figure suivante illustre le contenu possible d'un domaine.

FIGURE 21–4 Domaine Kerberos typique



Services de sécurité Kerberos

En plus d'assurer l'authentification sécurisée des utilisateurs, le service Kerberos fournit deux services de sécurité :

- **Intégrité :** tout comme l'authentification permet de s'assurer que les clients sur un réseau sont bien ceux qu'ils prétendent être, l'intégrité des données permet de s'assurer que les données qu'ils envoient sont valides et qu'elles n'ont pas été falsifiées pendant le transport. L'intégrité est assurée par l'intermédiaire de la somme de contrôle des données. L'intégrité inclut également l'authentification de l'utilisateur.
- **Confidentialité :** la confidentialité renforce la sécurité. La confidentialité n'inclut pas seulement la vérification de l'intégrité des données transmises, mais elle chiffre en outre les données avant leur transmission, afin de les protéger contre les écoutes électroniques. La confidentialité permet également d'authentifier les utilisateurs.

Les développeurs peuvent concevoir des applications basées sur RPC pour choisir un service de sécurité en utilisant l'interface de programmation RPCSEC_GSS.

Composants des différentes versions Kerberos

Les composants du service Kerberos ont été inclus dans de nombreuses versions. À l'origine, le service Kerberos et les modifications apportées au système d'exploitation de base pour la prise en charge du service Kerberos ont été distribués sous le nom du produit SEAM (Sun Enterprise Authentication Mecanism). À mesure que d'autres parties du produit SEAM ont été incluses dans le logiciel Oracle Solaris, le contenu de la version Oracle Solaris a diminué. Pour les versions Oracle Solaris, tous les éléments du produit SEAM sont inclus, de sorte que le produit SEAM n'est pas nécessaire. Le nom de produit SEAM figure dans la documentation pour des raisons historiques.

Le tableau suivant décrit les composants inclus dans chaque version. Les versions de produit sont répertoriées dans l'ordre chronologique. Tous les composants sont décrits dans les sections suivantes.

TABLEAU 21–1 Contenu de version Kerberos

Nom de version	Contenu
SEAM 1.0 dans Solaris Easy Access Server 3.0	Version complète du service Kerberos pour les versions Solaris 2.6 et 7
Service Kerberos dans la version Solaris 8	Logiciel client Kerberos uniquement
SEAM 1.0.1 dans Solaris 8 Admin Pack	KDC Kerberos et applications distantes pour la version Solaris 8
Service Kerberos dans la version Solaris 9	Fonctionnalité KDC et logiciel client uniquement
SEAM 1.0.2	Applications distantes Kerberos pour la version Solaris 9
Service Kerberos dans la version Solaris10	Version complète du service Kerberos avec améliorations

Composants Kerberos

Similaire à la distribution par MIT du produit Kerberos V5, le service Kerberos Oracle Solaris comprend les éléments suivants :

- KDC (Key Distribution Center) :
  - Démon d'administration de base de données Kerberos : `kadmind`.
  - Démon de traitement des tickets Kerberos : `krb5kdc` .
  - Programmes d'administration de base de données : `kadmin` (maître uniquement), `kadmin.local` et `kdb5_util`.
  - Logiciel de propagation de base de données : `kprop` (esclave uniquement) et `kpropd`.

- Programmes utilisateur de gestion des identifiants : `kinit` , `klist` et `kdestroy`.
- Programme utilisateur de modification du mot de passe Kerberos : `kpasswd`.
- Applications distantes : `ftp`, `rcp`, `rdist`, `rlogin` , `rsh`, `ssh` et `telnet`.
- Démons d'application distante : `ftpd`, `rlogind`, `rshd`, `sshd` et `telnetd`.
- Utilitaire d'administration de keytab : `ktutil`.
- GSS-API (API de service de sécurité générique) : permet aux applications d'utiliser plusieurs mécanismes de sécurité sans avoir à recompiler l'application à chaque fois qu'un nouveau mécanisme est ajouté. GSS-API utilise les interfaces standard permettant aux applications d'être portables pour de nombreux systèmes d'exploitation. GSS-API permet aux applications d'inclure les services de sécurité d'intégrité et de confidentialité, ainsi que l'authentification. Les commandes `ftp` et `ssh` utilisent GSS-API.
- RPCSEC_GSS API : permet d'activer les services NFS afin d'utiliser l'authentification Kerberos. RPCSEC_GSS est une variante de sécurité fournissant des services de sécurité indépendants des mécanismes utilisés. RPCSEC_GSS est installé sur la couche GSS-API. N'importe quel mécanisme de sécurité enfichable basé sur GSS_API peut être utilisé par des applications utilisant RPCSEC_GSS.

En outre, le service Kerberos Oracle Solaris inclut les éléments suivants :

- Outil d'administration graphique Kerberos (`gkadmin`) : permet d'administrer les principaux et les stratégies des principaux. Cette interface graphique basée sur Java est une alternative à la commande `kadmin`.
- Module de service Kerberos V5 pour PAM : assure l'authentification, la gestion de compte, la gestion de session et la gestion des mots de passe pour le service Kerberos. Le module peut être utilisé pour que l'authentification Kerberos soit transparente pour l'utilisateur.
- Modules de noyau : fournissent des implémentations basées sur le noyau du service Kerberos pour une utilisation par le service NFS, ce qui améliore considérablement les performances.

Ajouts Kerberos dans la version 5/08 de Solaris 10

Ces améliorations sont disponibles à compter de la version 5/08 de Solaris 10 :

- Le logiciel Solaris Kerberos a été synchronisé avec la version MIT 1.4. En particulier, le logiciel pour le KDC, la commande `kinit` et le mécanisme Kerberos ont été mis à jour.
- La prise en charge de l'accès aux enregistrement de principaux et de stratégie Kerberos à l'aide de LDAP à partir d'un serveur d'annuaire a été ajoutée. Cette modification simplifie l'administration et peut fournir une plus grande disponibilité, selon le déploiement des KDC et des DS. Reportez-vous à la section "Gestion d'un KDC sur un serveur d'annuaire LDAP" à la page 492 pour obtenir une liste des procédures relatives à LDAP.

- La prise en charge des clients Solaris sans configuration supplémentaire a été ajoutée à cette version. Des modifications ont été apportées au service Kerberos et à certains paramètres par défaut. Les clients Solaris Kerberos fonctionnent sans configuration côté client dans des environnements correctement configurés. Pour plus d'informations, reportez-vous à la section "Options de configuration du client" à la page 421.

Ajouts Kerberos dans la version Solaris 10 8/07

L'API MIT Kerberos V5 (krb5-api) est prise en charge dans la version Solaris 10 8/07. Pour plus d'informations, reportez-vous aux pages de manuel `libkrb5`(3LIB) et `krb5-config`(1). Reportez-vous également aux pages web du projet MIT Kerberos V5 sur mit.edu pour obtenir une documentation plus détaillée dès qu'elle sera disponible.

Bien que krb5-api soit désormais disponible, Sun encourage vivement l'utilisation de GSS-API pour l'authentification réseau, ainsi que l'intégrité et la confidentialité, car GSS-API est un mécanisme de sécurité indépendant et une norme IETF. Pour plus d'informations, reportez-vous à la page de manuel `libgss(3LIB)`.

Ajouts Kerberos dans la version 6/06 de Solaris10

Dans la version 6//06 de Solaris10, le démon `ktkt_warnd` peut renouveler automatiquement les informations d'identification, et pas uniquement avertir l'utilisateur de leur prochaine expiration. L'utilisateur doit être connecté pour que les informations d'identification soient renouvelées automatiquement.

Améliorations Kerberos dans la version 3/05 de Solaris10

Les améliorations suivantes de Kerberos sont incluses dans la version Oracle Solaris. Plusieurs améliorations ont été introduites dans les précédentes versions de Software Express et mises à jour dans les versions bêta de Solaris10.

- Les applications distantes, telles que `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` et `telnet`, prennent en charge le protocole Kerberos. Pour plus d'informations, reportez-vous aux pages de manuel correspondant à chaque commande ou démon et à la page de manuel `krb5_auth_rules(5)`.
- Grâce à la mise à jour incrémentielle rendue désormais possible, il n'est plus nécessaire de systématiquement transférer l'intégralité de la base de données de principaux Kerberos. La propagation incrémentielle présente les avantages suivants :
  - une meilleure cohérence des bases de données entre les serveurs ;
  - un besoin moindre en ressources, telles que les ressources réseau et CPU ;
  - une propagation des mises à jour bien plus adéquate ;

  - une automatisation de la méthode de propagation.
- Un nouveau script aide les administrateurs à définir rapidement et facilement un client Kerberos, en permettant une configuration automatique de ce dernier. Pour obtenir des instructions sur l'utilisation du nouveau script, reportez-vous à la section "Configuration des clients Kerberos" à la page 456. Pour plus d'informations, reportez-vous également à la page de manuel `kclient(1M)`.
- Plusieurs nouveaux types de chiffrement ont été ajoutés au service Kerberos. Ils viennent renforcer la sécurité et améliorer la compatibilité avec d'autres mises en œuvre Kerberos prenant en charge ces types de chiffrement. Pour plus d'informations, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584. Les types de chiffrement sont les suivants :
  - Le type de chiffrement AES peut être utilisé pour le chiffrement à haute vitesse et haute sécurité des sessions Kerberos.
  - ARCFOUR-HMAC offre une meilleure compatibilité avec les autres implémentations de Kerberos.
  - Le chiffrement triple DES (3DES) avec SHA1 accroît la sécurité. Ce type de chiffrement améliore par ailleurs l'interopérabilité avec d'autres mises en œuvre Kerberos le prenant en charge.
- Les types de chiffrement sont activés par le biais de la structure cryptographique. Cette structure peut fournir une cryptographie avec accélération matérielle pour le service Kerberos.
- Le logiciel KDC, les commandes utilisateur et les applications utilisateur prennent désormais en charge l'utilisation du protocole réseau TCP. Cette amélioration augmente la fiabilité des opérations et accroît l'interopérabilité avec les autres mises en œuvre Kerberos, y compris Active Directory de Microsoft. KDC écoute maintenant à la fois les ports UDP traditionnels et les ports TCP, de sorte qu'il peut répondre aux requêtes dans l'un des deux protocoles. Les commandes utilisateur et les applications essaient d'abord d'utiliser UDP lors de l'envoi d'une requête au KDC et, en cas d'échec, essaient TCP.
- La prise en charge d'IPv6 a été ajoutée au logiciel KDC avec les commandes `kinit`, `klist` et `kprop`. Par défaut, les adresses IPv6 sont prises en charge. Aucun paramètre de configuration n'a besoin d'être modifié pour activer la prise en charge d'IPv6. Aucun support pour IPv6 n'est disponible pour les commandes `kadmin` et `kadmind`.
- Une nouvelle option `-e` a été ajoutée à plusieurs sous-commandes de la commande `kadmin`. Elle permet de sélectionner le type de chiffrement lors de la création des principaux. Pour plus d'informations, reportez-vous à la page de manuel `kadmin(1M)`.
- Des ajouts au module `pam_krb5` permettent de gérer le cache des informations d'identification Kerberos à l'aide de la structure des modules PAM. Pour plus d'informations, reportez-vous à la page de manuel `pam_krb5(5)`.
- La détection automatique de KDC, du serveur d'administration, du serveur kpasswd et des mappages de nom de domaine ou d'hôte-domaine de Kerberos utilisant les recherches DNS est prise en charge. Cette amélioration élimine certaines étapes requises pour l'installation

d'un client Kerberos. Ce dernier est capable de localiser un serveur KDC à l'aide du DNS plutôt qu'en procédant à la lecture d'un fichier de configuration. Pour plus d'informations, reportez-vous à la page de manuel `krb5.conf(4)`.

- Un nouveau module PAM appelé `pam_krb5_migrate` a été intégré. Il facilite la migration automatique des utilisateurs vers le domaine Kerberos local si les utilisateurs ne disposent pas encore d'un compte Kerberos. Pour plus d'informations, reportez-vous à la page de manuel `pam_krb5_migrate(5)`.
- Le fichier `~/.k5login` peut désormais être utilisé avec les applications GSS, `ftp` et `ssh`. Pour plus d'informations, reportez-vous à la page de manuel `gss_auth_rules(5)`.
- L'utilitaire `kproplog` a été mis à jour pour afficher tous les noms d'attributs par entrée de journal. Pour plus d'informations, reportez-vous à la page de manuel `kproplog(1M)`.
- Une vérification stricte du TGT peut maintenant être désactivée à l'aide d'une option de configuration dans le fichier `krb5.conf`. Pour plus d'informations, reportez-vous à la page de manuel `krb5.conf(4)`.
- Les extensions des utilitaires de modification de mot de passe permettent au serveur d'administration Kerberos V5 d'Oracle Solaris d'accepter les demandes de modification de mot de passe émises par des clients qui n'exécutent pas le logiciel Oracle Solaris. Pour plus d'informations, reportez-vous à la page de manuel `kadmind(1M)`.
- L'emplacement par défaut du cache de rediffusion a été modifié : auparavant sur les systèmes de fichiers RAM, il se trouve désormais sous `/var/krb5/rcache/`, dans un emplacement de stockage persistant. Le nouvel emplacement empêche les rediffusions en cas de réinitialisation d'un système. Le code rcache a été amélioré sur le plan des performances. Toutefois, les performances générales du cache de rediffusion risquent d'être ralenties en raison de l'utilisation d'un stockage persistant.
- Le cache de rediffusion peut maintenant être configuré en vue de l'utilisation du stockage de fichiers ou de mémoire uniquement. Reportez-vous à la page de manuel `krb5envvar(5)` pour plus d'informations sur les variables d'environnement pouvant être configurées pour les emplacements ou types de cache d'informations d'identification et de table de clés.
- La table d'informations d'identification des services GSS n'est plus nécessaire pour le mécanisme GSS de Kerberos. Pour plus d'informations, reportez-vous à la section "Mappage d'informations d'identification GSS sur des informations d'identification UNIX" à la page 420 ou aux pages de manuel `gsscred(1M)`, `gssd(1M)` et `gsscred.conf(4)`.
- Les utilitaires Kerberos, `kinit` et `ktutil` sont désormais basés sur la version 1.2.1 de MIT Kerberos. Ce changement a apporté de nouvelles options à la commande `kinit` et de nouvelles sous-commandes à la commande `ktutil`. Pour plus d'informations, reportez-vous aux pages de manuel `kinit(1)` and `ktutil(1)`.
- Le KDC Oracle Solaris (Solaris Kerberos Key Distribution Center) et `kadmind` sont désormais basés sur MIT Kerberos version 1.2.1. Le KDC utilise désormais par défaut la base de données btree, plus fiable que l'actuelle base de données basée sur le hachage. Pour plus d'informations, reportez-vous à la page de manuel `kdb5_util(1M)`

- Les démons `kpropd`, `kadmind`, `krb5kdc` et `ktkt_warnd` sont gérés par l'utilitaire de gestion des services. Les actions d'administration appliquées à ce service (activation, désactivation ou redémarrage, par exemple), peuvent être réalisées à l'aide de la commande `svcadm`. La commande `svcs` permet de connaître l'état de service de tous les démons. Pour une présentation de SMF, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*.

Composants Kerberos dans la version Solaris 9

La version Solaris 9 comporte tous les composants inclus dans "Composants Kerberos" à la page 406, à l'exception des applications distantes.

Composants SEAM 1.0.2

La version SEAM 1.0.2 inclut les applications distantes. Ces applications sont la seule partie de SEAM 1.0 qui n'ont pas été intégrées à la version Solaris 9. Les composants pour les applications distantes sont les suivants :

- Applications client : `ftp`, `rcp`, `rlogin`, `rsh` et `telnet`.
- Démons de serveur : `ftpd`, `rlogind`, `rshd` et `telnetd`.

Composants Kerberos dans la version Solaris 8

La version Solaris 8 inclut uniquement les parties côté client du service Kerberos, de sorte que de nombreux composants ne sont pas inclus. Ce produit permet aux systèmes qui exécutent la version Solaris 8 de devenir des clients Kerberos sans devoir installer SEAM 1.0.1 séparément. Pour utiliser ces fonctionnalités, vous devez installer un KDC qui utilise Solaris Easy Access Server 3.0, l'Admin Pack Solaris 8, la distribution MIT ou Windows 2000. Les composants côté client ne sont pas utiles sans un KDC configuré pour distribuer les tickets. Les composants suivants sont inclus dans cette version :

- Programmes utilisateur pour l'obtention, l'affichage et la suppression des tickets : `kinit`, `klist` et `kdestroy`.
- Programme utilisateur de modification du mot de passe Kerberos : `kpasswd`.
- Utilitaire d'administration de keytab : `ktutil`.
- Ajouts au PAM (Pluggable Authentication Module, module d'authentification enfichable) : permet aux applications d'utiliser divers mécanismes d'authentification. Le module PAM peut être utilisé rendre les connexions et déconnexions transparentes pour l'utilisateur.
- Plug-ins GSS_API : fournit le protocole Kerberos et assure la prise en charge de la cryptographie.
- Client NFS et prise en charge du serveur.

Composants SEAM 1.0.1

La version 1.0.1 de SEAM inclut tous les composants de la version 1.0 de SEAM qui ne sont pas déjà inclus dans la version Solaris 8. Les composants sont les suivants :

- KDC (Key Distribution Center) (maître) :
  - Démon d'administration de base de données Kerberos : `kadmind`.
  - Démon de traitement des tickets Kerberos : `krb5kdc`
- KDC esclaves.
- Programmes d'administration de base de données : `kadmin` et `kadmin.local`.
- Logiciel de propagation de base de données : `kprop`.
- Applications distantes : `ftp`, `rcp`, `rlogin`, `rsh` et `telnet`.
- Démons d'application à distance : `ftpd`, `rlogind`, `rshd` et `telnetd`.
- Utilitaire d'administration : `kdb5_util`.
- Outil d'administration graphique Kerberos (`gkadmin`) : permet d'administrer les principaux et les stratégies des principaux. Cette interface graphique basée sur Java est une alternative à la commande `kadmin`.
- Procédure de préconfiguration : permet de définir les paramètres d'installation et de configuration de SEAM 1.0.1, ce qui automatise l'installation de SEAM. Cette procédure s'avère particulièrement utile pour les installations multiples.
- Plusieurs bibliothèques.

Composants SEAM 1.0

La version 1.0 de SEAM comprend tous les éléments inclus dans “Composants Kerberos” à la page 406, ainsi que les éléments suivants :

- Un utilitaire (`gsscred`) et un démon (`gssd`) : ces programmes aident à mapper les ID d'utilisateur UNIX (UID) aux noms de principaux. Ces programmes sont nécessaires car les serveurs NFS utilisent les UID UNIX pour identifier les utilisateurs et pas les noms de principaux, qui sont stockés sous un format différent.
- GSS-API (API de service de sécurité générique) : permet aux applications d'utiliser plusieurs mécanismes de sécurité sans avoir à recompiler l'application à chaque fois qu'un nouveau mécanisme est ajouté. Puisque GSS-API ne dépend pas d'une machine, elle convient aux applications sur Internet. GSS-API permet aux applications d'inclure les services de sécurité d'intégrité et de confidentialité, ainsi que l'authentification.
- RPCSEC_GSS API : permet d'activer les services NFS afin d'utiliser l'authentification Kerberos. RPCSEC_GSS est une variante de sécurité fournissant des services de sécurité indépendants des mécanismes utilisés. RPCSEC_GSS est installé sur la couche GSS-API. N'importe quel mécanisme de sécurité enfichable basé sur GSS_API peut être utilisé par des applications utilisant RPCSEC_GSS.

- Procédure de préconfiguration : permet de définir les paramètres d'installation et de configuration de SEAM 1.0, ce qui automatise l'installation. Cette procédure s'avère particulièrement utile pour les installations multiples.

◆ ◆ ◆ CHAPITRE 22

Planification du service Kerberos

Ce chapitre doit être étudié par les administrateurs qui sont impliqués dans l'installation et la maintenance du service Kerberos. Le chapitre traite de plusieurs options d'installation et de configuration que les administrateurs doivent résoudre avant d'installer ou de configurer le service.

La liste suivante répertorie les sujets qu'un administrateur système ou d'autres membres du personnel technique compétent doivent étudier :

Intérêt de la planification des déploiements de Kerberos

Avant d'installer le service Kerberos, vous devez résoudre plusieurs problèmes de configuration. Bien que la modification de la configuration après l'installation initiale ne soit pas impossible, certaines modifications peuvent être difficiles à implémenter. En outre, certaines modifications impliquent que le KDC soit reconstruit, de sorte qu'il est préférable d'examiner les objectifs à long terme lorsque vous planifiez votre configuration de Kerberos.

Le déploiement d'une infrastructure Kerberos implique d'effectuer des tâches telles que l'installation de KDC, de créer des clés pour les hôtes et de faire migrer des utilisateurs. La reconfiguration d'un déploiement Kerberos peut être aussi difficile que l'exécution d'un déploiement initial, donc planifiez un déploiement avec soin pour éviter d'avoir à reconfigurer.

Planification de domaines Kerberos

Un *domaine* est réseau logique qui définit un groupe de systèmes qui sont sous le même KDC maître. Comme pour l'établissement d'un nom de domaine DNS, les problèmes tels que le nom de domaine, le nombre et la taille de chaque domaine, ainsi que la relation d'un domaine à d'autres domaines pour l'authentification inter-domaine, doivent être résolus avant de configurer le service Kerberos.

Noms de domaine

Les noms de domaine peuvent être constitués de n'importe quelle chaîne de caractères ASCII. En général, le nom de domaine est le même que celui de votre nom de domaine DNS, sauf que le nom de domaine est en majuscules. Cette convention permet de différencier les problèmes avec le service Kerberos des problèmes avec l'espace de noms DNS, tout en utilisant un nom familier. Si vous ne souhaitez pas utiliser DNS ou que vous choisissez d'utiliser une autre chaîne, vous pouvez utiliser n'importe quelle chaîne. Toutefois, le processus de configuration nécessite plus de travail. L'utilisation de noms de domaine qui suivent les conventions de désignation d'Internet est judicieuse.

Nombre de domaines

Le nombre de domaines requis par votre installation dépend de plusieurs facteurs :

- Le nombre de clients à prendre en charge. Trop de clients dans un domaine rend l'administration plus difficile et finit par vous forcer à diviser le domaine. Les principaux facteurs qui déterminent le nombre de clients pouvant être pris en charge sont les suivants :
  - Quantité de trafic générée par chaque client Kerberos
  - Bande passante du réseau physique
  - Vitesse de l'hôte

  Étant donné que chaque installation aura différentes limitations, aucune règle n'existe pour déterminer le nombre maximum de clients.
- La distance qui les sépare des clients. Configurer plusieurs petits domaines peut avoir un sens si les clients sont dans différentes régions.
- Le nombre d'hôtes disponibles pour être installés en tant que KDC. Chaque domaine doit disposer d'au moins deux serveurs KDC, un serveur maître et un serveur esclave.

L'alignement des domaines Kerberos avec les domaines d'administration est recommandé. Il convient de noter qu'un domaine Kerberos V peut s'étendre sur plusieurs sous-domaines du domaine DNS auquel le domaine correspond.

Hiérarchie des domaines

Lorsque vous configurez plusieurs domaines pour l'authentification inter-domaine, vous devez décider comment lier les domaines entre eux. Vous pouvez établir une relation hiérarchique entre les domaines, ce qui fournit automatiquement les chemins d'accès aux domaines associés. Bien entendu, tous les domaines dans la chaîne hiérarchique doivent être configurés correctement. Les chemins d'accès automatiques peuvent alléger la charge administrative. Cependant, s'il existe de nombreux niveaux de domaines, il se peut que vous ne souhaitiez pas utiliser le chemin par défaut car cela nécessite trop de transactions.

Vous pouvez également choisir d'établir la relation de confiance de manière directe. Une relation de confiance directe est plus utile lorsqu'un trop grand nombre de niveaux hiérarchiques existent entre deux domaines ou lorsqu'il n'existe aucune relation hiérarchique. La connexion doit être définie dans le fichier `/etc/krb5/krb5.conf` sur tous les hôtes qui utilisent la connexion. Par conséquent, certains travaux supplémentaires sont nécessaires. La relation de confiance directe est également appelée relation transitive. Pour une introduction, reportez-vous à "Domaines Kerberos" à la page 403. Pour les procédures de configuration de plusieurs domaines, reportez-vous à la rubrique "Configuration de l'authentification inter-domaine" à la page 445.

Mappage de noms d'hôtes sur des domaines

Le mappage de noms d'hôtes sur des noms de domaine est défini dans la section `domain_realm` du fichier `krb5.conf`. Ces mappages peuvent être définis pour un domaine ou pour des hôtes spécifiques, selon les besoins.

Le DNS peut également être utilisé pour chercher des informations sur le KDC. L'utilisation du DNS facilite la modification des informations car vous n'avez pas besoin de modifier le fichier `krb5.conf` sur tous les clients chaque fois que vous apportez une modification. Pour plus d'informations, reportez-vous à la page de manuel `krb5.conf(4)`.

À partir des versions Solaris Express Developer Edition 1/08 et Solaris 10 5/08, les clients Solaris Kerberos peuvent mieux interopérer avec les serveurs Active Directory. Les serveurs Active Directory peuvent être configurés de façon à fournir le domaine au mappage d'hôte.

Noms des clients et des principaux de service

Lorsque vous utilisez le service Kerberos, le DNS doit être activé sur tous les hôtes. Avec le DNS, le principal doit contenir le nom de domaine complet (FQDN, fully qualified domain name) de chaque hôte. Par exemple, si le nom d'hôte est `boston`, le nom de domaine DNS `example.com` et le nom de domaine `EXAMPLE.COM`, alors le nom de principal de l'hôte doit être `host/boston.example.com@EXAMPLE.COM`. Les exemples de ce manuel nécessitent que le DNS soit configuré et utilisent le nom de domaine complet pour chaque hôte.

Le service Kerberos normalise les noms d'alias d'hôtes par l'intermédiaire du DNS, et utilise le formulaire normalisé (cname) lors de la construction du principal de service pour le service associé. C'est pourquoi, lors de la création d'un principal de service, le composant nom d'hôte des noms des principaux de service doit être la forme normalisée du nom d'hôte du système qui héberge le service.

Ce qui suit est un exemple de la façon dont le service Kerberos normalise les noms d'hôte. Si un utilisateur utilise la commande "ssh alpha.example.com", où `alpha.example.com` est un alias de nom d'hôte DNS pour le cname `beta.example.com`. Lorsque SSH appelle Kerberos et demande un ticket de service hôte pour `alpha.example.com`, le service Kerberos normalise d'`alpha.example.com` à `beta.example.com` et demande un ticket pour le principal de service "host/beta.example.com" au KDC.

Pour les noms de principal qui comprennent le nom de domaine complet (FQDN) de l'hôte, il est important de faire correspondre la chaîne qui décrit le nom de domaine DNS dans le fichier `/etc/resolv.conf`. Le service Kerberos requiert que le nom de domaine DNS soit en minuscules lorsque vous spécifiez le nom de domaine complet (FQDN) pour un principal. Le nom de domaine DNS peuvent inclure des majuscules et des minuscules, mais n'utilisez des lettres minuscules que lorsque vous créez un principal d'hôte. Par exemple, le nom de domaine DNS peut être `example.com`, `Example.COM` ou n'importe quelle autre variante. Le nom du principal d'hôte sera toujours `host/boston.example.com@EXAMPLE.COM`.

En outre, l'utilitaire de gestion des services a été configuré de manière à ce qu'un grand nombre de ces démons ou commandes ne démarre pas si le service de client DNS n'est pas en cours d'exécution. Les démons `kdb5_util`, `kadmind` et `kpropd`, ainsi que la commande `kprop`, sont configurés pour dépendre du service DNS. Pour exploiter au mieux les fonctionnalités disponibles à l'aide du service Kerberos et SMF, vous devez activer le service de client DNS sur tous les hôtes.

Ports pour les services d'administration et le KDC

Par défaut, les ports `88` et `750` sont utilisés pour le KDC, et le port `749` est utilisé pour le démon d'administration du KDC. Des numéros de port différents peuvent être utilisés. Toutefois, si vous modifiez les numéros de port, alors les fichiers `/etc/services` et `/etc/krb5/krb5.conf` doivent être modifiés sur chaque client. En plus de ces fichiers, le fichier `/etc/krb5/kdc.conf` doit être mis à jour sur chaque KDC.

Nombre de KDC esclaves

Les KDC esclaves génèrent des informations d'identification tout comme le KDC maître. Les KDC esclaves fournissent une sauvegarde si le maître n'est plus disponible. Chaque domaine doit avoir au moins un KDC esclave. Des KDC esclaves supplémentaires peuvent être nécessaires, selon les facteurs suivants :

- Nombre de segments physiques dans le domaine. Normalement, le réseau doit être défini de manière à ce que chaque segment puisse fonctionner, au moins de manière minimale, sans le reste du domaine. Pour ce faire, un KDC doit être accessible à partir de chaque segment. Le KDC dans cette instance pourrait être un maître ou un esclave.
- Nombre de clients dans le domaine. En ajoutant plusieurs serveurs KDC esclaves, vous pouvez réduire la charge des serveurs actuels.

Il est possible d'ajouter un trop grand nombre de KDC esclaves. N'oubliez pas que la base de données KDC doit être diffusée vers chaque serveur. Par conséquent, plus le nombre de serveurs KDC installés est grand, plus la mise à jour des données dans l'ensemble du domaine peut être longue. En outre, puisque chaque esclave conserve une copie de la base de données KDC, le risque de violation de sécurité augmente avec le nombre d'esclaves.

Par ailleurs, un ou plusieurs KDC esclaves peuvent facilement être configurés de façon à être échangés avec le KDC maître. L'avantage de configurer au moins un KDC esclave de cette manière est de pouvoir disposer d'un système préconfiguré facile à échanger avec le KDC maître en cas de panne de celui-ci. Pour obtenir des instructions sur la manière de configurer un KDC esclave échangeable, reportez-vous à la section “Échange d'un KDC maître et d'un KDC esclave” à la page 472.

Mappage d'informations d'identification GSS sur des informations d'identification UNIX

Le service Kerberos fournit un mappage par défaut des noms d'informations d'identification GSS sur les noms d'utilisateurs UNIX (UID) pour les applications GSS nécessitant ce mappage, comme NFS. Les noms d'informations d'identification GSS sont équivalents aux noms de principaux Kerberos lors de l'utilisation du service Kerberos. L'algorithme de mappage par défaut consiste à prendre un composant du nom de principal Kerberos et d'utiliser ce composant, qui est le nom primaire du principal, pour rechercher l'UID. La recherche est effectuée dans le domaine par défaut ou tout domaine autorisé à l'aide du paramètre `auth_to_local_realm` dans `/etc/krb5/krb5.conf`. Par exemple, le nom de principal d'utilisateur `bob@EXAMPLE.COM` est mappé sur l'UID de l'utilisateur UNIX nommé `bob` à l'aide de la table de mots de passe. Le nom de principal d'utilisateur `bob/admin@EXAMPLE.COM` n'est pas mappé, car le nom de principal comprend un composant d'instance d'`admin`. Si les mappages par défaut pour les informations d'identification de l'utilisateur sont suffisants, la table des informations d'identification GSS n'a pas besoin d'être renseignée. Dans les versions précédentes, le remplissage de la table des informations d'identification GSS était nécessaire pour faire fonctionner le service NFS. Si le mappage par défaut n'est pas suffisant, par exemple si vous souhaitez mapper un nom de principal contenant un composant d'instance, d'autres méthodes doivent être utilisées. Pour plus d'informations, reportez-vous aux références suivantes :

- “Création d'une table d'informations d'identification” à la page 452
- “Ajout d'une entrée unique à la table d'informations d'identification” à la page 452
- “Procédure de mappage d'informations d'identification entre domaines” à la page 453
- “Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 512

Migration automatique d'utilisateur vers un domaine Kerberos

Les utilisateurs UNIX ne disposant pas de comptes utilisateur valables dans le domaine Kerberos par défaut peuvent être automatiquement migrés à l'aide de la structure PAM. Plus précisément, le module `pam_krb5_migrate` est utilisé dans la pile d'authentification du service PAM. Les services sont configurés de sorte que, chaque fois qu'un utilisateur ne disposant pas d'un principal Kerberos parvient à se connecter à un système à l'aide de son mot de passe, un principal Kerberos est automatiquement créé pour celui-ci. Le mot de passe du nouveau principal est le même que le mot de passe UNIX. Reportez-vous à “Configuration de la migration automatique des utilisateurs dans un domaine Kerberos” à la page 468 pour obtenir des instructions sur la façon d'utiliser le module `pam_krb5_migrate`.

Choix du système de propagation de base de données

La base de données stockée sur le KDC maître doit être régulièrement propagée aux KDC esclaves. Vous pouvez configurer la propagation de la base de données pour qu'elle soit incrémentielle. Le processus incrémentiel propage uniquement les informations mises à jour aux KDC esclaves, plutôt que l'intégralité de la base de données. Pour plus d'informations sur la propagation de base de données, reportez-vous à la section “Administration de la base de données Kerberos” à la page 477.

Si vous n'utilisez pas la propagation incrémentielle, l'une des premières questions à résoudre est la fréquence de mise à jour du KDC esclave. Le besoin d'avoir des informations à jour disponibles pour tous les clients doit être comparé à la durée nécessaire pour effectuer la mise à jour.

Dans les installations de grande taille avec de nombreux KDC dans un domaine, un ou plusieurs esclaves peuvent propager les données de manière à ce que le processus s'effectue en parallèle. Cette stratégie permet de réduire le temps de la mise à jour, mais il augmente également le niveau de complexité dans l'administration du domaine. Pour obtenir une description complète de cette stratégie, reportez-vous à la section “Configuration d'une propagation parallèle” à la page 490.

Synchronisation de l'horloge dans un domaine

Tous les hôtes qui participent au système d'authentification Kerberos doivent avoir leurs horloges internes synchronisées dans une durée maximale spécifiée. Appelée *écart d'horloge*, cette fonction fournit un autre contrôle de sécurité Kerberos. Si l'écart d'horloge est dépassé entre des hôtes participants, les demandes sont rejetées.

Une façon de synchroniser toutes les horloges est d'utiliser le logiciel NTP (Network Time Protocol). Pour plus d'informations, reportez-vous à la section “Synchronisation des horloges entre les KDC et les clients Kerberos” à la page 470. D'autres façons de synchroniser les horloges sont disponibles, de sorte que l'utilisation du protocole NTP n'est pas nécessaire. Cependant, une forme ou une autre de synchronisation doit être utilisée pour empêcher les défaillances d'accès dues à un écart d'horloge.

Options de configuration du client

Une nouvelle fonctionnalité de la version Solaris 10 est l'utilitaire de configuration `kclient`. L'utilitaire peut être exécuté en mode interactif ou non interactif. En mode interactif, l'utilisateur est invité à entrer des valeurs de paramètre spécifiques à Kerberos, ce qui permet à l'utilisateur d'effectuer des modifications sur une installation existante lors de la configuration du client. En mode non interactif, un fichier avec des valeurs de paramètre prédéfinies est

utilisé. Les options de ligne de commande peuvent également être utilisées en mode non interactif. Les modes interactif et non interactif nécessitent moins d'étapes que le processus manuel, ce qui devrait rendre le processus plus rapide et moins sujet aux erreurs.

Dans la version Solaris 10 5/08, des modifications ont été apportées pour autoriser un client Kerberos sans configuration. Si ces règles sont respectées dans votre environnement, aucune procédure de configuration explicite n'est nécessaire pour un client Solaris Kerberos :

- Le service DNS est configuré de façon à renvoyer des enregistrements SRV aux KDC.
- Le nom de domaine correspond au nom de domaine DNS ou le KDC prend en charge les références.
- Le client Kerberos n'exige pas de `keytab`.

Dans certains cas, il peut être préférable de configurer explicitement le client Kerberos :

- Si les références ne sont pas utilisées, la logique d'absence de configuration se base sur le nom de domaine DNS de l'hôte pour déterminer le domaine. Cela introduit un petit risque pour la sécurité, mais celui-ci est beaucoup plus faible que l'activation de `dns_lookup_realm`.
- Le module `pam_krb5` s'appuie sur une entrée de clé d'hôte dans le `keytab`. Cette condition peut être désactivée dans le fichier `krb5.conf`, cependant ce n'est pas recommandé pour des raisons de sécurité. Reportez-vous à la page de manuel `krb5.conf(4)`.
- Le processus sans configuration est moins efficace que la configuration directe et se repose plus sur le DNS. Le processus effectue plus de recherches DNS que les clients configurés directement.

Pour une description de tous les processus de configuration des clients, reportez-vous à la section "Configuration des clients Kerberos" à la page 456

Amélioration de la sécurité de connexion des clients

Dans la version Solaris 10 11/06, dès l'ouverture de la session d'un client, le module `pam_krb5` vérifie que le KDC ayant émis le dernier TGT est le même KDC ayant émis le principal d'hôte du client stocké dans `/etc/krb5/krb5.keytab`. Le module `pam_krb5` vérifie le KDC lorsque le module est configuré dans la pile d'authentification. Pour certaines configurations, telles que des clients DHCP ne stockant pas de principal d'hôte de client, cette vérification doit être désactivée. Pour ce faire, vous devez définir l'option `verify_ap_req_nofail` dans le fichier `krb5.conf` sur false (faux). Pour plus d'informations, reportez-vous à la section "Désactivation de la vérification du TGT" à la page 466

Options de configuration de KDC

À partir de la version Solaris 10 5/08, la prise en charge de l'utilisation de LDAP pour gérer les fichiers de base de données de Kerberos a été ajoutée. Reportez-vous à "Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP" à la page 433 pour obtenir des instructions. L'utilisation de LDAP simplifie l'administration des sites qui nécessitent une meilleure coordination entre les bases de données Solaris Kerberos et leur configuration DS existante.

Types de chiffrement Kerberos

Un *type de chiffrement* est un identificateur qui spécifie l'algorithme de chiffrement, le mode de chiffrement et les algorithmes de hachage utilisés dans le service Kerberos. Les clés dans le service Kerberos sont associées à un type de chiffrement pour identifier l'algorithme et le mode cryptographiques à utiliser lorsque le service effectue des opérations cryptographiques à l'aide de la clé. Types de chiffrement pris en charge :

- `des-cbc-md5`
- `des-cbc-crc`
- `des3-cbc-sha1-kd`
- `arcfour-hmac-md5`
- `arcfour-hmac-md5-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

Remarque – Dans les versions antérieures à Solaris 10 8/07, le type de chiffrement `aes256-cts-hmac-sha1-96` peut être utilisé avec le service Kerberos si les packages Strong Cryptographic non fournis en standard sont installés.

Si vous souhaitez modifier le type de chiffrement, vous devez le faire lors de la création d'une nouvelle base de données de principal. En raison de l'interaction entre le KDC, le serveur et le client, il est difficile de modifier le type de chiffrement sur une base de données existante. Laissez ces paramètres non définis, sauf si vous recréez la base de données. Pour plus d'informations, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584.

Remarque – Si vous avez un KDC maître installé n'exécutant pas la version Solaris 10, le KDC esclave doit être mis à niveau vers la version Solaris 10 avant de mettre à niveau le KDC maître. Un KDC maître Solaris 10 utilise les nouveaux types de chiffrement, ce qu'un esclave plus ancien n'est pas en mesure de faire.

URL d'aide en ligne dans l'outil d'administration graphique de Kerberos

L'URL d'aide en ligne est utilisée par l'outil d'administration graphique de Kerberos, `gkadmin`, donc l'URL doit être correctement définie pour activer le menu Help Contents (Sommaire de l'aide). La version HTML de ce manuel peut être installée sur n'importe quel serveur approprié. Vous pouvez également décider d'utiliser les collections à l'adresse suivante : `http://www.oracle.com/technetwork/indexes/documentation/index.html`.

L'URL est spécifiée dans le fichier krb5.conf lors de la configuration d'un hôte afin d'utiliser le service Kerberos. L'URL doit pointer vers la section "Outil d'administration graphique de Kerberos" du chapitre "Administration des principaux et des stratégies Kerberos (tâches)" de ce manuel. Vous pouvez choisir une autre page HTML, si un autre emplacement est plus approprié.

◆ ◆ ◆ CHAPITRE 23

Configuration du service Kerberos (tâches)

Ce chapitre fournit les procédures de configuration pour les serveurs KDC, les serveurs d'application réseau, les serveurs NFS et les clients Kerberos. L'accès superutilisateur est requis pour un grand nombre de ces procédures ; elles doivent donc être utilisées par les administrateurs système ou les utilisateurs avancés. Les procédures de configuration inter-domaines et d'autres sujets liés aux serveurs KDC sont également abordés.

Liste des sujets abordés dans ce chapitre :

Configuration du service Kerberos (liste des tâches)

Certaines parties de la procédure de configuration dépendent d'autres parties et doivent être effectuées selon un ordre spécifique. Ces procédures établissent souvent les services requis pour utiliser le service Kerberos. D'autres procédures ne sont pas dépendantes de l'ordre et peuvent être effectuées si nécessaire. La liste des tâches ci-dessous présente un ordre suggéré en vue d'une installation Kerberos.

Tâche	Description	Voir
1. Planification de votre installation Kerberos	Permet de résoudre les problèmes de configuration avant de démarrer le processus de configuration du logiciel. La planification permet d'économiser du temps et d'autres ressources sur le long terme.	Chapitre 22, “Planification du service Kerberos”
2. (Facultatif) Installation du NTP	Configure le logiciel NTP (Network Time Protocol) ou un autre protocole de synchronisation d'horloge. Pour que le service Kerberos fonctionne correctement, les horloges de tous les systèmes du domaine doivent être synchronisées.	“Synchronisation des horloges entre les KDC et les clients Kerberos” à la page 470
3. Configuration des serveurs KDC	Configure et construit des serveurs KDC maître et KDC esclave et la base de données KDC pour un domaine.	“Configuration des serveurs KDC” à la page 427
4. (Facultatif) Augmentation de la sécurité sur les serveurs KDC	Permet d'éviter les violations de sécurité sur le serveur KDC.	“Procédure de restriction de l'accès aux serveurs KDC” à la page 495
5. (Facultatif) Configuration des serveurs KDC échangeables	Facilite la tâche d'échange du serveur KDC maître et esclave.	“Configuration d'un KDC échangeable” à la page 472

Configuration de services Kerberos supplémentaires (liste des tâches)

Une fois les étapes requises effectuées, les procédures suivantes peuvent être utilisées, le cas échéant.

Tâche	Description	Voir
Configuration de l'authentification inter-domaine	Active les communications entre deux domaines.	“Configuration de l'authentification inter-domaine” à la page 445
Configuration de serveurs d'application Kerberos	Permet à un serveur de prendre en charge des services tels que `ftp`, `telnet` et `rsh` utilisant l'authentification Kerberos.	“Configuration des serveurs d'application réseau Kerberos” à la page 447
Configuration des clients Kerberos	Permet à un client d'utiliser des services Kerberos.	“Configuration des clients Kerberos” à la page 456
Configuration du serveur NFS Kerberos	Permet à un serveur de partager un système de fichiers requérant l'authentification Kerberos.	“Configuration de serveurs NFS Kerberos” à la page 449
Augmentation du niveau de sécurité sur un serveur d'application	Augmente la sécurité sur un serveur d'application en restreignant l'accès aux transactions authentifiées uniquement.	“Procédure d'activation des applications utilisant Kerberos uniquement” à la page 494

Configuration des serveurs KDC

Une fois que vous avez installé le logiciel Kerberos, vous devez configurer les serveurs KDC. La configuration d'un KDC maître et d'au moins un KDC esclave fournit le service émetteur des informations d'identification. Ces informations d'identification étant la base du service Kerberos, les KDC doivent être installés avant de tenter d'effectuer d'autres tâches.

La différence principale entre un KDC maître et un KDC esclave est que seul le KDC maître peut traiter les demandes d'administration de base de données. Par exemple, la modification d'un mot de passe ou l'ajout d'un nouveau principal doivent s'effectuer sur le KDC maître. Ces modifications peuvent alors être propagées au KDC esclave. Les KDC esclave et maître génèrent tous deux des informations d'identification. Cette fonction fournit une redondance au cas où le KDC maître ne répond pas.

TABLEAU 23–1 Configuration de serveurs KDC (liste des tâches)

Tâche	Description	Voir
Configuration d'un serveur KDC maître	Configure et construit le serveur KDC maître et une base de données d'un domaine à l'aide d'un processus manuel, opération requise pour les installations plus complexes.	"Procédure de configuration manuelle d'un KDC maître" à la page 427
	Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus manuel et à l'aide de LDAP pour le KDC.	"Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP" à la page 433
Configuration d'un serveur KDC esclave	Configure et construit le serveur KDC esclave à l'aide d'un processus manuel, opération requise pour les installations plus complexes.	"Procédure de configuration manuelle d'un KDC esclave" à la page 440
Actualisation des clés principales sur un serveur KDC	Met à jour la clé de session sur un serveur KDC pour utiliser de nouveaux types de chiffrement.	"Procédure d'actualisation des clés TGS sur un serveur maître" à la page 444

▼ Procédure de configuration manuelle d'un KDC maître

Dans cette procédure, la propagation incrémentielle est configurée. En outre, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- `admin` principal = `kws/admin`
- URL de l'aide en ligne = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Remarque – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "URL d'aide en ligne dans l'outil d'administration graphique de Kerberos " à la page 424.

Avant de commencer Cette procédure nécessite que l'hôte soit configuré pour utiliser DNS. Pour obtenir des instructions de nommage spécifiques afin de déterminer si ce maître doit être échangeable, reportez-vous à la section "Échange d'un KDC maître et d'un KDC esclave" à la page 472.

1 Connectez-vous en tant que superutilisateur au KDC maître.

2 Éditez le fichier de configuration Kerberos (`krb5.conf`).

Vous devez modifier les noms de domaine et les noms de serveurs. Pour une description complète de ce fichier, reportez-vous à la page de manuel `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
        }
```

Dans cet exemple, les lignes pour `default_realm` , `kdc`, `admin_server` et toutes les entrées `domain_realm` ont été modifiées. En outre, la ligne définissant `help_url` a été modifiée.

Remarque – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_enctypes` ou `default_tgs_enctypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584.

3 Éditez le fichier de configuration KDC (`kdc.conf`).

Vous devez modifier le nom de domaine. Pour une description complète de ce fichier, reportez-vous à la page de manuel `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
                }
```

Dans cet exemple, la définition du nom de domaine dans la section `realms` a été modifiée. En outre, dans la section `realms`, des lignes ont été ajoutées pour activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal.

Remarque – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `permitted_enctypes`, `supported_enctypes` ou `master_key_type`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584.

---

4 Créez la base de données KDC à l'aide de la commande `kdb5_util`.

La commande `kdb5_util` crée la base de données KDC. En outre, lorsqu'elle est utilisée avec l'option `-s`, cette commande crée un fichier stash utilisé pour authentifier le KDC à lui-même avant le lancement des démons `kadmind` et `krb5kdc`.

```
kdc1 # /usr/sbin/kdb5_util create -s
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:      <Type the key>
Re-enter KDC database master key to verify:      <Type it again>
```

5 Modifiez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC.

```
kws/admin@EXAMPLE.COM    *
```

L'entrée donne au principal `kws/admin` du domaine `EXAMPLE.COM` la possibilité de modifier les principaux ou des stratégies dans le KDC. L'installation par défaut comprend un astérisque (*)

pour correspondre à tous principaux admin. Cette valeur par défaut peut constituer un risque de sécurité, il est donc plus sûr d'inclure une liste de tous les principaux admin. Pour plus d'informations, reportez-vous à la page de manuel kadm5.acl(4).

6 Démarrez la commande kadmin.local et ajoutez les principaux.

Les sous-étapes suivantes créent des principaux utilisés par le service Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

a. Ajoutez des principaux d'administration à la base de données.

Vous pouvez ajouter autant de principaux admin que nécessaire. Vous devez ajouter au moins un principal admin pour terminer le processus de configuration du KDC. Pour cet exemple, un principal kws/admin est ajouté. Vous pouvez remplacer kws par le nom de principal approprié.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM:      <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

b. Créez les principaux kiprop.

Le principal kiprop est utilisé pour autoriser les mises à jour depuis le KDC maître.

```
kadmin.local: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin.local:
```

c. Créez un fichier keytab pour le service kadmind.

Cette séquence de commandes crée un fichier keytab avec les entrées de principal pour kadmin/<FQDN> et changepw/<FQDN>. Ces principaux sont nécessaires pour que le service kadmind et les mots de passe soient modifiés. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier /etc/resolv.conf. Le principal kadmin/changepw est utilisé pour modifier les mots de passe à partir des clients qui n'exécutent pas une version de Solaris.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
```

```
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

d. Ajoutez le principal `kiprop` pour le serveur KDC maître dans le fichier keytab `kadmind`.

L'ajout du principal `kiprop` au fichier `kadm5.keytab` permet à la commande `kadmind` de s'authentifier elle-même lors du lancement de la propagation incrémentielle.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

e. Quittez `kadmin.local`.

Vous avez ajouté toutes les identités requises pour les prochaines étapes.

```
kadmin.local: quit
```

7 Démarrez les démons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

8 Démarrez `kadmin` et ajoutez d'autres principaux.

À ce stade, vous pouvez ajouter les principaux à l'aide de l'outil d'administration graphique Kerberos. Pour ce faire, vous devez vous connecter avec l'un des noms de principal `admin` que

vous avez précédemment créés dans cette procédure. Cependant, l'exemple de ligne de commande suivant est utilisé par souci de simplicité.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Créez l'`host` principal du KDC maître.

L'hôte principal est utilisé par les applications utilisant Kerberos, notamment `kprop`, pour propager les modifications aux KDC esclaves. Ce principal est également utilisé pour fournir un accès à distance sécurisé au serveur KDC à l'aide d'applications, comme `ssh`. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

b. (Facultatif) Créez le principal `kclient`.

Ce principal est utilisé par l'utilitaire `kclient` au cours de l'installation d'un client Kerberos. Si vous n'avez pas l'intention d'utiliser cet utilitaire, vous n'avez pas besoin d'ajouter le principal. Les utilisateurs de l'utilitaire `kclient` doivent utiliser ce mot de passe.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:      <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

c. Ajoutez l'`host` principal au fichier keytab du KDC maître.

L'ajout de l'hôte principal au fichier keytab autorise ce principal à être utilisé automatiquement par des serveurs d'application tels que `sshd` .

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. Quittez `kadmin`.

```
kadmin: quit
```

9 **(Facultatif) Synchronisez l'horloge des KDC maître en utilisant NTP ou un autre mécanisme de synchronisation d'horloge.**

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

10 **Configurez les KDC esclaves.**

Pour assurer la redondance, veillez à installer au moins un KDC esclave. Pour obtenir des instructions spécifiques, reportez-vous à la section "Procédure de configuration manuelle d'un KDC esclave" à la page 440.

▼ Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP

À partir de la version Solaris 10 5/08, un KDC peut être configuré pour utiliser un serveur de données LDAP à l'aide de la procédure suivante.

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- Serveur d'annuaire = `dsserver.example.com`
- `admin` principal = `kws/admin`
- FMRI pour le service LDAP = `svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1`
- URL de l'aide en ligne = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Remarque – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "URL d'aide en ligne dans l'outil d'administration graphique de Kerberos " à la page 424.

Avant de commencer

Cette procédure nécessite également que l'hôte soit configuré pour utiliser DNS. Pour de meilleures performances, installez le KDC et le service d'annuaire LDAP sur le même serveur. En outre, un serveur d'annuaire doit être en cours d'exécution. La procédure ci-dessous fonctionne avec des serveurs utilisant la version Sun Java Directory Server Enterprise Edition.

1. **Connectez-vous en tant que superutilisateur au KDC.**

2. **Créez un certificat pour le serveur d'annuaire et importez le certificat.**

   Les étapes suivantes permettent de configurer un KDC S10 pour utiliser le certificat auto-signé Directory Server 6.1. Si le certificat est arrivé à expiration, suivez les instructions de renouvellement de certificat dans la section "To Manage Self-Signed Certificates" du *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide*.

   a. **Exportez le certificat de serveur d'annuaire auto-signé.**

      ```
      # /usr/sfw/bin/certutil -L -n defaultCert -d /export/sun-ds6.1/directory/alias \
              -P 'slapd-' -a > /var/tmp/ds_cert.pem
      ```

   b. **Créez la base de données de certificats locaux.**

      ```
      # /usr/sfw/bin/certutil -N -d /var/ldap
      ```

   c. **Ajoutez le certificat du répertoire d'annuaire à la base de données de certificats locaux.**

      ```
      # /usr/sfw/bin/certutil -A -n defaultCert -i /var/tmp/ds_cert -a -t CT -d /var/ldap
      ```

   d. **Importez le certificat du serveur d'annuaire.**

```
# pktool setpin keystore=nss dir=/var/ldap
# chmod a+r /var/ldap/*.db
# pktool import keystore=nss objtype=cert trust="CT" infile=/tmp/defaultCert.certutil.der \
        label=defaultCert dir=/var/ldap
```

3. **Renseignez l'annuaire LDAP, si nécessaire.**

4. **Ajoutez le schéma Kerberos pour le schéma existant.**

```
# ldapmodify -h dsserver.example.com -D "cn=directory manager" -f /usr/share/lib/ldif/kerberos.ldif
```

5. **Créez le conteneur Kerberos dans l'annuaire LDAP.**

   Ajoutez les entrées suivantes au fichier `krb5.conf`.

   a. **Définissez le type de base de données.**

      Ajoutez une entrée pour définir le `database_module` sur la section `realms`.

      ```
      database_module = LDAP
      ```

   b. **Définissez le module de base de données.**

      ```
      [dbmodules]
          LDAP = {
              ldap_kerberos_container_dn = "cn=krbcontainer,dc=example,dc=com"
              db_library = kldap
              ldap_kdc_dn = "cn=kdc service,ou=profile,dc=example,dc=com"
              ldap_kadmind_dn = "cn=kadmin service,ou=profile,dc=example,dc=com"
              ldap_cert_path = /var/ldap
              ldap_servers = ldaps://dsserver.example.com
          }
      ```

c. Créez le KDC dans l'annuaire LDAP.

Cette commande crée `krbcontainer` et plusieurs autres objets. Elle crée également un fichier stash de clé principale `/var/krb5/.k5.EXAMPLE.COM`.

```
# kdb5_ldap_util -D "cn=directory manager" create -P abcd1234 -r EXAMPLE.COM -s
```

6 Dissimulez les mots de passe KDC de liaison DN (Distinguished Name, nom distinctif).

Ces mots de passe sont utilisés par le KDC lorsqu'il se connecte au DS. Le KDC utilise des rôles différents en fonction du type d'accès utilisé par le KDC.

```
# kdb5_ldap_util stashsrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
# kdb5_ldap_util stashsrvpw "cn=kadmin service,ou=profile,dc=example,dc=com"
```

7 Ajoutez des rôles de service KDC.

a. Créez un fichier `kdc_roles.ldif` avec un contenu comme suit :

```
dn: cn=kdc service,ou=profile,dc=example,dc=com
cn: kdc service
sn: kdc service
objectclass: top
objectclass: person
userpassword: test123

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: test123
```

b. Créez des entrées de rôle dans l'annuaire LDAP

```
# ldapmodify -a -h dsserver.example.com -D "cn=directory manager" -f kdc_roles.ldif
```

8 Définissez les listes de contrôle d'accès (ACL) pour les rôles relatifs au KDC.

```
# cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
# Set kadmin ACL for everything under krbcontainer.
dn: cn=krbcontainer,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///cn=krbcontainer,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
      acl kadmin_ACL; allow (all)\
      userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)

# Set kadmin ACL for everything under the people subtree if there are
# mix-in entries for krb princs:
dn: ou=people,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///ou=people,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
      acl kadmin_ACL; allow (all)\
      userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)
EOF
```

9 Éditez le fichier de configuration Kerberos (`krb5.conf`).

Vous devez modifier les noms de domaine et les noms de serveurs. Pour une description complète de ce fichier, reportez-vous à la page de manuel `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
        }
```

Dans cet exemple, les lignes pour `default_realm` , `kdc`, `admin_server` et toutes les entrées `domain_realm` ont été modifiées. En outre, la ligne définissant `help_url` a été modifiée.

Remarque – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_enctypes` ou `default_tgs_enctypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “Utilisation des types de chiffrement Kerberos” à la page 584.

---

10 Éditez le fichier de configuration KDC (`kdc.conf`).

Vous devez modifier le nom de domaine. Pour une description complète de ce fichier, reportez-vous à la page de manuel `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
```

```
sunw_dbprop_enable = true
sunw_dbprop_master_ulogsize = 1000
}
```

Dans cet exemple, la définition du nom de domaine dans la section `realms` a été modifiée. En outre, dans la section `realms`, des lignes ont été ajoutées pour activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal.

Remarque – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `permitted_enctypes`, `supported_enctypes` ou `master_key_type`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584.

---

11 Modifiez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC.

```
kws/admin@EXAMPLE.COM    *
```

L'entrée donne au principal `kws/admin` du domaine `EXAMPLE.COM` la possibilité de modifier les principaux ou des stratégies dans le KDC. L'installation par défaut comprend un astérisque (*) pour correspondre à tous principaux `admin`. Cette valeur par défaut peut constituer un risque de sécurité, il est donc plus sûr d'inclure une liste de tous les principaux `admin`. Pour plus d'informations, reportez-vous à la page de manuel `kadm5.acl(4)`.

12 Démarrez la commande `kadmin.local` et ajoutez les principaux.

Les sous-étapes suivantes créent des principaux utilisés par le service Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

a. Ajoutez des principaux d'administration à la base de données.

Vous pouvez ajouter autant de principaux `admin` que nécessaire. Vous devez ajouter au moins un principal `admin` pour terminer le processus de configuration du KDC. Pour cet exemple, un principal `kws/admin` est ajouté. Vous pouvez remplacer `kws` par le nom de principal approprié.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM:     <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

b. Créez un fichier keytab pour le service `kadmind`.

Cette séquence de commande crée un fichier keytab avec les entrées de principaux pour `kadmin` et `changepw`. Ces principaux sont nécessaires pour le service `kadmind`. Notez que

lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

c. Quittez `kadmin.local`.

Vous avez ajouté toutes les identités requises pour les prochaines étapes.

```
kadmin.local: quit
```

13 (Facultatif) Configurez la dépendance LDAP pour les services Kerberos.

Si LDAP et les serveurs KDC sont en cours d'exécution sur le même hôte et que le service LDAP est configuré avec un FMRI SMF, ajoutez une dépendance de service LDAP pour les démons Kerberos. Ceci redémarre le service KDC si le service LDAP est redémarré.

a. Ajoutez la dépendance au service krb5kdc.

```
# svccfg -s security/krb5kdc
svc:/network/security/krb5kdc> addpg dsins1 dependency
svc:/network/security/krb5kdc> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/krb5kdc> setprop dsins1/grouping = astring: "require_all"
```

```
svc:/network/security/krb5kdc> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/krb5kdc> setprop dsins1/type = astring: "service"
svc:/network/security/krb5kdc> exit
```

b. Ajoutez la dépendance au service kadmin.

```
# svccfg -s security/kadmin
svc:/network/security/kadmin> addpg dsins1 dependency
svc:/network/security/kadmin> setprop dsins1/entities =\
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmin> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/kadmin> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmin> setprop dsins1/type = astring: "service"
svc:/network/security/kadmin> exit
```

14 Démarrez les démons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

15 Démarrez `kadmin` et ajoutez d'autres principaux.

À ce stade, vous pouvez ajouter les principaux à l'aide de l'outil d'administration graphique Kerberos. Pour ce faire, vous devez vous connecter avec l'un des noms de principal `admin` que vous avez précédemment créés dans cette procédure. Cependant, l'exemple de ligne de commande suivant est utilisé par souci de simplicité.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Créez l'`host` principal du KDC maître.

L'hôte principal est utilisé par les applications utilisant Kerberos, notamment `klist` et `kprop`. Les clients utilisent ce principal lors du montage d'un système de fichiers NFS authentifié. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

b. (Facultatif) Créez le principal `kclient`.

Ce principal est utilisé par l'utilitaire `kclient` au cours de l'installation d'un client Kerberos. Si vous n'avez pas l'intention d'utiliser cet utilitaire, vous n'avez pas besoin d'ajouter le principal. Les utilisateurs de l'utilitaire `kclient` doivent utiliser ce mot de passe.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:     <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:      <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

c. Ajoutez l'hôte principal au fichier keytab du KDC maître.

L'ajout de l'hôte principal au fichier keytab autorise ce principal à être utilisé de manière automatique.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. Quittez `kadmin`.

```
kadmin: quit
```

16 (Facultatif) Synchronisez l'horloge des KDC maître en utilisant NTP ou un autre mécanisme de synchronisation d'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

17 Configurez les KDC esclaves.

Pour assurer la redondance, veillez à installer au moins un KDC esclave. Pour obtenir des instructions spécifiques, reportez-vous à la section "Procédure de configuration manuelle d'un KDC esclave" à la page 440.

▼ Procédure de configuration manuelle d'un KDC esclave

Dans cette procédure, un nouveau KDC esclave nommé `kdc2` est configuré. En outre, la propagation incrémentielle est configurée. Cette procédure utilise les paramètres de configuration ci-dessous :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com`
- `admin` principal = `kws/admin`

Avant de commencer Le KDC maître doit être configuré. Pour obtenir des instructions spécifiques afin de déterminer si cet esclave doit être échangeable, reportez-vous à la section "Échange d'un KDC maître et d'un KDC esclave" à la page 472.

1 Sur le KDC maître, connectez-vous en tant que superutilisateur.

2 Sur le KDC maître, démarrez `kadmin`.

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Sur le KDC maître, ajoutez des principaux d'hôtes esclaves à la base de données, si ce n'est pas déjà fait.

Pour que l'esclave fonctionne, il doit avoir un hôte principal. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc2.example.com
Principal "host/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

b. Sur le KDC maître, créez le principal `kiprop`.

Le principal `kiprop` est utilisé pour autoriser la propagation incrémentielle à partir du KDC maître.

```
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

c. Quittez `kadmin`.

```
kadmin: quit
```

3 Sur le KDC maître, modifiez le fichier de configuration Kerberos (`krb5.conf`).

Vous devez ajouter une entrée pour chaque esclave. Pour une description complète de ce fichier, reportez-vous à la page de manuel `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
 .
 .
[realms]
                EXAMPLE.COM = {
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                admin_server = kdc1.example.com
        }
```

4 Sur le KDC maître, ajoutez une entrée `kiprop` au fichier `kadm5.acl`.

Cette entrée permet au KDC maître de recevoir des demandes de propagation incrémentielle pour le serveur kdc2.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

5 Sur le KDC maître, redémarrez `kadmind` pour utiliser les nouvelles entrées dans le fichier `kadm5.acl`.

```
kdc1 # svcadm restart network/security/kadmin
```

6 Sur tous les KDC esclaves, copiez les fichiers d'administration à partir du serveur KDC maître.

Cette étape doit être effectuée sur tous les KDC esclaves, car le serveur KDC maître a mis à jour des informations requises par chaque serveur KDC. Vous pouvez utiliser `ftp` ou tout autre mécanisme de transfert similaire pour extraire des copies des fichiers suivants du KDC maître :

- `/etc/krb5/krb5.conf`
- `/etc/krb5/kdc.conf`

7 Sur tous les KDC esclaves, ajoutez une entrée pour le KDC maître et le KDC esclave dans le fichier de configuration de propagation de base de données, `kpropd.acl`.

Ces informations doivent être mises à jour sur tous les serveurs KDC esclaves.

```
kdc2 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

8 Sur tous les KDC esclaves, assurez-vous que le fichier d'ACL Kerberos, `kadm5.acl`, n'est pas renseigné.

Un fichier `kadm5.acl` non modifié ressemble à ce qui suit :

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Si le fichier contient des entrées `kiprop`, supprimez-les.

9 Sur le nouvel esclave, modifiez une entrée de `kdc.conf`.

Remplacez l'entrée `sunw_dbprop_master_ulogsize` par une entrée définissant `sunw_dbprop_slave_poll`. L'entrée définit la durée d'interrogation sur 2 minutes.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
```

```
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_slave_poll = 2m
        }
```

10 Sur le nouvel esclave, démarrez la commande `kadmin`.

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Ajoutez l'hôte principal de l'esclave au fichier keytab de l'esclave en utilisant `kadmin`.

Cette entrée permet à `kprop` et à d'autres applications utilisant Kerberos de fonctionner. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: ktadd host/kdc2.example.com
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

b. Ajoutez le principal `kiprop` au fichier keytab du KDC esclave.

L'ajout du principal `kiprop` au fichier `krb5.keytab` permet à la commande `kpropd` de s'authentifier elle-même lors du lancement de la propagation incrémentielle.

```
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Quittez `kadmin`.

```
kadmin: quit
```

11 Sur le nouvel esclave, démarrez le démon de propagation Kerberos.

```
kdc2 # /usr/lib/krb5/kpropd
```

12 Sur le nouvel esclave, créez un fichier stash à l'aide de `kdb5_util` .

```
kdc2 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key

Enter KDC database master key:      <Type the key>
```

13 Arrêtez le démon de propagation Kerberos.

```
kdc2 # pkill kpropd
```

14 (Facultatif) Sur le nouveau KDC esclave, synchronisez l'horloge du KDC maître à l'aide du protocole NTP ou d'un autre mécanisme de synchronisation de l'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

15 Sur le nouvel esclave, démarrez le démon KDC (`krb5kdc`).

Lorsque le service `krb5kdc` est activé, `kpropd` démarre également si le système est configuré en tant qu'esclave.

```
kdc2 # svcadm enable network/security/krb5kdc
```

▼ Procédure d'actualisation des clés TGS sur un serveur maître

Lorsque le principal de TGS (Ticket Granting Service, service d'octroi de tickets) n'a qu'une clé DES, ce qui est le cas pour les serveurs KDC créés avant la version Solaris10, la clé restreint le type de chiffrement de la clé de session du TGT à DES. Si un KDC est mis à jour pour une version prenant en charge d'autres types de chiffrement renforcés, l'administrateur peut s'attendre à ce que le chiffrement renforcé soit utilisé pour toutes les clés de session générées par le KDC. En revanche, si les clés du principal de TGS ne sont pas actualisées pour inclure les nouveaux types de chiffrement, la clé de session du TGT restera limitée à DES. La procédure suivante actualise la clé afin que d'autres types de chiffrement puissent être utilisés.

- **Actualisez la clé de principal du TGS.**

```
kdc1 % /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Exemple 23–1 Actualisation des clés de principal à partir d'un serveur maître

Si vous n'êtes pas connecté au KDC maître en tant que `root`, vous pouvez actualiser le principal de TGS à l'aide de la commande suivante :

```
kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
```

Configuration de l'authentification inter-domaine

Il existe plusieurs manières de relier les domaines pour que les utilisateurs d'un domaine puissent être authentifiés dans un autre domaine. L'authentification inter-domaine est réalisée par la mise en place d'une clé secrète partagée par les deux domaines. La relation entre les domaines peut être hiérarchique ou directionnelle (voir "Hiérarchie des domaines" à la page 417).

▼ Procédure d'établissement de l'authentification inter-domaine hiérarchique

L'exemple de cette procédure utilise deux domaines, `ENG.EAST.EXAMPLE.COM` et `EAST.EXAMPLE.COM`. L'authentification inter-domaine est établie dans les deux directions. Cette procédure doit être effectuée sur le KDC maître dans les deux domaines.

Avant de commencer Le KDC maître de chaque domaine doit être configuré. Pour tester complètement le processus d'authentification, plusieurs clients Kerberos doivent être configurés.

1 Connectez-vous en tant que superutilisateur au premier KDC maître.

2 Créez des principaux de service de TGT pour les deux domaines.

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lorsque vous avez configuré le KDC maître.

```
# /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM:      <Type password>
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM:      <Type password>
kadmin: quit
```

Remarque – Le mot de passe que vous avez spécifié pour chaque service de principal doit être identique dans les deux KDC. Par conséquent, le mot de passe pour le service principal `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` doit être le même dans les deux domaines.

3 Ajoutez des entrées dans le fichier de configuration Kerberos (`krb5.conf`) pour définir les noms de domaine pour chaque domaine.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
 .
 .
[domain_realm]
        .eng.east.example.com = ENG.EAST.EXAMPLE.COM
        .east.example.com = EAST.EXAMPLE.COM
```

Dans cet exemple, les noms de domaine pour `ENG.EAST.EXAMPLE.COM` et `EAST.EXAMPLE.COM` sont définis. Il est important d'inclure d'abord le sous-domaine, parce que la recherche dans le fichier s'effectue du haut vers le bas.

4 Copiez le fichier de configuration Kerberos pour tous les clients dans ce domaine.

Pour que l'authentification inter-domaine fonctionne, la nouvelle version du fichier de configuration Kerberos (`/etc/krb5/krb5.conf`) doit être installée sur tous les systèmes (y compris les KDC esclaves et les autres serveurs).

5 Répétez toutes ces étapes dans le second domaine.

▼ Procédure d'établissement de l'authentification inter-domaine directe

L'exemple de cette procédure utilise deux domaines, `ENG.EAST.EXAMPLE.COM` et `SALES.WEST.EXAMPLE.COM`. L'authentification inter-domaine est établie dans les deux directions. Cette procédure doit être effectuée sur le KDC maître dans les deux domaines.

Avant de commencer Le KDC maître de chaque domaine doit être configuré. Pour tester complètement le processus d'authentification, plusieurs clients Kerberos doivent être configurés.

1 Connectez-vous en tant que superutilisateur à l'un des serveurs KDC maîtres.

2 Créez des principaux de service de TGT pour les deux domaines.

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lorsque vous avez configuré le KDC maître.

```
# /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
```

```
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
Enter password for principal
  krgtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM:       <Type the password>
kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal
  krgtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM:       <Type the password>
kadmin: quit
```

Remarque – Le mot de passe que vous avez spécifié pour chaque service de principal doit être identique dans les deux KDC. Par conséquent, le mot de passe pour le service principal `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` doit être identique dans les deux domaines.

3 Ajoutez des entrées dans le fichier de configuration Kerberos pour définir le chemin d'accès direct au domaine distant.

Cet exemple représente les clients dans le domaine `ENG.EAST.EXAMPLE.COM`. Vous pourriez avoir besoin de changer le nom de domaine pour obtenir les définitions adéquates dans le domaine `SALES.WEST.EXAMPLE.COM`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
 .
 .
[capaths]
    ENG.EAST.EXAMPLE.COM = {
        SALES.WEST.EXAMPLE.COM = .
    }

    SALES.WEST.EXAMPLE.COM = {
         ENG.EAST.EXAMPLE.COM = .
    }
```

4 Copiez le fichier de configuration Kerberos pour tous les clients dans le domaine actuel.

Pour que l'authentification inter-domaine fonctionne, la nouvelle version du fichier de configuration Kerberos (`/etc/krb5/krb5.conf`) doit être installée sur tous les systèmes (y compris les KDC esclaves et les autres serveurs).

5 Répétez toutes ces étapes pour le second domaine.

Configuration des serveurs d'application réseau Kerberos

Les serveurs d'application réseau sont des hôtes fournissant un accès à l'aide d'une ou plusieurs applications réseau parmi les suivantes : `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` et `telnet`. Seules quelques étapes sont nécessaires pour activer la version Kerberos de ces commandes sur un serveur.

▼ Procédure de configuration d'un serveur d'application réseau Kerberos

Cette procédure utilise les paramètres de configuration ci-dessous :

- Serveur d'application = `boston`
- `admin` principal = `kws/admin`
- Nom de domaine DNS = `example.com`
- Nom de domaine = `EXAMPLE.COM`

Avant de commencer Cette procédure nécessite que le KDC maître ait été configuré. Pour tester complètement le processus, plusieurs clients Kerberos doivent être configurés.

1 (Facultatif) Installez le client NTP ou un autre mécanisme de synchronisation d'horloge.

Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

2 Ajoutez des principaux pour le nouveau serveur et mettez à jour le fichier keytab du serveur.

La commande suivante indique l'existence de l'hôte principal :

```
boston # klist -k |grep host
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
```

Si la commande ne renvoie pas de principal, créez de nouveaux comptes utilisateur en suivant les étapes ci-dessous.

L'utilisation de l'outil d'administration graphique Kerberos pour ajouter un principal est expliquée à la section "Création d'un principal Kerberos" à la page 524. L'exemple dans les étapes suivantes montre comment ajouter les principaux requis à l'aide de la ligne de commande. Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

```
boston # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Créez l'`host` principal du serveur.

L'`host` principal est utilisé :

- pour authentifier le trafic lors de l'utilisation des commandes à distance, comme `rsh` et `ssh` ;
- par `pam_krb5` afin d'empêcher les attaques par mystification de KDC en utilisant l'`host` principal pour vérifier que les informations d'identification Kerberos d'un utilisateur ont été obtenues auprès d'un KDC de confiance ;

- pour autoriser l'utilisateur `root` à acquérir automatiquement des informations d'identification Kerberos en l'absence d'un principal `root`. Cela peut être utile lors d'un montage NFS manuel où le partage requiert des informations d'identification Kerberos.

Ce principal est obligatoire si le trafic qui utilise l'application distante doit être authentifié à l'aide du service Kerberos. Si le serveur a plusieurs noms d'hôte associés, créez un principal pour chaque nom d'hôte sous la forme de nom de domaine complet(FQDN) du nom d'hôte.

```
kadmin: addprinc -randkey host/boston.example.com
Principal "host/boston.example.com" created.
kadmin:
```

b. Ajoutez l'`host` principal du serveur au fichier keytab du serveur.

Si la commande `kadmin` n'est pas en cours d'exécution, redémarrez-la avec une commande similaire à la suivante : `/usr/sbin/kadmin -p` *kws*`/admin` .

Si le serveur a plusieurs noms d'hôte associés, ajoutez un principal au fichier keytab de chaque nom d'hôte.

```
kadmin: ktadd host/boston.example.com
Entry for principal host/boston.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Quittez `kadmin`.

```
kadmin: quit
```

Configuration de serveurs NFS Kerberos

Les services NFS utilisent les ID d'utilisateur (UID) UNIX pour identifier un utilisateur et ne peuvent pas utiliser directement les informations d'identification GSS. Pour traduire les données d'identification en UID, il peut être nécessaire de créer une table mappant les informations d'identification d'utilisateur et les UID UNIX. Pour plus d'informations sur le mappage par défaut des informations d'identification, reportez-vous à la section “Mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 420. Les procédures décrites dans cette section se concentrent sur les tâches nécessaires pour configurer un serveur Kerberos NFS, administrer la table d'informations d'identification Kerberos, et initier des modes de sécurité pour les systèmes de fichiers montés sur NFS. La liste ci-dessous décrit les tâches traitées dans cette section.

TABLEAU 23–2 Configuration de serveurs Kerberos NFS (liste des tâches)

Tâche	Description	Voir
Configuration d'un serveur NFS Kerberos	Permet à un serveur de partager un système de fichiers requérant l'authentification Kerberos.	"Procédure de configuration des serveurs NFS Kerberos" à la page 450
Création d'une table d'informations d'identification	Génère une table d'informations d'identification pouvant être utilisée pour assurer le mappage des informations d'identification GSS aux UID UNIX, si le mappage par défaut n'est pas suffisant.	"Création d'une table d'informations d'identification" à la page 452
Modification de la table d'informations d'identification qui mappe les informations d'identification et les UID UNIX	Met à jour les informations de la table d'informations d'identification.	"Ajout d'une entrée unique à la table d'informations d'identification" à la page 452
Mappage des informations d'identification entre deux domaines similaires	Fournit des instructions sur la méthode de mappage des UID d'un domaine à un autre si les domaines partagent un fichier de mots de passe.	"Procédure de mappage d'informations d'identification entre domaines" à la page 453
Partage d'un système de fichiers à l'aide de l'authentification Kerberos	Partage un système de fichiers avec des modes de sécurité de sorte que l'authentification Kerberos est requise.	"Configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos" à la page 454

▼ Procédure de configuration des serveurs NFS Kerberos

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- Serveur NFS = `denver.example.com`
- `admin` principal = `kws/admin`

1 Remplissez les conditions préalables à la configuration d'un serveur Kerberos NFS.

Le KDC maître doit être configuré. Pour tester complètement le processus, vous avez besoin de plusieurs clients.

2 (Facultatif) Installez le client NTP ou un autre mécanisme de synchronisation d'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être synchronisée avec l'heure sur le serveur KDC dans une différence maximum définie par la relation `clockskew` dans le fichier `krb5.conf` pour que l'opération d'authentification réussisse. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

3. **Configurez le serveur NFS en tant que client Kerberos.**

   Suivez les instructions de la section "Configuration des clients Kerberos" à la page 456.

4. **Démarrez `kadmin`.**

   Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section "Création d'un principal Kerberos" à la page 524. Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

   ```
   denver # /usr/sbin/kadmin -p kws/admin
   Enter password:      <Type kws/admin password>
   kadmin:
   ```

   a. **Créez le principal de service NFS du serveur.**

      Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

      Répétez cette étape pour chaque interface unique sur le système susceptible d'être utilisée pour accéder aux données NFS. Si un hôte possède plusieurs interfaces avec des noms uniques, chaque nom unique doit avoir son propre principal de service NFS.

      ```
      kadmin: addprinc -randkey nfs/denver.example.com
      Principal "nfs/denver.example.com" created.
      kadmin:
      ```

   b. **Ajoutez le principal de service du serveur NFS au fichier keytab du serveur.**

      Répétez cette étape pour chaque principal de service dans l'Étape a.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

   c. **Quittez `kadmin`.**

      ```
      kadmin: quit
      ```

5. **(Facultatif) Créez les mappages d'informations d'identification GSS spéciaux, si nécessaire.**

   Normalement, le service Kerberos génère des mappages appropriés entre les informations d'identification GSS et les UID UNIX. Le mappage par défaut est décrit dans la section "Mappage d'informations d'identification GSS sur des informations d'identification UNIX"

à la page 420. Si le mappage par défaut n'est pas suffisant, reportez-vous à la section "Création d'une table d'informations d'identification" à la page 452 pour plus d'informations.

6 **Partagez le système de fichiers NFS avec les modes de sécurité Kerberos.**

Pour plus d'informations, reportez-vous à la section "Configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos" à la page 454.

▼ Création d'une table d'informations d'identification

La table d'informations d'identification `gsscred` est utilisée par un serveur NFS pour mapper les informations d'identification Kerberos à un UID. Par défaut, la première partie du nom du principal est mappée avec un nom de connexion UNIX. Pour que les clients NFS puissent monter des systèmes de fichiers à partir d'un serveur NFS à l'aide de l'authentification Kerberos, ce tableau doit être créé si le mappage par défaut n'est pas suffisant.

1 **Modifiez le fichier `/etc/gss/gsscred.conf` et changez le mécanisme de sécurité.**

Modifiez le mécanisme en `files`.

2 **Créez la table d'informations d'identification à l'aide de la commande `gsscred`.**

```
# gsscred -m kerberos_v5 -a
```

La commande `gsscred` rassemble les informations provenant de l'ensemble des sources répertoriées avec l'entrée `passwd` dans le fichier `/etc/nsswitch.conf`. Vous pouvez être amené à supprimer temporairement l'entrée `files` , si vous ne souhaitez pas que les entrées de mot de passe local soient incluses dans la table d'informations d'identification. Pour plus d'informations, reportez-vous à la page de manuel `gsscred(1M)`.

▼ Ajout d'une entrée unique à la table d'informations d'identification

Avant de commencer Cette procédure nécessite que la table `gsscred` ait déjà été créée sur le serveur NFS. Pour obtenir des instructions, reportez-vous à la section "Création d'une table d'informations d'identification" à la page 452.

1 **Connectez-vous en tant que superutilisateur au serveur NFS.**

2 **Ajoutez une entrée à la table d'informations d'identification à l'aide de la commande `gsscred`.**

```
# gsscred -m mech [ -n name [ -u uid ]] -a
```

mech Définit le mécanisme de sécurité à utiliser.

name Définit le nom de principal de l'utilisateur, tel que défini dans le KDC.

uid Définit l'UID de l'utilisateur, tel que défini dans la base de données de mots de passe.

`-a` Ajoute l'UID au mappage du nom de principal.

Exemple 23–2 Ajout d'un principal à composants multiples à la table d'informations d'identification

Dans l'exemple suivant, l'entrée est ajoutée à un principal appelé `sandy/admin` associé à l'UID `3736` .

```
# gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

Exemple 23–3 Ajout d'un principal à un domaine différent de la table d'informations d'identification

Dans l'exemple suivant, l'entrée est ajoutée à un principal appelé `sandy/admin@EXAMPLE.COM` associé à l'UID 3736.

```
# gsscred -m kerberos_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a
```

▼ Procédure de mappage d'informations d'identification entre domaines

Cette procédure assure le mappages d'informations d'identification approprié entre des domaines utilisant le même fichier de mots de passe. Dans cet exemple, les domaines `CORP.EXAMPLE.COM` et `SALES.EXAMPLE.COM` utilisent le même fichier de mots de passe. Les informations d'identification pour `bob@CORP.EXAMPLE.COM` et `bob@SALES.EXAMPLE.COM` sont mappées avec le même UID.

1. **Connectez-vous en tant que superutilisateur.**

2. **Sur le système client, ajoutez des entrées au fichier `krb5.conf`.**

```
# cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = CORP.EXAMPLE.COM
 .
[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

Exemple 23–4 Mappage des informations d'identification entre domaines utilisant le même fichier de mot de passe

Cet exemple illustre le mappage d'informations d'identification approprié entre des domaines qui utilisent le même fichier de mots de passe. Dans cet exemple, les domaines `CORP.EXAMPLE.COM` et `SALES.EXAMPLE.COM` utilisent le même fichier de mots de passe. Les informations d'identification pour `bob@CORP.EXAMPLE.COM` et `bob@SALES.EXAMPLE.COM` sont mappées avec le même UID. Sur le système client, ajoutez des entrées au fichier `krb5.conf`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = CORP.EXAMPLE.COM
 .
[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

Erreurs fréquentes Pour plus d'information sur le processus de dépannage des problèmes de mappage d'informations d'identification, reportez-vous à la section "Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX" à la page 512.

▼ Configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos

Cette procédure permet à un serveur NFS de fournir un accès NFS sécurisé à l'aide de différents modes ou variantes de sécurité. Lorsqu'un client négocie une variante de sécurité avec le serveur NFS, la première variante proposée par le serveur auquel le client a accès est utilisée. Cette variante est utilisée pour toutes les demandes de client suivantes du système de fichiers partagé par le serveur NFS.

1 Connectez-vous en tant que superutilisateur au serveur NFS.

2 Vérifiez que le fichier keytab comporte un principal de service NFS.

La commande `klist` signale s'il existe un fichier keytab et affiche les principaux. Si les résultats indiquent qu'aucun fichier keytab ou principal de service NFS n'existe, vous devez vérifier que toutes les étapes décrites à la section "Procédure de configuration des serveurs NFS Kerberos" à la page 450 ont bien été effectuées dans leur totalité.

```
# klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
---- --------------------------------------------------------
   3 nfs/denver.example.com@EXAMPLE.COM
```

```
   3 nfs/denver.example.com@EXAMPLE.COM
   3 nfs/denver.example.com@EXAMPLE.COM
   3 nfs/denver.example.com@EXAMPLE.COM
```

3 Activez les modes de sécurité Kerberos dans le fichier `/etc/nfssec.conf`.

Modifiez le fichier `/etc/nfssec.conf` et supprimez le "#" placé devant les modes de sécurité Kerberos.

```
# cat /etc/nfssec.conf
 .
 .
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5            390003  kerberos_v5     default -               # RPCSEC_GSS
krb5i           390004  kerberos_v5     default integrity       # RPCSEC_GSS
krb5p           390005  kerberos_v5     default privacy         # RPCSEC_GSS
```

4 Modifiez le fichier `/etc/dfs/dfstab` et ajoutez l'option `sec=` avec les modes de sécurité requis aux entrées correspondantes.

`share -F nfs -o sec=`*mode file-system*

mode Spécifie les modes de sécurité à utiliser lors du partage du système de fichiers. Lorsque plusieurs modes de sécurité sont utilisés, le premier mode figurant dans la liste est utilisé comme valeur par défaut.

file-system Définit le chemin d'accès au système de fichiers à partager.

Tous les clients tentant d'accéder à des fichiers dans le système de fichiers nommé requièrent l'authentification Kerberos. Pour accéder aux fichiers, le principal d'utilisateur sur le client NFS doit être authentifié.

5 Assurez-vous que le service NFS est en cours d'exécution sur le serveur.

Si cette commande est la première commande `share` ou le premier jeu de commandes `share` que vous avez lancé, les démons NFS ne sont probablement pas en cours d'exécution. La commande suivante redémarre les démons :

```
# svcadm restart network/nfs/server
```

6 (Facultatif) Si l'agent de montage automatique est en cours d'utilisation, modifiez la base de données `auto_master` pour sélectionner un mode de sécurité autre que celui par défaut.

Vous n'avez pas besoin de suivre cette procédure si vous n'utilisez pas l'agent de montage automatique pour accéder au système de fichiers ou si la sélection par défaut du mode de sécurité est acceptable.

file-system `auto_home -nosuid,sec=`*mode*

7 **(Facultatif) Émettez manuellement la commande `mount` pour accéder au système de fichiers à l'aide d'un autre mode que celui par défaut.**

Vous pouvez aussi utiliser la commande `mount` pour spécifier le mode de sécurité, mais cette alternative ne tire pas parti de l'agent de montage automatique.

```
# mount -F nfs -o sec=mode file-system
```

Exemple 23–5 Partage d'un système de fichiers avec un mode de sécurité Kerberos

Dans cet exemple, la ligne du fichier `dfstab` signifie que l'authentification Kerberos doit aboutir avant que les fichiers puissent être accessibles via le service NFS.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5 /export/home
```

Exemple 23–6 Partage d'un système de fichiers avec plusieurs modes de sécurité Kerberos

Dans cet exemple, les trois modes de sécurité Kerberos ont été sélectionnés. Le mode utilisé est négocié entre le client et le serveur NFS. Si le premier mode dans la commande échoue, le mode suivant est essayé. Pour plus d'informations, reportez-vous à la page de manuel `nfssec(5)`.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

Configuration des clients Kerberos

Les clients Kerberos incluent tout hôte qui n'est pas un serveur KDC sur le réseau et qui doit utiliser les services Kerberos. Cette section décrit les procédures d'installation d'un client Kerberos, ainsi que des informations spécifiques sur l'utilisation de l'authentification `root` pour monter des systèmes de fichiers NFS.

Configuration des clients Kerberos (liste des tâches)

La liste des tâches ci-dessous comprend toutes les procédures associées à la configuration des clients Kerberos. Chaque ligne comprend un identificateur de tâche, une description de la raison pour laquelle cette tâche doit être effectuée, suivie d'un lien vers la tâche.

Tâche	Description	Voir
Établissement d'un profil d'installation client Kerberos	Génère un profil d'installation client pouvant être utilisé pour installer automatiquement un client Kerberos.	"Procédure de création d'un profil d'installation de client Kerberos" à la page 457

Tâche	Description	Voir
Configuration d'un client Kerberos	Installe manuellement un client Kerberos. Utilisez cette procédure si chaque installation de client requiert des paramètres d'installation uniques.	"Configuration manuelle d'un client Kerberos" à la page 460
	Installe automatiquement un client Kerberos. Utilisez cette procédure si les paramètres d'installation sont identiques pour tous les clients.	"Configuration automatique d'un client Kerberos" à la page 458
	Installe interactivement un client Kerberos. Utilisez cette procédure si seuls quelques-uns des paramètres d'installation doivent être modifiés.	"Configuration interactive d'un client Kerberos" à la page 459
Autorisation donnée à un client d'accéder à un système de fichiers NFS en tant qu'utilisateur `root`.	Crée un principal `root` sur le client, de manière à ce que le client puisse monter un système de fichiers NFS partagé avec accès `root`. Permet également au client de définir un accès `root` non interactif au système de fichiers NFS, de manière à ce que les tâches cron puissent s'exécuter.	"Accès à un système de fichiers NFS protégé par Kerberos en tant qu'utilisateur `root`" à la page 466
Désactivation de la vérification du KDC qui a émis un TGT (Ticket Granting Ticket) client	Permet aux clients ne disposant pas d'un principal d'hôte stocké dans le fichier keytab local d'ignorer le contrôle de sécurité qui vérifie que le KDC ayant émis le TGT est le même serveur que celui ayant émis le principal d'hôte.	"Désactivation de la vérification du TGT" à la page 466

▼ Procédure de création d'un profil d'installation de client Kerberos

Cette procédure permet de créer un profil kclient à utiliser lorsque vous installez un client Kerberos. L'utilisation du profil kclient permet de réduire les risques de faute de frappe. En outre, le profil permet de réduire l'intervention de l'utilisateur par rapport au processus interactif.

1 Connectez-vous en tant que superutilisateur.

2 Créez un profil d'installation kclient.

Un exemple de profil kclient pourrait ressembler à l'exemple suivant :

```
client# cat /net/denver.example.com/export/install/profile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

▼ Configuration automatique d'un client Kerberos

Avant de commencer Cette procédure utilise un profil d'installation. Reportez-vous à la section "Procédure de création d'un profil d'installation de client Kerberos" à la page 457.

1 Connectez-vous en tant que superutilisateur.

2 Exécutez le script d'installation `kclient`.

Vous devez fournir le mot de passe pour le principal `clntconfig` afin de terminer le processus.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile

Starting client setup
--------------------------------------------------

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

--------------------------------------------------
Setup COMPLETE.

client#
```

Exemple 23–7 Configuration automatique d'un client Kerberos avec des remplacements de ligne de commande

L'exemple suivant remplace les paramètres `DNSARG` et `KDC` définis dans le profil d'installation.

```
# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile\
-d dns_fallback -k kdc2.example.com

Starting client setup
--------------------------------------------------

kdc1.example.com

Setting up /etc/krb5/krb5.conf.
```

```
Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

-------------------------------------------------
Setup COMPLETE.

client#
```

▼ Configuration interactive d'un client Kerberos

Cette procédure utilise l'utilitaire d'installation `kclient` sans profil d'installation.

1 Connectez-vous en tant que superutilisateur.

2 Exécutez le script d'installation `kclient`.

Vous devez fournir les informations suivantes :

- Nom de domaine Kerberos
- Nom d'hôte KDC maître
- Nom de principal administratif
- Mot de passe du principal administratif

Exemple 23–8 Exécution de l'utilitaire d'installation `kclient`

La sortie suivante indique les résultats de l'exécution de la commande `kclient`.

```
client# /usr/sbin/kclient

Starting client setup
-------------------------------------------------

Do you want to use DNS for kerberos lookups ? [y/n]: n
        No action performed.
Enter the Kerberos realm: EXAMPLE.COM
Specify the KDC hostname for the above realm: kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Enter the krb5 administrative principal to be used: clntconfig/admin
Obtaining TGT for clntconfig/admin ...
```

```
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>
Do you plan on doing Kerberized nfs ? [y/n]: n

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Do you want to copy over the master krb5.conf file ? [y/n]: y
Enter the pathname of the file to be copied: \
/net/denver.example.com/export/install/krb5.conf

Copied /net/denver.example.com/export/install/krb5.conf.

-------------------------------------------------
Setup COMPLETE !
#
```

▼ Configuration manuelle d'un client Kerberos

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com`
- Serveur NFS = `denver.example.com`
- Client = `client.example.com`
- `admin` principal = `kws/admin`
- Utilisateur principal = `mre`
- URL de l'aide en ligne = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Remarque – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section “URL d'aide en ligne dans l'outil d'administration graphique de Kerberos ” à la page 424.

---

1 Connectez-vous en tant que superutilisateur.

2 Éditez le fichier de configuration Kerberos (`krb5.conf`).

Pour modifier le fichier de version Kerberos par défaut, vous devez modifier les noms de domaine et les noms de serveur. Vous devez également identifier le chemin d'accès aux fichiers d'aide pour `gkadmin`.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
        }

[domain_realm]
        .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
        default = FILE:/var/krb5/kdc.log
        kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
```

Remarque – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_enctypes` ou `default_tgs_enctypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section "Utilisation des types de chiffrement Kerberos" à la page 584.

---

3 (Facultatif) Modifiez le processus utilisé pour localiser les KDC.

À partir de la version Solaris 10 5/08, par défaut, le domaine Kerberos pour le mappage KDC est effectué dans l'ordre suivant :

- Définition de la section `realms` dans `krb5.conf` ;
- Recherche des enregistrements SRV dans le DNS.

Vous pouvez modifier ce comportement en ajoutant `dns_lookup_kdc` ou `dns_fallback` à la section `libdefaults` du fichier `krb5.conf`. Pour plus d'informations, reportez-vous à la page de manuel `krb5.conf(4)`. Notez que les références sont toujours tentées en premier.

4 (Facultatif) Modifiez le processus utilisé pour déterminer le domaine d'un hôte.

À partir de la version Solaris 10 5/08, par défaut, le mappage l'hôte au domaine est déterminé dans l'ordre suivant :

- Si le KDC prend en charge les références, le KDC peut indiquer au client le domaine auquel appartient l'hôte.
- Par la définition du fichier `domain_realm` du fichier `krb5.conf`.
- Le nom de domaine DNS de l'hôte.
- Le domaine par défaut.

Vous pouvez modifier ce comportement en ajoutant `dns_lookup_kdc` ou `dns_fallback` à la section `libdefaults` du fichier `krb5.conf`. Pour plus d'informations, reportez-vous à la page de manuel `krb5.conf(4)`. Notez que les références sont toujours tentées en premier.

5 (Facultatif) Synchronisez l'horloge du client avec l'horloge du KDC maître à l'aide de NTP ou d'un autre mécanisme de synchronisation d'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être synchronisée avec l'heure sur le serveur KDC dans une différence maximum définie par la relation `clockskew` dans le fichier `krb5.conf` pour que l'opération d'authentification réussisse. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

6 Démarrez `kadmin`.

Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section "Création d'un principal Kerberos" à la page 524. Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. (Facultatif) Créez un principal d'utilisateur s'il n'en existe pas déjà.

Vous devez créer un principal d'utilisateur uniquement si aucun principal n'est affecté à l'utilisateur associé à cet hôte.

```
kadmin: addprinc mre
Enter password for principal mre@EXAMPLE.COM:      <Type the password>
Re-enter password for principal mre@EXAMPLE.COM:      <Type it again>
kadmin:
```

b. (Facultatif) Créez un principal `root` et ajoutez le principal au fichier keytab du serveur.

Cette étape est nécessaire pour que le client dispose d'un accès `root` aux systèmes de fichiers montés à l'aide du service NFS. Cette étape est également requise si l'accès `root` non interactif est nécessaire, par exemple pour l'exécution des tâches cron en tant que `root`.

Vous pouvez ignorer cette étape si le client ne nécessite pas l'accès `root` à un système de fichiers distant monté à l'aide du service NFS. Le principal de `root` doit être un principal à deux composants, avec pour second composant le nom d'hôte du système du client Kerberos, pour éviter la création d'un principal `root` à l'échelle du domaine. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Créez un principal `host` et ajoutez le principal au fichier keytab du serveur.

Le principal `host` est utilisé par les services d'accès à distance pour fournir l'authentification. L'identité permet à `root` d'acquérir des informations d'identification, s'il n'en existe pas déjà dans le fichier keytab.

```
kadmin: addprinc -randkey host/denver.example.com
Principal "host/denver.example.com@EXAMPLE.COM" created.
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

d. (Facultatif) Ajoutez le principal de service du serveur NFS au fichier keytab du serveur.

Cette étape n'est requise que si le client a besoin d'accéder aux systèmes de fichiers NFS à l'aide de l'authentification Kerberos.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type ArcFour
```

```
        with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
        with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

e. Quittez `kadmin`.

```
kadmin: quit
```

7 (Facultatif) Activez Kerberos avec NFS.

a. Activez les modes de sécurité Kerberos dans le fichier `/etc/nfssec.conf`.

Modifiez le fichier `/etc/nfssec.conf` et supprimez le "#" placé devant les modes de sécurité Kerberos.

```
# cat /etc/nfssec.conf
 .
 .
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5            390003  kerberos_v5     default -               # RPCSEC_GSS
krb5i           390004  kerberos_v5     default integrity       # RPCSEC_GSS
krb5p           390005  kerberos_v5     default privacy         # RPCSEC_GSS
```

b. Activez DNS.

Si le fichier `/etc/resolv.conf` n'a pas déjà été créé, créez ce fichier en tant que principal de service, car la normalisation du principal de service dépend du DNS. Pour plus d'informations, reportez-vous à la page de manuel `resolv.conf(4)`.

c. Redémarrez le service `gssd`.

Une fois le fichier `/etc/resolv.conf` créé ou modifié, vous devez redémarrer le démon `gssd` pour relire les modifications.

```
# svcadm restart network/rpc/gss
```

8 Si vous souhaitez que le client renouvelle automatiquement le TGT ou qu'il avertisse les utilisateurs de l'expiration du ticket Kerberos, créez une entrée dans le fichier `/etc/krb5/warn.conf` .

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

Exemple 23–9 Configuration d'un client Kerberos à l'aide d'un KDC non-Solaris

Un client Kerberos peut être configuré pour fonctionner avec un KDC non Solaris. Dans ce cas, une ligne doit être incluse dans le fichier `/etc/krb5/krb5.conf` à la section `realms`. Cette ligne change le protocole utilisé lorsque le client est en cours de communication avec le serveur de changement de mot de passe Kerberos. Le format de cette ligne est le suivant.

```
[realms]
                EXAMPLE.COM = {
```

```
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                admin_server = kdc1.example.com
                kpasswd_protocol = SET_CHANGE
        }
```

Exemple 23–10 Enregistrements DNS TXT pour le mappage de l'hôte et du nom de domaine au domaine Kerberos

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
                                1989020501   ;serial
                                10800        ;refresh
                                3600         ;retry
                                3600000      ;expire
                                86400 )      ;minimum

                        IN      NS      kdc1.example.com.
kdc1                    IN      A       192.146.86.20
kdc2                    IN      A       192.146.86.21

_kerberos.example.com.              IN      TXT     "EXAMPLE.COM"
_kerberos.kdc1.example.com.         IN      TXT     "EXAMPLE.COM"
_kerberos.kdc2.example.com.         IN      TXT     "EXAMPLE.COM"
```

Exemple 23–11 Enregistrements DNS SRV pour les emplacements de serveur Kerberos

Cet exemple définit les enregistrements pour l'emplacement des KDC, du serveur `admin` et du serveur `kpasswd`, respectivement.

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
                                1989020501   ;serial
                                10800        ;refresh
                                3600         ;retry
                                3600000      ;expire
                                86400 )      ;minimum

                                   IN      NS      kdc1.example.com.
kdc1                               IN      A       192.146.86.20
kdc2                               IN      A       192.146.86.21

_kerberos._udp.EXAMPLE.COM         IN      SRV 0 0 88  kdc2.example.com
_kerberos._tcp.EXAMPLE.COM         IN      SRV 0 0 88  kdc2.example.com
_kerberos._udp.EXAMPLE.COM         IN      SRV 1 0 88  kdc1.example.com
_kerberos._tcp.EXAMPLE.COM         IN      SRV 1 0 88  kdc1.example.com
_kerberos-adm._tcp.EXAMPLE.COM     IN      SRV 0 0 749 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM          IN      SRV 0 0 749 kdc1.example.com
```

▼ Désactivation de la vérification du TGT

Cette procédure permet de désactiver le contrôle de sécurité qui vérifie que le KDC de l'hôte principal stocké dans le fichier `/etc/krb5/krb5.keytab` local est le même KDC qui a émis le TGT. Cette vérification permet d'empêcher les attaques par usurpation de DNS. Cependant, pour certaines configurations client, l'hôte principal peut ne pas être disponible, et cette vérification doit alors être désactivée pour que le client puisse fonctionner. Voici les configurations requérant que cette vérification soit désactivée :

- L'adresse IP du client est affectée de manière dynamique. Par exemple, un client DHCP.
- Le client n'est pas configuré pour héberger les services, de sorte qu'aucun hôte principal n'a été créé.
- La clé d'hôte n'est pas stockée sur le client.

1 Connectez-vous en tant que superutilisateur.

2 Modifiez le fichier `krb5.conf`.

Si l'option `verify_ap_req_nofail` est définie sur `false`, le processus de vérification du TGT n'est pas activé. Pour plus d'informations sur cette option, reportez-vous à la page de manuel `krb5.conf(4)`.

```
client # cat /etc/krb5/krb5.conf
[libdefaults]
        default_realm = EXAMPLE.COM
        verify_ap_req_nofail = false
  ...
```

Remarque – L'option `verify_ap_req_nofail` peut être saisie dans la section `[libdefaults]` ou `[realms]` du fichier `krb5.conf`. Si la valeur de l'option est dans la section `[libdefaults]`, le paramètre est utilisé pour tous les domaines. Si la valeur de l'option est dans la section `[realms]` , le paramètre s'applique uniquement au domaine défini.

▼ Accès à un système de fichiers NFS protégé par Kerberos en tant qu'utilisateur `root`

Cette procédure permet à un client d'accéder à un système de fichiers NFS requérant l'authentification Kerberos avec le privilège d'ID `root`, en particulier lorsque le système de fichiers NFS est partagé avec des options comme `-o sec=krb5,root=client1.sun.com`.

1 Connectez-vous en tant que superutilisateur.

2 Démarrez `kadmin`.

Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section "Création d'un principal Kerberos" à la page 524. Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Créez un principal `root` pour le client NFS.

Ce principal permet de fournir un accès équivalent à root aux systèmes de fichiers montés NFS requérant l'authentification Kerberos. Le principal `root` doit être un principal à deux composants, avec pour second composant le nom d'hôte du système du client Kerberos, pour éviter la création d'un principal root à l'échelle du domaine. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin:
```

b. Ajoutez le principal `root` au fichier keytab du serveur.

Cette étape est nécessaire si vous avez ajouté un principal `root` afin que le client puisse avoir l'accès `root` aux systèmes de fichiers montés à l'aide du service NFS. Cette étape est également requise si l'accès `root` non interactif est nécessaire, par exemple pour l'exécution des tâches cron en tant que `root`.

```
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

c. Quittez `kadmin`.

```
kadmin: quit
```

▼ Configuration de la migration automatique des utilisateurs dans un domaine Kerberos

Les utilisateurs ne disposant pas d'un principal Kerberos peuvent être automatiquement migrés vers un domaine Kerberos existant. La migration s'effectue à l'aide de la structure PAM pour le service en cours d'utilisation par l'empilage du module `pam_krb5_migrate` dans la pile d'authentification du service dans `/etc/pam.conf`.

Dans cet exemple, les noms de services PAM `dtlogin` et `other` sont configurés pour utiliser la migration automatique. Les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- KDC maître = `kdc1.example.com`
- Machine hébergeant le service de migration = `server1.example.com`
- Principal du service de migration = `host/server1.example.com`

Avant de commencer Configurez `server1` en tant que client Kerberos du domaine `EXAMPLE.COM`. Pour plus d'informations, reportez-vous à la section "Configuration des clients Kerberos" à la page 456.

1 Vérifiez si un hôte principal de service existe pour `server1` .

L'hôte principal de service dans le fichier `keytab` de `server1` est utilisé pour authentifier le serveur auprès du KDC maître.

```
server1 # klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
    KVNO Principal
    ---- -------------------------------------------------
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
       3 host/server1.example.com@EXAMPLE.COM
```

2 Apportez des modifications au fichier de configuration PAM.

a. Ajoutez des entrées pour le service `dtlogin`.

```
# cat /etc/pam.conf
 .
 .
#
# dtlogin service (explicit because of pam_krb5_migrate)
#
dtlogin       auth requisite          pam_authtok_get.so.1
dtlogin       auth required           pam_dhkeys.so.1
dtlogin       auth required           pam_unix_cred.so.1
dtlogin       auth sufficient         pam_krb5.so.1
dtlogin       auth requisite          pam_unix_auth.so.1
dtlogin       auth optional           pam_krb5_migrate.so.1
```

b. (Facultatif) Forcez une modification immédiate du mot de passe, si nécessaire.

Il est possible de définir le délai d'expiration du mot de passe des nouveaux comptes Kerberos sur l'heure actuelle (maintenant), afin de forcer la modification immédiate du mot de passe Kerberos. Pour définir l'heure d'expiration sur l'heure actuelle, ajoutez l'option `expire_pw` aux lignes utilisant le module `pam_krb5_migrate`. Pour plus d'informations, reportez-vous à la page de manuel `pam_krb5_migrate(5)`.

```
# cat /etc/pam.conf
 .
 .
dtlogin  auth optional           pam_krb5_migrate.so.1 expire_pw
```

c. Ajoutez le module `pam_krb5` à la pile de compte.

Cet ajout prévoit l'expiration du mot de passe de Kerberos afin de bloquer l'accès.

```
# cat /etc/pam.conf
 .
 .
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite       pam_roles.so.1
other   account required        pam_krb5.so.1
other   account required        pam_unix_account.so.1
```

d. Ajoutez le module `pam_krb5` à la pile de mot de passe.

Cet ajout permet la mise à jour des mots de passe lorsque ceux-ci expirent.

```
# cat /etc/pam.conf
 .
 .
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password management
#
other   password required       pam_dhkeys.so.1
other   password requisite      pam_authtok_get.so.1
other   password requisite      pam_authtok_check.so.1
other   password sufficient     pam_krb5.so.1
other   password required       pam_authtok_store.so.1
```

3 Sur le KDC maître, mettez à jour le fichier de contrôle d'accès.

Les entrées suivantes accordent des privilèges de migration et de consultation au principal de service `host/server1.example.com` pour tous les utilisateurs, excepté l'utilisateur `root`. Il est important que les utilisateurs qui ne doivent pas être migrés soient répertoriés dans le fichier `kadm5.acl` à l'aide du privilège `U`. Ces entrées doivent figurer avant l'entrée "permit all" ou `ui`. Pour plus d'informations, reportez-vous à la page de manuel `kadm5.acl(4)`.

```
kdc1 # cat /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

4 **Sur le KDC maître, redémarrez le démon d'administration Kerberos.**

Cette étape permet au démon `kadmind` d'utiliser les nouvelles entrées `kadm5.acl`.

```
kdc1 # svcadm restart network/security/kadmin
```

5 **Sur le KDC maître, ajoutez les entrées au fichier `pam.conf`.**

Les entrées suivantes permettent au démon `kadmind` d'utiliser le service PAM `k5migrate` pour valider le mot de passe utilisateur UNIX pour les comptes qui nécessitent une migration.

```
# grep k5migrate /etc/pam.conf
k5migrate       auth    required        pam_unix_auth.so.1
k5migrate       account required        pam_unix_account.so.1
```

Synchronisation des horloges entre les KDC et les clients Kerberos

Tous les hôtes participant au système d'authentification Kerberos doivent avoir leurs horloges internes synchronisées dans une quantité maximale de temps spécifiée (appelée *écart d'horloge*). Cette exigence constitue un autre contrôle de sécurité Kerberos. Si l'écart d'horloge est dépassé entre des hôtes participants, les demandes du client sont rejetées.

L'écart d'horloge détermine également la durée pendant laquelle les serveurs d'application doivent assurer le suivi de tous les messages du protocole Kerberos, afin de reconnaître et de rejeter les demandes rediffusées. Ainsi, plus l'écart d'horloge est élevé, plus les serveurs d'application doivent collecter d'informations.

La valeur par défaut pour l'écart d'horloge maximal est de 300 secondes (5 minutes). Vous pouvez modifier cette valeur par défaut dans la section `libdefaults` du fichier `krb5.conf`.

Remarque – Pour des raisons de sécurité, l'écart d'horloge ne doit pas dépasser 300 secondes.

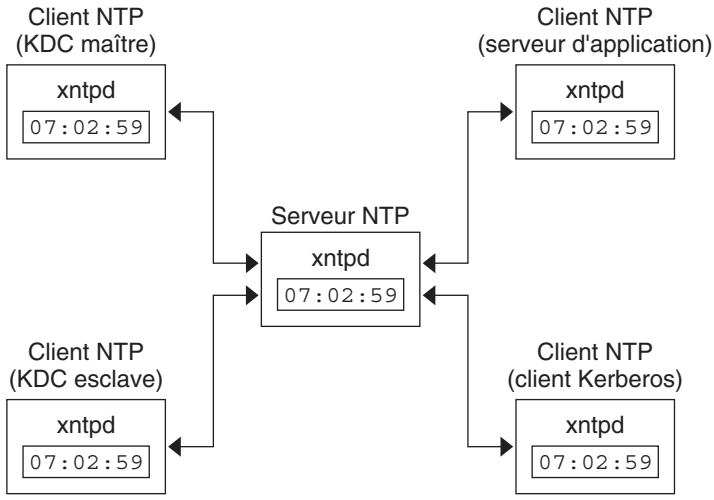
Dans la mesure où il est important de conserver la synchronisation des horloges entre le KDC et les clients Kerberos, vous devez utiliser le logiciel NTP (Network Time Protocol) pour les synchroniser. Le logiciel NTP du domaine public de l'Université du Delaware est inclus dans le logiciel Oracle Solaris.

Remarque – Un autre moyen de synchroniser les horloges consiste à utiliser la commande `rdate` et les tâches `cron` ; ce processus peut être moins complexe que l'utilisation du protocole NTP. Toutefois, cette section se concentre sur l'utilisation du protocole NTP. En outre, si vous utilisez le réseau pour synchroniser les horloges, le protocole de synchronisation de l'horloge doit lui-même être sécurisé.

NTP vous permet de gérer avec précision la synchronisation de l'heure ou de l'horloge du réseau, ou les deux, dans un environnement réseau. NTP est fondamentalement une implémentation serveur-client. Sélectionnez le système qui sera l'horloge principale (serveur NTP). Ensuite, définissez tous les autres systèmes (clients NTP) de sorte qu'ils synchronisent leurs horloges avec l'horloge principale.

Pour synchroniser les horloges, NTP utilise le démon `xntpd` qui définit et actualise l'heure du jour d'un système UNIX en accord avec les serveurs de temps standard Internet. L'exemple suivant montre un exemple de cette implémentation serveur-client NTP.

FIGURE 23–1 Synchronisation des horloges à l'aide de NTP



S'assurer que les KDC et les clients Kerberos maintiennent leurs horloges synchronisées implique la mise en œuvre des étapes suivantes :

1. Configuration d'un serveur NTP sur votre réseau. Ce serveur peut être n'importe quel système, à l'exception du KDC maître. Reportez-vous à la section "Gestion du protocole NTP (tâches)" du *Guide d'administration système : Services réseau* pour connaître les tâches de serveur NTP.
2. Lorsque vous configurez les clients KDC et Kerberos sur le réseau, définissez-les de sorte qu'ils soient des clients NTP sur le serveur NTP. Reportez-vous à la section "Gestion du protocole NTP (tâches)" du *Guide d'administration système : Services réseau* pour connaître les tâches de client NTP.

Échange d'un KDC maître et d'un KDC esclave

Vous devez utiliser les procédures décrites dans cette section pour faciliter l'échange d'un KDC maître et d'un KDC esclave. Vous devez remplacer le KDC maître par un KDC esclave uniquement si le serveur du KDC maître est en panne pour une raison quelconque, ou si le KDC maître doit être réinstallé (par exemple, en cas d'installation de nouveau matériel).

▼ Configuration d'un KDC échangeable

Effectuez cette procédure sur le serveur KDC esclave que vous souhaitez libérez pour devenir le KDC maître. Cette procédure suppose que vous utilisez la propagation incrémentielle.

1 **Utilisez les noms d'alias pour le KDC maître et le KDC esclave échangeable pendant l'installation du KDC.**

Lorsque vous définissez les noms d'hôte des KDC, assurez-vous que chaque système possède un alias inclus dans le DNS. Vous pouvez également utiliser les noms d'alias lorsque vous définissez les hôtes dans le fichier `/etc/krb5/krb5.conf`.

2 **Effectuez les étapes suivantes pour installer un KDC esclave.**

Avant tout échange, ce serveur doit fonctionner comme n'importe quel autre KDC esclave dans le domaine. Reportez-vous à la section "Procédure de configuration manuelle d'un KDC esclave" à la page 440 pour obtenir des instructions.

3 **Déplacez les commandes de KDC maître.**

Pour empêcher les commandes du KDC maître d'être exécutées à partir de ce KDC esclave, déplacez les commandes `kprop`, `kadmind` et `kadmin.local` à un endroit réservé.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc4 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
```

▼ Procédure d'échange d'un KDC maître et d'un KDC esclave

Dans cette procédure, le serveur de KDC maître échangé est appelé `kdc1`. Le KDC esclave qui devient le nouveau KDC maître est appelé `kdc4`. Cette procédure suppose que vous utilisez la propagation incrémentielle.

Avant de commencer Cette procédure nécessite que le serveur de KDC esclave ait été défini en tant qu'esclave échangeable. Pour plus d'informations, reportez-vous à la section "Configuration d'un KDC échangeable" à la page 472.

1 Sur le nouveau KDC maître, démarrez `kadmin`.

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Créez de nouveaux principaux pour le service `kadmind`.

L'exemple suivant montre la première commande `addprinc` sur deux lignes, mais elle doit être saisie sur une seule ligne.

```
kadmin: addprinc -randkey -allow_tgs_req +password_changing_service -clearpolicy \
       changepw/kdc4.example.com
Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

b. Créez un fichier keytab.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc4.example.com
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc4.example.com
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin:
```

c. Quittez `kadmin`.

```
kadmin: quit
```

2 Sur le nouveau KDC maître, forcez la synchronisation.

Les étapes suivantes forcent une mise à jour complète de KDC sur le serveur esclave.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

3 Sur le nouveau KDC maître, vérifiez que la mise à jour est terminée.

```
kdc4 # /usr/sbin/kproplog -h
```

4 Sur le nouveau KDC maître, redémarrez le service KDC.

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

5 Sur le nouveau KDC maître, effacez le journal de mise à jour.

Ces étapes réinitialisent le journal de mise à jour pour le nouveau serveur KDC maître.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

6 Sur l'ancien KDC maître, arrêtez les processus `kadmind` et `krb5kdc`.

Lorsque vous interrompez le processus `kadmind`, vous empêchez toute modification apportée à la base de données KDC.

```
kdc1 # svcadm disable network/security/kadmin
kdc1 # svcadm disable network/security/krb5kdc
```

7 Sur l'ancien KDC maître, spécifiez la durée d'interrogation pour demander les propagations.

Mettez en commentaire l'entrée `sunw_dbprop_master_ulogsize` du fichier `/etc/krb5/kdc.conf` et ajoutez une entrée définissant `sunw_dbprop_slave_poll`. L'entrée définit la durée d'interrogation sur 2 minutes.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
#               sunw_dbprop_master_ulogsize = 1000
                sunw_dbprop_slave_poll = 2m
        }
```

8 Sur l'ancien KDC maître, déplacez les commandes de KDC maître et le fichier `kadm5.acl`.

Pour empêcher l'exécution des commandes de KDC maître, déplacez les commandes `kprop`, `kadmind` et `kadmin.local` à une place réservée.

```
kdc1 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc1 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc1 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
kdc1 # mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save
```

9 Sur le serveur DNS, modifiez les noms d'alias du KDC maître.

Pour changer de serveurs, modifiez le fichier de zone `example.com` et modifiez l'entrée pour `masterkdc`.

```
masterkdc IN CNAME kdc4
```

10 Sur le serveur DNS, redémarrez le serveur de nom de domaine Internet.

Exécutez la commande suivante pour recharger les nouvelles informations d'alias :

```
# svcadm refresh network/dns/server
```

11 Sur le nouveau KDC maître, déplacez les commandes de KDC maître et le fichier esclave `kpropd.acl`.

```
kdc4 # mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop
kdc4 # mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind
kdc4 # mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local
kdc4 # mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save
```

12 Sur le nouveau KDC maître, créez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC. Ce fichier doit également répertorier tous les esclaves qui émettent des requêtes de propagation incrémentielle. Pour plus d'informations, reportez-vous à la page de manuel `kadm5.acl(4)`.

```
kdc4 # cat /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM   *
kiprop/kdc1.example.com@EXAMPLE.COM p
```

13 Sur le nouveau KDC maître, spécifiez la taille de journal de mise à jour dans le fichier`kdc.conf`.

Mettez en commentaire l'entrée `sunw_dbprop_slave_poll` et ajoutez une entrée définissant `sunw_dbprop_master_ulogsize`. L'entrée définit la taille du journal à 1000 entrées.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
```

```
                        max_life = 8h 0m 0s
                        max_renewable_life = 7d 0h 0m 0s
                        sunw_dbprop_enable = true
                #       sunw_dbprop_slave_poll = 2m
                        sunw_dbprop_master_ulogsize = 1000
                }
```

14 Sur le nouveau KDC maître, ajoutez le principal `kiprop` au fichier keytab `kadmind`.

```
kdc4 # kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc4.example.com
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: quit
```

15 Sur le nouveau KDC maître, démarrez `kadmind` et `krb5kdc`.

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmin
```

16 Sur l'ancien KDC maître, ajoutez le principal de service `kiprop`.

L'ajout du principal `kiprop` au fichier `krb5.keytab` permet au démon `kpropd` de s'authentifier auprès du service de propagation incrémentielle.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Authenticating as pricipal kws/admin@EXAMPLE.COM with password.
Enter password:     <Type kws/admin password>
kadmin: ktadd kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

17 Sur l'ancien KDC maître, ajoutez une entrée pour chaque KDC répertorié dans `krb5.conf` au fichier de configuration de propagation, `kpropd.acl`.

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

```
host/kdc3.example.com@EXAMPLE.COM
host/kdc4.example.com@EXAMPLE.COM
```

18 Sur l'ancien KDC maître, démarrez `kpropd` et `krb5kdc`.

Lorsque le démon `krb5kdc`démarre, `kpropd` démarre également si le système est configuré en tant qu'esclave.

```
kdc1 # svcadm enable network/security/krb5kdc
```

Administration de la base de données Kerberos

La base de données Kerberos est l'épine dorsale de Kerberos et sa maintenance doit s'effectuer correctement. Cette section présente certaines procédures d'administration de la base de données Kerberos, telles que la sauvegarde et la restauration de la base de données, la définition de la propagation incrémentielle ou parallèle, ainsi que l'administration du fichier stash. Les étapes de configuration initiale de la base de données sont détaillées dans la section "Procédure de configuration manuelle d'un KDC maître" à la page 427.

Sauvegarde et propagation de la base de données Kerberos

La propagation de la base de données Kerberos du KDC maître au KDC esclave est l'une des tâches de configuration les plus importantes. Si la propagation n'est pas suffisamment fréquente, la synchronisation entre le KDC maître et les KDC esclaves est perdue. Par conséquent, en cas de défaillance du KDC maître, le KDC esclave n'aura pas les informations de base de données les plus récentes. En outre, si un KDC esclave a été configuré en tant que KDC maître à des fins d'équilibrage de charge, les clients qui utilisent le KDC esclave en tant que KDC maître ne disposeront pas des dernières informations. Par conséquent, vous devez vous assurer que la propagation est suffisamment fréquente ou configurer les serveurs pour une propagation incrémentielle, en fonction de la fréquence à laquelle vous modifiez la base de données Kerberos. La propagation incrémentielle est préférable à une propagation manuelle parce qu'elle élimine les frais d'administration liés à la propagation manuelle de la base de données. En outre, une propagation complète de la base de données n'est pas totalement efficace.

Lorsque vous configurez le KDC maître, vous configurez la commande `kprop_script` dans une tâche `cron` pour sauvegarder automatiquement la base de données Kerberos dans le fichier dump `/var/krb5/slave_datatrans` et la propager vers les KDC esclaves. Mais, comme avec n'importe quel fichier, la base de données Kerberos peut être corrompue. Si la corruption de données se produit sur un KDC esclave, il se peut que vous ne le remarquiez pas, dans la mesure où la propagation automatique suivante de la base de données permet d'installer une nouvelle copie. Toutefois, si la corruption se produit sur le KDC maître, la base de données corrompue est propagée à l'ensemble des KDC esclaves pendant la propagation suivante. Et, la sauvegarde corrompue écrase le fichier de sauvegarde non altéré précédent sur le KDC maître.

Parce qu'il n'y a pas de copie de sauvegarde "sûre" dans ce scénario, vous devez également définir une tâche `cron` pour copier, à intervalles réguliers, le fichier dump `slave_datatrans` dans un autre emplacement ou pour créer une autre copie de sauvegarde à l'aide de la commande `dump` de `kdb5_util`. Puis, si votre base de données est endommagée, vous pouvez restaurer la sauvegarde la plus récente sur le KDC maître en utilisant la commande `load` de `kdb5_util`.

Autre remarque importante : puisque le fichier dump de la base de données contient les clés de principal, vous devez protéger le fichier de tout accès par des utilisateurs non autorisés. Par défaut, la base de données du fichier de vidage dispose d'autorisations de lecture et d'écriture uniquement en tant que `root`. Afin de les protéger contre tout accès non autorisé, utilisez uniquement la commande `kprop` pour propager la base de données du fichier de vidage, qui chiffre les données en cours de transfert. En outre, `kprop` propage les données uniquement aux KDC esclaves, ce qui réduit les risques d'envoi par inadvertance du fichier dump de la base de données à des hôtes non autorisés.

Attention – Si la base de données Kerberos est mise à jour après sa propagation et que la base de données est ensuite corrompue avant la propagation suivante, les KDC esclaves ne contiennent pas les mises à jour. Les mises à jour seront perdues. Pour cette raison, si vous ajoutez des mises à jour importantes de la base de données Kerberos avant une propagation programmée, vous devez propager manuellement la base de données afin d'éviter toute perte de données.

Fichier `kpropd.acl`

Le fichier `kpropd.acl` sur un KDC esclave fournit une liste de noms d'hôte principal, un nom par ligne, qui spécifie les systèmes à partir desquels le KDC peut recevoir une base de données mise à jour par la propagation. Si le KDC maître est utilisé pour propager tous les KDC esclaves, le fichier `kpropd.acl` sur chaque esclave doit contenir uniquement le nom d'hôte principal du KDC maître.

Toutefois, l'installation de Kerberos et les étapes de configuration dans ce manuel vous indiquent que vous devez ajouter le même fichier `kpropd.acl` sur le KDC maître et les KDC esclaves. Ce fichier contient tous les noms de principaux d'hôtes KDC. Cette configuration vous permet de propager à partir de n'importe quel KDC, dans le cas où la propagation des KDC serait temporairement indisponible. De plus, en conservant une copie identique sur tous les KDC, la configuration est plus facile à gérer.

Commande `kprop_script`

La commande `kprop_script` utilise la commande `kprop` pour propager la base de données Kerberos à d'autres KDC. Si la commande `kprop_script` est exécutée sur un KDC esclave, elle se propage à la copie de la base de données Kerberos du KDC esclave vers d'autres KDC. La commande `kprop_script` accepte une liste de noms d'hôte pour les arguments, séparés par des espaces, qui indiquent les KDC à propager.

Quand `kprop_script` est exécutée, elle crée une copie de sauvegarde de la base de données Kerberos pour le fichier `/var/krb5/slave_datatrans` et copie le fichier dans les KDC spécifiés. La base de données Kerberos est verrouillée jusqu'à ce que la propagation soit terminée.

▼ Sauvegarde de la base de données Kerberos

1 Connectez-vous en tant que superutilisateur au KDC maître.

2 Sauvegardez la base de données Kerberos à l'aide de la commande `dump` de la commande `kdb5_util`.

`# /usr/sbin/kdb5_util dump [-verbose] [-d` *dbname*`] [`*filename* `[`*principals*`...]]`

`-verbose` Imprime le nom de chaque principal et stratégie en cours de sauvegarde.

dbname Définit le nom de la base de données à sauvegarder. Notez que vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si l'option `-d` n'est pas spécifiée, le nom de la base de données par défaut est `/var/krb5/principal` .

filename Définit le fichier utilisé pour sauvegarder la base de données. Vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si vous ne spécifiez pas un fichier, la base de données est transférée vers la sortie standard.

principals Définit une liste d'un ou plusieurs principaux (séparés par un espace) à sauvegarder. Vous devez utiliser des noms de principaux entièrement qualifiés. Si vous ne spécifiez aucun principal, l'intégralité de la base de données est sauvegardée.

Exemple 23–12 Sauvegarde de la base de données Kerberos

Dans l'exemple suivant, la base de données Kerberos est sauvegardée dans un fichier appelé `dumpfile`. Dans la mesure où l'option `-verbose` est spécifiée, chaque principal est imprimé lorsqu'il est sauvegardé.

```
# kdb5_util dump -verbose dumpfile
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/ENG.EXAMPLE.COM@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

Dans l'exemple suivant, les principaux `pak` et `pak/admin` de la base de données Kerberos sont sauvegardés.

```
# kdb5_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
```

▼ Procédure de restauration de la base de données Kerberos

1 **Connectez-vous en tant que superutilisateur au KDC maître.**

2 **Sur le serveur maître, arrêtez les démons KDC.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

3 **Restaurez la base de données Kerberos à l'aide de la commande `load` de la commande `kdb_util`.**

```
# /usr/sbin/kdb5_util load [-verbose] [-d dbname] [-update] [filename]
```

`-verbose` Imprime le nom de chaque principal et stratégie en cours de restauration.

dbname Définit le nom de la base de données à restaurer. Notez que vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si l'option `-d` n'est pas spécifiée, le nom de la base de données par défaut est `/var/krb5/principal` .

`-update` Met à jour la base de données existante. Dans le cas contraire, une nouvelle base de données est créée ou la base de données existante est écrasée.

filename Définit le fichier à partir duquel restaurer la base de données. Vous pouvez spécifier un chemin d'accès absolu pour le fichier.

4 **Démarrez les démons KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

Exemple 23–13 Restauration de la base de données Kerberos

Dans l'exemple suivant, la base de données appelée `database1` est restaurée dans le répertoire courant à partir du fichier `dumpfile`. Comme l'option `-update` n'est pas spécifiée, la restauration crée une nouvelle base de données.

```
# kdb5_util load -d database1 dumpfile
```

▼ Procédure de conversion d'une base de données Kerberos après une mise à niveau du serveur

Si votre base de données KDC a été créée sur un serveur exécutant la version Solaris 8 ou Solaris 9, la conversion de la base de données vous permet de tirer parti du format de base de données amélioré.

Avant de commencer Assurez-vous que la base de données utilise un format ancien.

1. **Sur le serveur maître, arrêtez les démons KDC.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

2. **Créez un répertoire pour stocker une copie temporaire de la base de données.**

```
kdc1 # mkdir /var/krb5/tmp
kdc1 # chmod 700 /var/krb5/tmp
```

3. **Videz la base de données KDC.**

```
kdc1 # kdb5_util dump /var/krb5/tmp/prdb.txt
```

4. **Enregistrez des copies des fichiers de la base de données actuelle.**

```
kdc1 # cd /var/krb5
kdc1 # mv princ* tmp/
```

5. **Chargez la base de données.**

```
kdc1 # kdb5_util load /var/krb5/tmp/prdb.txt
```

6. **Démarrez les démons KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

▼ Reconfiguration d'un KDC maître pour l'utilisation de la propagation incrémentielle

Les étapes de cette procédure peuvent être utilisées pour reconfigurer un KDC maître pour qu'il utilise la propagation incrémentielle. Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com`
- `admin` principal = `kws/admin`

1. **Ajoutez des entrées à `kdc.conf`.**

   Vous devez activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal. Pour plus d'informations, reportez-vous à la page de manuel `kdc.conf(4)`.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
```

```
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
        }
```

2 Créez le principal `kiprop`.

Le principal `kiprop` est utilisé pour authentifier le serveur KDC maître et autoriser les mises à jour depuis le KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

3 Ajoutez le principal `kiprop` au fichier keytab `kadmind`.

L'ajout du principal `kiprop` au fichier `kadm5.keytab` permet à la commande `kadmind` de s'authentifier elle-même lorsqu'elle est démarrée.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: quit
```

4 Sur le KDC maître, ajoutez une entrée kiprop au fichier `kadm5.acl`.

Cette entrée permet au KDC maître de recevoir des demandes de propagation incrémentielle du serveur `kdc2`.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

5 **Mettez en commentaire la ligne `kprop` dans le fichier crontab `root`.**

Cette étape permet d'éviter que le KDC maître ne propage sa copie de la base de données KDC.

```
kdc1 # crontab -e
#ident  "@(#)root       1.20    01/11/06 SMI"
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * * /usr/sbin/logadm
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
#10 3 * * * /usr/lib/krb5kprop_script kdc2.example.sun.com #SUNWkr5ma
```

6 **Redémarrez `kadmind`.**

```
kdc1 # svcadm restart network/security/kadmin
```

7 **Reconfigurez tous les serveurs KDC esclaves qui utilisent la propagation incrémentielle.**

Reportez-vous à la section "Procédure de reconfiguration d'un KDC esclave pour l'utilisation de la propagation incrémentielle" à la page 483 pour obtenir des instructions complètes.

▼ Procédure de reconfiguration d'un KDC esclave pour l'utilisation de la propagation incrémentielle

1 **Ajoutez des entrées à `krb5.conf`.**

Les nouvelles entrées autorisent la propagation incrémentielle et définissent la durée d'interrogation à 2 minutes.

```
kdc2 # cat /etc/krb5/krb5.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM= {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_slave_poll = 2m
        }
```

2 Ajoutez le principal `kiprop` au fichier `krb5.keytab` .

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

3 Désactivez `kpropd`.

```
kdc2 # svcadm disable network/security/krb5_prop
```

4 Redémarrez le serveur KDC.

```
kdc2 # svcadm restart network/security/krb5kdc
```

▼ Procédure de configuration d'un KDC esclave pour l'utilisation de la propagation complète

Cette procédure montre comment reconfigurer un serveur KDC esclave exécutant la version Solaris10 pour qu'il utilise la propagation complète. Normalement, la procédure est nécessaire uniquement si le serveur KDC maître exécute la version Solaris 9 ou une version antérieure. Dans ce cas, le serveur KDC maître ne prend pas en charge la propagation incrémentielle, de sorte que le serveur esclave doit être configuré pour que la propagation fonctionne.

Dans cette procédure, un KDC esclave nommé `kdc3` est configuré. Cette procédure utilise les paramètres de configuration ci-dessous :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com` et `kdc3.example.com`
- `admin` principal = `kws/admin`
- URL de l'aide en ligne = `http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

Remarque – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "URL d'aide en ligne dans l'outil d'administration graphique de Kerberos " à la page 424.

Avant de commencer Le KDC maître doit être configuré. Pour obtenir des instructions spécifiques afin de déterminer si cet esclave doit être échangeable, reportez-vous à la section "Échange d'un KDC maître et d'un KDC esclave" à la page 472.

1 Sur le KDC maître, connectez-vous en tant que superutilisateur.

2 Sur le KDC maître, démarrez `kadmin`.

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

a. Sur le KDC maître, ajoutez des principaux d'hôtes esclaves à la base de données, si ce n'est pas déjà fait.

Pour que l'esclave fonctionne, il doit avoir un hôte principal. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc3.example.com
Principal "host/kdc3@EXAMPLE.COM" created.
kadmin:
```

b. Quittez `kadmin`.

```
kadmin: quit
```

3 Sur le KDC maître, modifiez le fichier de configuration Kerberos (`krb5.conf`).

Vous devez ajouter une entrée pour chaque esclave. Pour une description complète de ce fichier, reportez-vous à la page de manuel `krb5.conf(4)`.

```
kdc1 # cat /etc/krb5/krb5.conf
 .
 .
[realms]
                EXAMPLE.COM = {
                kdc = kdc1.example.com
                kdc = kdc2.example.com
                kdc = kdc3.example.com
                admin_server = kdc1.example.com
        }
```

4. **Sur le KDC maître, ajoutez une entrée pour le KDC maître et chaque KDC esclave dans le fichier `kpropd.acl`.**

   Reportez-vous à la page de manuel kprop(1M)pour obtenir une description complète de ce fichier.

   ```
   kdc1 # cat /etc/krb5/kpropd.acl
   host/kdc1.example.com@EXAMPLE.COM
   host/kdc2.example.com@EXAMPLE.COM
   host/kdc3.example.com@EXAMPLE.COM
   ```

5. **Sur tous les KDC esclaves, copiez les fichiers d'administration à partir du serveur KDC maître.**

   Cette étape doit être effectuée sur tous les KDC esclaves, car le serveur KDC maître a mis à jour des informations requises par chaque serveur KDC. Vous pouvez utiliser `ftp` ou tout autre mécanisme de transfert similaire pour extraire des copies des fichiers suivants du KDC maître :

   - `/etc/krb5/krb5.conf`
   - `/etc/krb5/kdc.conf`
   - `/etc/krb5/kpropd.acl`

6. **Sur tous les KDC esclaves, assurez-vous que le fichier d'ACL Kerberos, `kadm5.acl`, n'est pas renseigné.**

   Un fichier `kadm5.acl` non modifié ressemble à ce qui suit :

   ```
   kdc2 # cat /etc/krb5/kadm5.acl
   */admin@___default_realm___ *
   ```

   Si le fichier contient des entrées `kiprop`, supprimez-les.

7. **Sur le nouvel esclave, démarrez la commande `kadmin`.**

   Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

   ```
   kdc2 # /usr/sbin/kadmin -p kws/admin
   Enter password:      <Type kws/admin password>
   kadmin:
   ```

   a. **Ajoutez le principal `host` de l'esclave au fichier keytab de ce dernier en utilisant `kadmin`.**

      Cette entrée permet à `kprop` et à d'autres applications utilisant Kerberos de fonctionner. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le fichier `/etc/resolv.conf`.

```
kadmin: ktadd host/kdc3.example.com
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type ArcFour
```

```
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

b. Quittez `kadmin`.

```
kadmin: quit
```

8 Sur le KDC maître, ajoutez le nom du KDC esclave à la tâche `cron` , qui exécute automatiquement les sauvegardes, en exécutant `crontab -e`.

Ajoutez le nom de chaque serveur KDC esclave à la fin de la ligne `kprop_script`.

```
10 3 * * * /usr/lib/krb5/kprop_script kdc2.example.com kdc3.example.com
```

Vous pouvez aussi modifier l'heure des sauvegardes. Cette entrée démarre le processus de sauvegarde tous les jours à 3h10.

9 Sur le nouvel esclave, démarrez le démon de propagation Kerberos.

```
kdc3 # svcadm enable network/security/krb5_prop
```

10 Sur le KDC maître, sauvegardez et propagez la base de données à l'aide de `kprop_script`.

Si une copie de sauvegarde de la base de données est déjà disponible, il n'est pas nécessaire d'effectuer une autre sauvegarde. Reportez-vous à la section "Propagation manuelle de la base de données Kerberos aux KDC esclaves" à la page 489 pour obtenir des instructions.

```
kdc1 # /usr/lib/krb5/kprop_script kdc3.example.com
Database propagation to kdc3.example.com: SUCCEEDED
```

11 Sur le nouvel esclave, créez un fichier stash à l'aide de `kdb5_util` .

```
kdc3 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key

Enter KDC database master key:      <Type the key>
```

12 (Facultatif) Sur le nouveau KDC esclave, synchronisez l'horloge du KDC maître à l'aide du protocole NTP ou d'un autre mécanisme de synchronisation de l'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 470.

13 Sur le nouvel esclave, démarrez le démon KDC (`krb5kdc`).

```
kdc3 # svcadm enable network/security/krb5kdc
```

▼ Procédure de vérification de la synchronisation des serveurs KDC

Si la propagation incrémentielle a été configurée, cette procédure permet de s'assurer que les informations sur le KDC esclave ont été mises à jour.

1. **Sur le serveur KDC maître, exécutez la commande `kproplog`.**

   ```
   kdc1 # /usr/sbin/kproplog -h
   ```

2. **Sur un serveur KDC esclave, exécutez la commande `kproplog`.**

   ```
   kdc2 # /usr/sbin/kproplog -h
   ```

3. **Vérifiez que les valeurs du dernier numéro de série et du dernier horodatage correspondent.**

Exemple 23–14 Vérification de la synchronisation des serveurs KDC

L'exemple suivant est un exemple des résultats de l'exécution de la commande `kproplog` sur le serveur KDC maître.

```
kdc1 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulog)
Update log dump:
    Log version #: 1
    Log state: Stable
    Entry block size: 2048
    Number of entries: 2500
    First serial #: 137966
    Last serial #: 140465
    First time stamp: Fri Nov 28 00:59:27 2004
    Last time stamp: Fri Nov 28 01:06:13 2004
```

L'exemple suivant est un exemple des résultats de l'exécution de la commande `kproplog` sur le serveur KDC esclave.

```
kdc2 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulog)
Update log dump:
    Log version #: 1
    Log state: Stable
    Entry block size: 2048
    Number of entries: 0
    First serial #: None
    Last serial #: 140465
    First time stamp: None
    Last time stamp: Fri Nov 28 01:06:13 2004
```

Notez que les valeurs pour le dernier numéro de série et le dernier horodatage sont identiques, ce qui indique que l'esclave est synchronisé avec le serveur KDC maître.

Dans la sortie du serveur KDC esclave, notez qu'aucune entrée de mise à jour n'existe dans le journal de mise à jour du serveur KDC esclave. Il n'y a pas d'entrées dans la mesure où le serveur KDC esclave ne conserve pas de jeu de mises à jour, à l'inverse du serveur KDC maître. En outre, le serveur KDC esclave n'inclut pas d'informations sur le premier numéro de série ou le premier horodatage car il ne s'agit pas d'informations pertinentes.

▼ Propagation manuelle de la base de données Kerberos aux KDC esclaves

Cette procédure vous indique comment propager la base de données Kerberos à l'aide de la commande `kprop`. Utilisez cette procédure si vous avez besoin de synchroniser un KDC esclave avec le KDC maître à l'extérieur de la tâche périodique `cron`. À la différence de `kprop_script` , vous pouvez utiliser `kprop` pour propager uniquement la sauvegarde actuelle de la base de données sans nouvelle sauvegarde préalable de la base de données Kerberos.

Remarque – N'utilisez pas cette procédure si vous utilisez la propagation incrémentielle.

1. **Connectez-vous en tant que superutilisateur au KDC maître.**
2. **(Facultatif) Sauvegardez la base de données à l'aide de la commande `kdb5_util`.**

   ```
   # /usr/sbin/kdb5_util dump /var/krb5/slave_datatrans
   ```

3. **Propagez la base de données à un KDC esclave en utilisant la commande `kprop`.**

   ```
   # /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC
   ```

Exemple 23–15 Propagation manuelle de la base de données Kerberos au KDC esclave à l'aide de `kprop_script`

Si vous souhaitez sauvegarder la base de données et la propager à un KDC esclave à l'extérieur de la tâche périodique `cron`, vous pouvez également utiliser la commande `kprop_script` comme suit :

```
# /usr/lib/krb5/kprop_script slave-KDC
```

Configuration d'une propagation parallèle

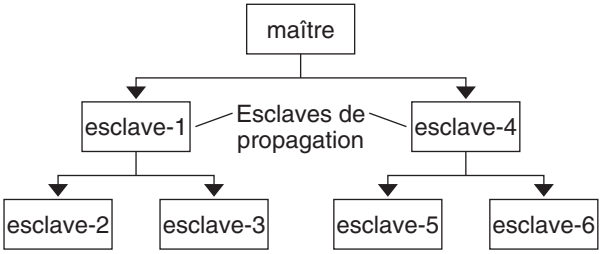
Dans la plupart des cas, le KDC maître est utilisé exclusivement pour propager sa base de données Kerberos aux KDC esclaves. Cependant, si votre site comporte beaucoup de KDC esclaves, vous pouvez envisager le partage de la charge du processus de propagation, aussi appelé *propagation parallèle*.

Remarque – N'utilisez pas cette procédure si vous utilisez la propagation incrémentielle.

La propagation parallèle autorise des KDC esclaves spécifiques à partager les fonctions de propagation avec le KDC maître. Ce partage permet à la propagation de s'effectuer plus rapidement et d'alléger la charge du KDC maître.

Par exemple, supposons que votre site dispose d'un KDC maître et de six KDC esclaves (illustrés dans la Figure 23–2), où `slave-1` jusqu'à `slave-3` correspond à un regroupement logique et `slave-4` jusqu'à `slave-6` correspond à un autre regroupement logique. Pour configurer une propagation parallèle, vous pouvez faire en sorte que le KDC maître propage la base de données à `slave-1` et `slave-4`. À leur tour, ces KDC esclaves pourraient propager la base de données aux KDC esclaves dans leur groupe.

FIGURE 23–2 Exemple de configuration de propagation parallèle



Étapes de configuration d'une propagation parallèle

Ce qui suit n'est pas une procédure détaillée étape par étape, mais une liste de haut niveau des étapes de configuration permettant d'activer la propagation parallèle. Ces étapes impliquent ce qui suit :

1. Sur le KDC maître, modification de l'entrée `kprop_script` dans sa tâche `cron` afin d'inclure les arguments uniquement pour les KDC esclaves qui effectueront la propagation suivante (les *esclaves de propagation*).

2. Sur chaque esclave de propagation, l'ajout d'une entrée `kprop_script` dans sa tâche `cron`, qui doit inclure les arguments pour que les esclaves réalisent la propagation. Pour que la propagation parallèle s'effectue, la tâche `cron` doit être configurée de sorte qu'elle s'exécute après que la nouvelle base de données Kerberos soit propagée à l'esclave de propagation.

   Remarque – Le temps que prend un esclave de propagation à se propager dépend de facteurs tels que la bande passante du réseau et la taille de la base de données Kerberos.

3. Sur chaque KDC esclave, configurez les autorisations appropriées à propager. Cette étape s'effectue en ajoutant le nom de l'hôte principal de son KDC de propagation à son fichier `kpropd.acl`.

EXEMPLE 23–16 Configuration d'une propagation parallèle

Dans la Figure 23–2, l'entrée `kprop_script` du KDC maître doit ressembler à ce qui suit :

```
0 3 * * * /usr/lib/krb5/kprop_script slave-1.example.com slave-4.example.com
```

L'entrée `kprop_script` du `slave-1` doit ressembler à ce qui suit :

```
0 4 * * * /usr/lib/krb5/kprop_script slave-2.example.com slave-3.example.com
```

Notez que la propagation sur l'esclave démarre une heure après sa propagation par le maître.

Le fichier `kpropd.acl` sur les esclaves de propagation doit contenir l'entrée suivante :

```
host/master.example.com@EXAMPLE.COM
```

Le fichier `kpropd.acl` sur les KDC esclaves propagés par `slave-1` contient l'entrée suivante :

```
host/slave-1.example.com@EXAMPLE.COM
```

Administration du fichier stash

Le *fichier stash* contient la clé principale de la base de données Kerberos, qui est créée automatiquement lorsque vous créez une base de données Kerberos. Si le fichier stash est corrompu, vous pouvez utiliser la commande `stash` de l'utilitaire `kdb5_util` pour remplacer le fichier corrompu. Le seul moment où vous devez supprimer un fichier stash est après la suppression de la base de données Kerberos avec la commande `destroy` de `kdb5_util`. Dans la mesure où le fichier stash n'est pas automatiquement supprimé avec la base de données, vous devez d'abord supprimer le fichier stash pour terminer le nettoyage.

▼ Procédure de suppression d'un fichier stash

1 **Connectez-vous en tant que superutilisateur au KDC contenant le fichier stash.**

2 **Supprimez le fichier stash.**

```
# rm stash-file
```

Où *stash-file* est le chemin d'accès du fichier stash. Par défaut, le fichier stash est situé dans `/var/krb5/.k5.` *realm*.

Remarque – Si vous devez recréer le fichier stash, vous pouvez utiliser l'option `-f` de la commande `kdb5_util`.

Gestion d'un KDC sur un serveur d'annuaire LDAP

La plupart des tâches d'administration du KDC qui utilisent un serveur d'annuaire LDAP sont identiques à celles du serveur DB2. Il existe quelques nouvelles tâches spécifiques à l'utilisation de LDAP.

TABLEAU 23–3 Configuration des serveurs KDC pour l'utilisation de LDAP (liste des tâches)

Tâche	Description	Voir
Configuration d'un KDC maître	Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus manuel et à l'aide de LDAP pour le KDC.	"Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP" à la page 433
Association des attributs de principaux Kerberos aux types de classe objet non Kerberos.	Permet de partager les informations stockées avec les enregistrements Kerberos avec d'autres bases de données LDAP.	"Procédure d'association des attributs de principaux Kerberos dans un type de classe d'objet non Kerberos" à la page 492
Destruction d'un domaine	Supprime toutes les données associées à un domaine.	"Procédure de suppression d'un domaine d'un serveur d'annuaire LDAP" à la page 493

▼ Procédure d'association des attributs de principaux Kerberos dans un type de classe d'objet non Kerberos

Cette procédure permet aux attributs de principaux Kerberos d'être associés aux types de classe d'objet non Kerberos. Dans cette procédure, les attributs `krbprincipalaux`, `krbTicketPolicyAux` et `krbPrincipalName` sont associés à la classe d'objet "personnes".

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Serveur d'annuaire = `dsserver.example.com`
- Principal d'utilisateur = `willf@EXAMPLE.COM`

1 Connectez-vous en tant que superutilisateur.

2 Préparez chaque entrée dans les classes d'objet personnes.

Répétez cette étape pour chaque entrée.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
dn: uid=willf,ou=people,dc=example,dc=com
changetype: modify
objectClass: krbprincipalaux
objectClass: krbTicketPolicyAux
krbPrincipalName: willf@EXAMPLE.COM
EOF
```

3 Ajoutez un attribut de sous-arborescence pour le conteneur de domaine.

Cette étape permet d'effectuer des recherches d'entrées de principal dans le conteneur `ou=people,dc=example,dc=com` , ainsi que dans le conteneur EXAMPLE.COM par défaut.

```
# kdb5_ldap_util -D "cn=directory manager" modify \
            -subtrees 'ou=people,dc=example,dc=com' -r EXAMPLE.COM
```

4 (Facultatif) Si les enregistrements de KDC sont stockés dans DB2, migrez les entrées DB2.

a. Videz les entrées DB2.

```
# kdb5_util dump > dumpfile
```

b. Chargez la base de données dans le serveur LDAP.

```
# kdb5_util load -update dumpfile
```

5 (Facultatif) Ajoutez les attributs de principal au KDC.

```
# kadmin.local -q 'addprinc willf'
```

▼ Procédure de suppression d'un domaine d'un serveur d'annuaire LDAP

Cette procédure peut être utilisée si un autre serveur d'annuaire LDAP a été configuré pour gérer un domaine.

1 Connectez-vous en tant que superutilisateur.

2 Supprimez le domaine.

```
# kdb5_ldap_util -D "cn=directory manager" destroy
```

Renforcement de la sécurité des serveurs Kerberos

Suivez les étapes ci-dessous pour accroître la sécurité des serveurs d'application Kerberos et des serveurs KDC.

TABLEAU 23–4 Renforcement de la sécurité des serveurs Kerberos (liste des tâches)

Tâche	Description	Voir
Activation de l'accès à l'aide de l'authentification Kerberos	Limitez l'accès réseau à un serveur pour permettre l'authentification Kerberos uniquement	"Procédure d'activation des applications utilisant Kerberos uniquement" à la page 494
Restriction de l'accès aux serveurs KDC	Améliorez la sécurité des serveurs KDC et de leurs données.	"Procédure de restriction de l'accès aux serveurs KDC" à la page 495
Amélioration de la sécurité du mot de passe à l'aide d'un fichier de dictionnaire	Augmentez la sécurité de tous les nouveaux mots de passe en vérifiant le nouveau mot de passe par rapport à un dictionnaire.	"Utilisation d'un fichier dictionnaire pour augmenter la sécurité de mot de passe" à la page 495

▼ Procédure d'activation des applications utilisant Kerberos uniquement

Cette procédure restreint l'accès réseau au serveur qui exécute `telnet`, `ftp`, `rcp`, `rsh` et `rlogin` pour utiliser des transactions authentifiées par Kerberos uniquement.

1 Modifiez la propriété `exec` pour le service `telnet`.

Ajoutez l'option `-a user` à la propriété `exec` pour `telnet` pour limiter l'accès aux utilisateurs capables de fournir des informations d'authentification valides.

```
# inetadm -m svc:/network/telnet:default exec="/usr/sbin/in.telnetd -a user"
```

2 (Facultatif) Si elle n'est pas déjà configurée, modifiez la propriété `exec` pour le service `telnet`.

Ajoutez l'option `-a` à la propriété `exec` pour que `ftp` autorise uniquement les connexions authentifiées par Kerberos.

```
# inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a"
```

3 Désactivez les autres services.

Les démons `in.rshd` et `in.rlogind` doivent être désactivés.

```
# svcadm disable network/shell
# svcadm disable network/login:rlogin
```

▼ Procédure de restriction de l'accès aux serveurs KDC

Les serveurs KDC maîtres et esclaves disposent de copies de la base de données KDC stockées localement. La restriction de l'accès à ces serveurs pour sécuriser les bases de données est importante pour la sécurité globale de l'installation Kerberos.

1 Désactivez les services distants, en fonction des besoins.

Pour fournir un serveur KDC sécurisé, tous les services réseau non essentiels doivent être désactivés. Selon votre configuration, certains de ces services sont peut-être déjà désactivés. Vérifiez le statut du service avec la commande `svcs`. Dans la plupart des cas, les seuls services devant s'exécuter sont `krb5kdc` et `kadmin`, si le KDC est un maître. En outre, tous les services utilisant l'interface de transport loopback (`ticlts`, `ticotsord` et `ticots`) peuvent rester activés.

```
# svcadm disable network/comsat
# svcadm disable network/dtspc/tcp
# svcadm disable network/finger
# svcadm disable network/login:rlogin
# svcadm disable network/rexec
# svcadm disable network/shell
# svcadm disable network/talk
# svcadm disable network/tname
# svcadm disable network/uucp
# svcadm disable network/rpc_100068_2-5/rpc_udp
```

2 Restreignez l'accès au matériel prenant en charge le KDC.

Pour limiter l'accès physique, assurez-vous que le serveur KDC et son moniteur se trouvent dans un site sécurisé. Les utilisateurs ne doivent pas être en mesure d'accéder à ce serveur d'une façon ou d'une autre.

3 Stockez les sauvegardes de la base de données KDC sur des disques locaux ou les KDC esclaves.

Réalisez des sauvegardes sur bande de votre KDC uniquement si les bandes sont stockées en toute sécurité. Suivez la même pratique pour les copies de fichiers keytab. Il serait préférable de stocker ces fichiers sur un système de fichiers local non partagé avec d'autres systèmes. Le système de stockage de fichiers peut être le serveur KDC maître ou n'importe lequel des KDC esclaves.

▼ Utilisation d'un fichier dictionnaire pour augmenter la sécurité de mot de passe

Un fichier dictionnaire peut être utilisé par le service Kerberos pour éviter qu'un mot dans le dictionnaire soit utilisé en tant que mot de passe lors de la création de nouvelles informations d'identification. Pour rendre plus difficile le fait de deviner un mot de passe, il est judicieux d'éviter l'utilisation de mots du dictionnaire en tant mots de passe. Par défaut, le fichier `/var/krb5/kadm5.dict` est utilisé, mais il est vide.

1 Connectez-vous en tant que superutilisateur au KDC maître.

2 Éditez le fichier de configuration KDC (`kdc.conf`).

Vous devez ajouter une ligne afin d'informer le service d'utiliser un fichier dictionnaire. Dans cet exemple, le dictionnaire utilisé est celui inclus dans l'utilitaire `spell`. Reportez-vous à la page de manuel `kdc.conf(4)` pour obtenir une description complète du fichier de configuration.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
        kdc_ports = 88,750

[realms]
        EXAMPLE.COM = {
                profile = /etc/krb5/krb5.conf
                database_name = /var/krb5/principal
                admin_keytab = /etc/krb5/kadm5.keytab
                acl_file = /etc/krb5/kadm5.acl
                kadmind_port = 749
                max_life = 8h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                sunw_dbprop_enable = true
                sunw_dbprop_master_ulogsize = 1000
                dict_file = /usr/share/lib/dict/words
                }
```

3 Redémarrez les démons Kerberos.

```
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

◆ ◆ ◆ CHAPITRE 24

Messages d'erreur et dépannage de Kerberos

Ce chapitre fournit les solutions aux messages d'erreur que vous pouvez recevoir lorsque vous utilisez le service Kerberos. Ce chapitre fournit également quelques conseils de dépannage pour différents problèmes. La liste suivante répertorie les informations fournies dans ce chapitre :

Messages d'erreur Kerberos

Cette section fournit des informations sur les messages d'erreur Kerberos, y compris la raison de chaque erreur et une façon de corriger la corriger.

Messages d'erreur de l'outil SEAM

`Unable to view the list of principals or policies; use the Name field.`

Origine : Le principal `admin` avec lequel vous vous êtes connecté n'a pas de privilège de liste (`l`) dans le fichier ACL de Kerberos (`kadm5.acl`). Par conséquent, vous ne pouvez pas afficher la liste des principaux ou la liste des stratégies.

Solution : Vous devez saisir les noms des principaux et des stratégies dans le champ de nom pour travailler sur ces derniers, ou vous devez vous connecter à l'aide d'un principal qui dispose des privilèges appropriés.

`JNI: Java array creation failed`

`JNI: Java class lookup failed`

`JNI: Java field lookup failed`

`JNI: Java method lookup failed`

`JNI: Java object lookup failed`

`JNI: Java object field lookup failed`

`JNI: Java string access failed`

`JNI: Java string creation failed`

Origine : Un grave problème existe avec l'interface native Java utilisée par l'outil SEAM (`gkadmin`).

Solution : Quittez `gkadmin` et redémarrez-le. Si le problème persiste, veuillez signaler un bogue.

Messages d'erreur Kerberos courants (A-M)

Cette section fournit une liste alphabétique (A-M) des messages d'erreur courants pour les commandes Kerberos, les démons Kerberos, la structure PAM, l'interface GSS, le service NFS et la bibliothèque Kerberos.

`All authentication systems disabled; connection refused`

Origine : Cette version de `rlogind` ne prend pas en charge de mécanisme d'authentification.

Solution : Vérifiez que la commande `rlogind` est appelée avec l'option `-k`.

`Another authentication mechanism must be used to access this host`

Origine : L'authentification n'a pas pu être effectuée.

Solution : Assurez-vous que le client utilise le mécanisme Kerberos V5 pour l'authentification.

`Authentication negotiation has failed, which is required for encryption. Good bye.`

Origine : L'authentification n'a pas pu être négociée avec le serveur.

Solution : Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle authdebug` et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

`Bad krb5 admin server hostname while initializing kadmin interface`

Origine : Un nom d'hôte non valide est configuré pour `admin_server` dans le fichier `krb5.conf`.

Solution : Assurez-vous que le nom d'hôte correct pour le KDC maître est indiqué sur la ligne `admin_server` du fichier `krb5.conf`.

`Bad lifetime value`
Origine : La valeur de durée de vie fournie n'est pas valide ou incorrectement formatée.

Solution : Assurez-vous que la valeur fournie est cohérente avec la section des formats d'heure de la page de manuel `kinit(1)`.

`Bad start time value`
Origine : La valeur d'heure de démarrage fournie n'est pas valide ou incorrectement formatée.

Solution : Assurez-vous que la valeur fournie est cohérente avec la section des formats d'heure de la page de manuel `kinit(1)`.

`Cannot contact any KDC for requested realm`
Origine : Aucun KDC n'a répondu dans le domaine demandé.

Solution : Assurez-vous qu'au moins un KDC (maître ou esclave) est accessible ou que le démon `krb5kdc` est en cours d'exécution sur les KDC. Consultez le fichier `/etc/krb5/krb5.conf` pour la liste de KDC configurés (`kdc` = *kdc-name*).

`Cannot determine realm for host`
Origine : Kerberos n'est pas en mesure de déterminer le nom de domaine de l'hôte.

Solution : Assurez-vous qu'il y a un nom de domaine par défaut ou que les mappages de nom de domaine sont définis dans le fichier de configuration Kerberos (`krb5.conf`).

`Cannot find KDC for requested realm`
Origine : Aucun KDC n'a été trouvé dans le domaine demandé.

Solution : Assurez-vous que le fichier de configuration Kerberos (`krb5.conf`) indique un KDC dans la section `realm` .

`cannot initialize realm` *realm-name*
Origine : Le KDC n'a peut-être pas de fichier stash.

Solution : Assurez-vous que le KDC dispose d'un fichier stash. Si tel n'est pas le cas, créez un fichier stash en utilisant la commande `kdb5_util` et essayez de redémarrer la commande `krb5kdc`.

`Cannot resolve KDC for requested realm`
Origine : Kerberos n'est pas en mesure de déterminer un KDC pour le domaine.

Solution : Assurez-vous que le fichier de configuration Kerberos (`krb5.conf`) indique un KDC dans la section `realm` .

`Cannot reuse password`

Origine : Le mot de passe que vous avez spécifié a déjà été utilisé par ce principal.

Solution : Choisissez un mot de passe qui n'a pas été choisi avant, ou du moins qui ne fait pas partie des mots de passe qui sont conservés dans la base de données KDC pour chaque principal. Cette stratégie est appliquée par la stratégie du principal.

`Can't get forwarded credentials`

Origine : Le transfert de données d'identification n'a pas pu être établi.

Solution : Assurez-vous que le principal dispose d'informations d'identification transmissibles.

`Can't open/find Kerberos configuration file`

Origine : Le fichier de configuration Kerberos (`krb5.conf`) n'était pas disponible.

Solution : Assurez-vous que le `krb5.conf` est disponible au bon emplacement et qu'il dispose des autorisations nécessaires. Ce fichier doit être accessible en écriture par `root` et lisible par tout le monde.

`Client did not supply required checksum--connection rejected`

Origine : L'authentification avec somme de contrôle n'a pas été négociée avec le client. Le client utilise peut-être un ancien protocole Kerberos V5 qui ne prend pas en charge la prise en charge de connexion initiale.

Solution : Assurez-vous que le client utilise un protocole Kerberos V5 qui prend en charge la prise en charge de connexion initiale.

`Client/server realm mismatch in initial ticket request`

Origine : Un conflit de domaine entre le client et le serveur s'est produit dans la requête de ticket initiale.

Solution : Assurez-vous que le serveur avec lequel vous communiquez est dans le même domaine que le client, ou que les configurations du domaine sont correctes.

`Client or server has a null key`

Origine : Le principal a une clé nulle.

Solution : Modifiez le principal afin qu'il dispose d'une clé non nulle en utilisant la commande `cpw` de `kadmin`.

`Communication failure with server while initializing kadmin interface`

Origine : Le démon `kadmind` n'était pas en cours d'exécution sur l'hôte qui a été spécifié pour le serveur d'administration, également appelé KDC maître.

Solution : Assurez-vous d'avoir spécifié le nom d'hôte correct pour le KDC maître. Si vous avez spécifié le nom d'hôte correct, assurez-vous que `kadmind` est en cours d'exécution sur le KDC maître que vous avez spécifié.

`Credentials cache file permissions incorrect`

Origine : Vous ne disposez pas des autorisations de lecture ou d'écriture sur le cache d'informations d'identification (`/tmp/krb5cc_` *uid*).

Solution : Assurez-vous que vous disposez des autorisations de lecture ou d'écriture sur le cache d'informations d'identification.

`Credentials cache I/O operation failed` *XXX*

Origine : Kerberos a rencontré un problème lors de l'écriture dans le cache d'informations d'identification du système (`/tmp/krb5cc_`*uid*).

Solution : Assurez-vous que le cache d'informations d'identification n'a pas été supprimé et qu'il reste de l'espace sur le périphérique en utilisant la commande `df`.

`Decrypt integrity check failed`

Origine : Vous avez peut-être un ticket non valide.

Solution : Vérifiez les deux conditions suivantes :

- Assurez-vous que vos informations d'identification sont valides. Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.
- Assurez-vous que l'hôte cible dispose d'un fichier keytab avec la version correcte de la clé du service. Utilisez `kadmin` pour afficher le numéro de version de la clé du principal service (par exemple, `host/`*FQDN-hostname*) dans la base de données Kerberos. Utilisez également `klist -k` sur l'hôte cible pour vérifiez qu'il a le même numéro de version de clé.

`Encryption could not be enabled. Goodbye.`

Origine : Le chiffrement n'a pas pu être négocié avec le serveur.

Solution : Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle encdebug` et consultez les messages de débogage pour en savoir plus.

`failed to obtain credentials cache`

Origine : Pendant l'initialisation de `kadmin`, une panne s'est produite lorsque `kadmin` a essayé afin d'obtenir des informations d'identification pour le principal `admin`.

Solution : Assurez-vous que vous avez utilisé le bon principal et le bon mot de passe lorsque vous avez exécuté `kadmin`.

`Field is too long for this implementation`
Origine : Le message qui a été envoyé par une application utilisant Kerberos était trop long. Cette erreur peut être générée si le protocole de transport est UDP, dont la taille maximale de message par défaut est 65535 octets. En outre, il existe des limites sur les champs individuels dans un message de protocole qui est envoyé par le service Kerberos.

Solution : Vérifiez que vous n'avez pas restreint le transport à UDP dans le fichier `/etc/krb5/kdc.conf` du serveur KDC.

`GSS-API (or Kerberos) error`
Origine : Ce message est un message d'erreur GSS-API ou Kerberos générique pouvant être causé par divers problèmes.

Solution : Vérifiez le fichier `/var/krb5/kdc.log` pour trouver le message d'erreur plus spécifique qui a été enregistré lorsque l'erreur s'est produite.

`Hostname cannot be canonicalized`
Origine : Le client Kerberos ne peut pas trouver le nom d'hôte complet pour le serveur.

Solution : Assurez-vous que le nom d'hôte du serveur est défini dans le DNS et que les mappages adresse sur nom d'hôte et nom d'hôte sur adresse sont cohérents.

`Illegal cross-realm ticket`
Origine : Le ticket envoyé n'a pas les bons inter-domaines. Les domaines n'ont peut-être pas les bonnes relations d'approbation configurées.

Solution : Assurez-vous que les domaines que vous utilisez ont les bonnes relations d'approbation.

`Improper format of Kerberos configuration file`
Origine : Le fichier de configuration Kerberos a des entrées non valides.

Solution : Assurez-vous que toutes les relations dans le fichier `krb5.conf` sont suivies du signe " = "et d'une valeur. En outre, vérifiez que les crochets sont présents dans les paires pour chaque sous-section.

`Inappropriate type of checksum in message`
Origine : Le message contient une somme de contrôle non valide.

Solution : Vérifiez quels types de somme de contrôle valides sont indiqués dans les fichiers `krb5.conf` et `kdc.conf` .

`Incorrect net address`
Origine : Une incohérence s'est produite dans l'adresse réseau. L'adresse réseau dans le ticket qui a était transmis est différente de l'adresse réseau où le ticket a été traité. Ce message peut se produire lorsque des tickets sont transmis.

Solution : Assurez-vous que les adresses réseau sont correctes. Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.

`Invalid credential was supplied`

`Service key not available`

Origine : Le ticket de service du cache d'informations d'identification est peut-être incorrect.

Solution : Détruisez le cache d'informations d'identification actuel et exécutez de nouveau `kinit` avant d'essayer d'utiliser ce service.

`Invalid flag for file lock mode`

Origine : Une erreur Kerberos interne s'est produite.

Solution : Veuillez signaler un bogue.

`Invalid message type specified for encoding`

Origine : Kerberos n'a pas pu reconnaître le type de message qui a été envoyé par l'application utilisant Kerberos.

Solution : Si vous utilisez une application utilisant Kerberos qui a été développé par votre site ou un fournisseur, assurez-vous qu'elle utilise Kerberos correctement.

`Invalid number of character classes`

Origine : Le mot de passe que vous avez spécifié pour le principal ne contient pas suffisamment de classes de mot de passe, tel qu'appliqué par la stratégie du principal.

Solution : Assurez-vous que vous avez spécifié un mot de passe avec le nombre minimal de classes de mot de passe requis par la stratégie.

`KADM err: Memory allocation failure`

Origine : Il n'y a pas suffisamment de mémoire pour exécuter `kadmin`.

Solution : Libérez de la mémoire et essayez d'exécuter `kadmin` à nouveau.

`kadmin: Bad encryption type while changing host/<FQDN>'s key`

Origine : Plusieurs types de chiffrement par défaut sont inclus dans la version de base de la version Solaris 10 8/07. Les clients peuvent demander des types de chiffrement qui ne sont peut-être pas pris en charge par un KDC exécuté sur une version antérieure du logiciel.

Solution : Plusieurs solutions existent pour résoudre ce problème. La plus facile à mettre en œuvre est donnée en premier :

1. Ajoutez les packages SUNWcry et SUNWcryr sur le serveur KDC. Ceci permet d'augmenter le nombre de types de chiffrement pris en charge par le KDC.

2. Définissez `permitted_enctypes` dans `krb5.conf` sur le client pour que le type de chiffrement `aes256` ne soit pas inclus. Cette étape doit être effectuée sur chaque nouveau client.

`KDC can't fulfill requested option`
Origine : Le KDC n'a pas autorisé l'option demandée. Il est possible que des options postdatables ou transmissibles soient demandées et que le KDC refuse. Un autre problème peut être une demande de renouvellement d'un TGT, sans avoir de TGT renouvelable.

Solution : Déterminez si vous demandez une option que le KDC n'autorise pas ou un type de ticket qui n'est pas disponible.

`KDC policy rejects request`
Origine : La stratégie du KDC n'a pas autorisé la demande. Par exemple, la demande au KDC n'a pas d'adresse IP. Ou une transmission a été demandée, mais le KDC ne l'a pas autorisée.

Solution : Assurez-vous que vous utilisez `kinit` avec les options appropriées. Si nécessaire, vous pouvez modifier la stratégie associée au principal ou modifier les attributs du principal afin d'autoriser la demande. Vous pouvez modifier la stratégie ou le principal en utilisant `kadmin`.

`KDC reply did not match expectation`
Origine : La réponse du KDC ne contient pas le nom de principal attendu ou d'autres valeurs dans la réponse n'étaient pas correctes.

Solution : Assurez-vous que le KDC avec lequel vous communiquez est conforme à RFC4120, que la demande envoyée est une demande Kerberos V5, ou que le KDC est disponible.

`kdestroy: Could not obtain principal name from cache`
Origine : Le cache d'informations d'identification est manquant ou endommagé.

Solution : Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via `kinit`, si nécessaire.

`kdestroy: No credentials cache file found while destroying cache`
Origine : Le cache d'informations d'identification (`/tmp/krb5c_` *uid*) est manquant ou endommagé.

Solution : Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via `kinit`, si nécessaire.

`kdestroy: TGT expire warning NOT deleted`
Origine : Le cache d'informations d'identification est manquant ou endommagé.

Solution : Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via `kinit`, si nécessaire.

`Kerberos authentication failed`
Origine : Le mot de passe Kerberos est incorrect ou ne peut pas être synchronisé avec le mot de passe UNIX.

Solution : Si les mots de passe ne sont pas synchronisés, vous devez spécifier un mot de passe différent pour terminer l'authentification Kerberos. Il est possible que l'utilisateur ait oublié son mot de passe d'origine.

`Kerberos V5 refuses authentication`
Origine : L'authentification n'a pas pu être négociée avec le serveur.

Solution : Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle authdebug` et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

`Key table entry not found`
Origine : Il n'existe aucune entrée pour le principal de service dans le fichier keytab du serveur d'application réseau.

Solution : Ajouter le principal de service approprié au fichier keytab du serveur afin de pouvoir fournir le service utilisant Kerberos.

`Key version number for principal in key table is incorrect`
Origine : La version de clé d'un principal dans le fichier keytab est différente de la version dans la base de données Kerberos. Soit la clé d'un service a été modifiée, soit vous utilisez un ancien ticket de service.

Solution : Si la clé d'un service a été modifiée (par exemple, en utilisant `kadmin`), vous devez extraire la nouvelle clé et la stocker dans le fichier keytab de l'hôte où le service est en cours d'exécution.

Sinon, vous utilisez peut-être un ancien ticket de service qui a une ancienne clé. Vous aurez peut-être besoin d'exécuter la commande `kdestroy` , puis la commande `kinit` à nouveau.

`kinit: gethostname failed`
Origine : Une erreur dans la configuration réseau local provoque l'échec de `kinit`.

Solution : Assurez-vous que l'hôte est correctement configuré.

`login: load_modules: can not open module /usr/lib/security/pam_krb5.so.1`
Origine : Le module PAM de Kerberos est manquant ou il ne s'agit pas d'un binaire exécutable valide.

Solution : Assurez-vous que le module PAM de Kerberos est dans les `/usr/lib/security` Directory et qu'il s'agit d'un fichier exécutable valide binaire. Assurez-vous également que le `/etc/pam.conf` contient le chemin d'accès correct à `pam_krb5.so.1`.

`Looping detected inside krb5_get_in_tkt`
Origine : Kerberos a tenté à plusieurs reprises d'obtenir les tickets initiaux mais n'a pas réussi.

Solution : Assurez-vous qu'au moins un KDC répond aux demandes d'authentification.

`Master key does not match database`
Origine : Le vidage de base de données chargé n'a pas été créé à partir d'une base de données qui contient la clé principale. La clé principale est située dans `/var/krb5/.k5.`*REALM*.

Solution : Assurez-vous que la clé principale dans le vidage de base de données chargé correspond à la clé principale qui se trouve dans `/var/krb5/.k5.`*REALM*.

`Matching credential not found`
Origine : Les informations d'identification correspondant à votre demande n'ont pas été trouvées. Votre demande exige l'utilisation d'informations d'authentification qui ne sont pas disponibles dans le cache d'informations d'identification.

Solution : Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.

`Message out of order`
Origine : Les messages qui ont été envoyés à l'aide d'une confidentialité à ordre séquentielle ont été livrés sans tenir compte de l'ordre. Certains messages ont peut-être été perdus dans le processus.

Solution : Vous devez réinitialiser la session Kerberos.

`Message stream modified`
Origine : Un conflit est survenu entre la somme de contrôle calculée et la somme de contrôle du message. Le message a peut-être été modifié pendant la transmission, ce qui peut indiquer un problème de sécurité.

Solution : Assurez-vous que les messages sont envoyés sur le réseau correctement. Étant donné que ce message peut également indiquer la possible altération des messages pendant qu'ils sont en cours d'envoi, détruisez vos tickets à l'aide de `kdestroy` et réinitialisez les services Kerberos que vous êtes en train d'utiliser.

Messages d'erreur Kerberos courants (N-Z)

Cette section fournit une liste alphabétique (N-Z) des messages d'erreur courants pour les commandes Kerberos, les démons Kerberos, la structure PAM, l'interface GSS, le service NFS et la bibliothèque Kerberos.

`No credentials cache file found`
Origine : Kerberos n'a pas trouvé le cache d'informations d'identification (`/tmp/krb5cc_`*uid*).

Solution : Assurez-vous que le fichier d'informations d'identification existe et qu'il est lisible. Si ce n'est pas le cas, essayez d'exécuter `kinit` une nouvelle fois.

`No credentials were supplied, or the credentials were unavailable or inaccessible`

`No credential cache found`

Origine : Le cache d'informations d'identification de l'utilisateur est incorrect ou n'existe pas.

Solution : L'utilisateur doit exécuter `kinit` avant d'essayer de démarrer le service.

`No credentials were supplied, or the credentials were unavailable or inaccessible`

`No principal in keytab matches desired name`

Origine : Une erreur s'est produite lors de la tentative d'authentification du serveur.

Solution : Assurez-vous que l'hôte ou le principal de service est dans le fichier keytab du serveur.

`Operation requires "`*privilege*`" privilege`

Origine : Le principal `admin` qui était en cours d'utilisation n'a pas les privilèges appropriés configurés dans le fichier `kadm5.acl`.

Solution : Utilisez une identité qui dispose des privilèges appropriés. Vous pouvez également configurer le principal qui a été utilisé afin qu'il dispose des privilèges appropriés en modifiant le fichier `kadm5.acl`. Généralement, un principal contenant `/admin` dans son nom est doté des privilèges appropriés.

`PAM-KRB5 (auth): krb5_verify_init_creds failed: Key table entry not found`

Origine : L'application distante a tenté de lire le principal de service de l'hôte dans le fichier `/etc/krb5/krb5.keytab` local, fichier, mais il n'existe pas.

Solution : Ajoutez le principal de service de l'hôte au fichier keytab du serveur.

`Password is in the password dictionary`

Origine : Le mot de passe que vous avez spécifié se trouve dans un dictionnaire de mots de passe en cours d'utilisation. Votre mot de passe n'est pas un bon choix.

Solution : Choisissez un mot de passe qui mélange plusieurs classes de mot de passe.

`Permission denied in replay cache code`

Origine : Le cache de rediffusion du système n'a pas pu être ouvert. Votre serveur peut avoir été exécuté pour la première fois sous un ID utilisateur différent de votre ID d'utilisateur actuel.

Solution : Assurez-vous que le cache de rediffusion possède les autorisations appropriées. Le cache de rediffusion est stocké sur l'hôte sur lequel l'application de serveur utilisant Kerberos est en cours d'exécution. Le fichier du cache de rediffusion est appelé `/var/krb5/rcache/rc_`*service_name_ uid* pour les utilisateurs non-`root`. Pour les utilisateurs root le fichier du cache de rediffusion est appelé `/var/krb5/rcache/root/rc_`*service_name*.

`Protocol version mismatch`
Origine : Une demande Kerberos V4 a probablement été envoyée au KDC. Le service Kerberos ne prend en charge que le protocole Kerberos V5.

Solution : Assurez-vous que vos applications utilisent le protocole Kerberos V5.

`Request is a replay`
Origine : La requête a déjà été envoyée à ce serveur et traitée. Les tickets ont peut-être été volés et quelqu'un d'autre essaie de les réutiliser.

Solution : Attendez quelques minutes et relancez la demande.

`Requested principal and ticket don't match`
Origine : Le principal de service auquel vous vous connectez et le ticket de service que vous avez ne correspondent pas.

Solution : Assurez-vous que le service DNS fonctionne correctement. Si vous utilisez un logiciel d'un autre fabricant, assurez-vous qu'il utilise correctement les noms de principaux.

`Requested protocol version not supported`
Origine : Une demande Kerberos V4 a probablement été envoyée au KDC. Le service Kerberos ne prend en charge que le protocole Kerberos V5.

Solution : Assurez-vous que vos applications utilisent le protocole Kerberos V5.

`Server refused to negotiate authentication, which is required for encryption. Good bye.`
Origine : L'application distante n'est pas capable ou a été configuré de manière à ne pas accepter l'authentification Kerberos du client.

Solution : Fournissez une application distante qui peut négocier l'authentification ou configurez l'application pour qu'elle utilise les indicateurs appropriés pour activer l'authentification.

`Server refused to negotiate encryption. Good bye.`
Origine : Le chiffrement n'a pas pu être négocié avec le serveur.

Solution : Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle encdebug` et consultez les messages de débogage pour en savoir plus.

`Server rejected authentication (during sendauth exchange)`

Origine : Le serveur avec lequel vous tentez de communiquer a rejeté l'authentification. La plupart du temps, cette erreur se produit pendant la propagation de base de données kerberos. Certaines causes courantes peuvent être des problèmes avec le fichier `kpropd.acl`, DNS ou le fichier keytab.

Solution : Si vous recevez ce message d'erreur lorsque vous exécutez des applications autres que `kprop`, cherchez à savoir si le fichier keytab du serveur est correct.

`The ticket isn't for us`

`Ticket/authenticator don't match`

Origine : Un conflit est survenu entre le ticket et l'authentificateur. Le nom du principal de la demande peut ne pas correspondre au nom du principal de service. Soit le ticket a été envoyé avec un FQDN du principal alors que le service attendait un autre nom, soit le service attendait un FQDN et a reçu un autre nom.

Solution : Si vous recevez ce message d'erreur lorsque vous exécutez des applications autres que `kprop`, cherchez à savoir si le fichier keytab du serveur est correct.

`Ticket expired`

Origine : Votre ticket a expiré.

Solution : Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.

`Ticket is ineligible for postdating`

Origine : Le principal n'autorise pas ses tickets à être postdatés.

Solution : Modifier le principal avec `kadmin` pour l'autoriser.

`Ticket not yet valid`

Origine : Le ticket postdaté n'est pas encore valide.

Solution : Créez un nouveau ticket avec la date correcte ou attendez que le ticket actuel soit valide.

`Truncated input file detected`

Origine : La fichier de vidage de base de données qui a été utilisé dans l'opération n'est pas un fichier de vidage complet.

Solution : Recréez le fichier de vidage ou utilisez-en un autre.

`Unable to securely authenticate user ... exit`

Origine : L'authentification n'a pas pu être négociée avec le serveur.

Solution : Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle authdebug` et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

`Wrong principal in request`
Origine : Le ticket contenait un nom de principal non valide. Cette erreur peut indiquer un problème de DNS ou de FQDN.

Solution : Assurez-vous que le principal du service correspond au principal du ticket.

Dépannage de Kerberos

Cette section fournit des informations de dépannage pour le logiciel Kerberos.

Problèmes avec le format du fichier `krb5.conf`

Si le fichier `krb5.conf` n'est pas formaté correctement, le message d'erreur suivant peut être affiché sur le terminal ou dans le fichier journal :

```
Improper format of Kerberos configuration file while initializing krb5 library
```

S'il y a un problème avec le format du fichier `krb5.conf`, les services associés sont vulnérables aux attaques. Vous devez résoudre le problème avant d'autoriser l'utilisation des fonctions de Kerberos.

Problèmes de propagation de la base de données Kerberos

Si la propagation de base de données Kerberos échoue, essayez `/usr/bin/rlogin -x` entre le KDC esclave et le KDC maître, et depuis le KDC maître vers le serveur KDC esclave.

Si les KDC ont été configurés de façon à restreindre l'accès, `rlogin` est désactivé et ne peut pas être utilisé pour résoudre ce problème. Pour activer `rlogin` sur un KDC, vous devez activer le service `eklogin`.

```
# svcadm enable svc:/network/login:eklogin
```

Une fois que vous avez résolu le problème, vous devez désactiver le service `eklogin`.

Si `rlogin` ne fonctionne pas, les problèmes proviennent probablement des fichiers keytab des KDC. Si `rlogin` ne fonctionne pas, le problème ne provient pas du fichier keytab ou du service de noms, car `rlogin` et le logiciel de propagation utilisent le même principal `host/` *host-name*. Dans ce cas, assurez-vous que le fichier `kpropd.acl` est correct.

Problèmes de montage d'un système de fichiers NFS utilisant Kerberos

- Si un montage de système de fichiers NFS utilisant Kerberos échoue, assurez-vous que le fichier `/var/rcache/root` existe sur le serveur NFS. Si le système de fichiers n'est pas détenu par `root`, supprimez-le et essayez de le monter une nouvelle fois.
- Si vous avez un problème d'accès à un système de fichiers NFS utilisant Kerberos, assurez-vous que le service `gssd` est activé sur votre système et le serveur NFS.
- Si vous voyez le message d'erreur `invalid argument` ou `bad directory` lorsque vous tentez d'accéder à un système de fichiers NFS utilisant Kerberos, le problème est peut-être que vous n'utilisez pas un nom DNS complet lorsque vous essayez de monter le système de fichiers NFS. L'hôte qui est en cours de montage n'est pas le même que le composant du nom de l'hôte du principal de service dans le fichier keytab du serveur.

  Ce problème peut également se produire si votre serveur dispose de plusieurs interfaces Ethernet, et que vous avez configuré DNS pour qu'il utilise un plan de type "nom par interface" au lieu de "plusieurs enregistrements d'adresses par hôte". Pour le service Kerberos, vous devez configurer plusieurs enregistrements d'adresses par hôte comme suit [1] :

```
my.host.name.   A       1.2.3.4
                A       1.2.4.4
                A       1.2.5.4

my-en0.host.name.       A       1.2.3.4
my-en1.host.name.       A       1.2.4.4
my-en2.host.name.       A       1.2.5.4

4.3.2.1         PTR     my.host.name.
4.4.2.1         PTR     my.host.name.
4.5.2.1         PTR     my.host.name.
```

Dans cet exemple, la configuration autorise une référence pour les différentes interfaces et un seul principal de service au lieu de trois principaux de service dans le fichier keytab du serveur.

Problèmes d'authentification en tant que `root`

En cas d'échec de l'authentification lorsque vous essayez de vous connecter en tant que superutilisateur sur votre système et que vous avez déjà ajouté le principal `root` au fichier keytab de votre hôte, il y a deux problèmes potentiels à vérifier. Tout d'abord, assurez-vous que le principal `root` dans le fichier keytab a un nom d'hôte complet comme instance. Si c'est le cas, vérifiez le fichier `/etc/resolv.conf` pour vous assurer que le système est correctement configuré en tant que client DNS.

[1] Ken Hornstein, "FAQ Kerberos," [http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#kerbdns], consulté le 10 mars 2010.

Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX

Pour être en mesure de contrôler les correspondances d'informations d'identification, commencez par décommenter cette ligne du fichier `/etc/gss/gsscred.conf`.

```
SYSLOG_UID_MAPPING=yes
```

Ensuite demandez au service `gssd` d'obtenir des informations depuis le fichier `/etc/gss/gsscred.conf`.

```
# pkill -HUP gssd
```

Maintenant, vous devez être en mesure de contrôler les mappages d'informations d'identification quand `gssd` les demande. Les mappages sont enregistrés par `syslogd`, si le fichier `syslog.conf` est configuré pour l'utilitaire système `auth` avec le niveau de gravité `debug`.

◆ ◆ ◆ CHAPITRE 25

Administration des principaux et des stratégies Kerberos (tâches)

Ce chapitre décrit les procédures d'administration des principaux et des stratégies qui leur sont associées. Ce chapitre indique également comment administrer un fichier keytab d'hôte.

Ce chapitre est destiné à tous ceux qui ont besoin d'administrer des principaux et des stratégies. Avant d'utiliser ce chapitre, vous devez vous familiariser avec les principaux et les stratégies, y compris les considérations de planification. Reportez-vous au Chapitre 21, “Introduction au service Kerberos” et au Chapitre 22, “Planification du service Kerberos”, respectivement.

La liste suivante répertorie les informations disponibles dans le présent chapitre :

Méthodes d'administration des principaux et des stratégies Kerberos

La base de données Kerberos sur le KDC maître contient tous les principaux Kerberos du domaine, leurs mots de passe, les stratégies et d'autres informations administratives. Pour créer et supprimer des principaux et pour modifier leurs attributs, vous pouvez utiliser les commandes `kadmin` ou `gkadmin`.

La commande `kadmin` fournit une interface de ligne de commande interactive qui permet de mettre à jour les principaux, les stratégies et les fichiers keytab de Kerberos. Il existe deux versions de la commande `kadmin` :

- `kadmin` : utilise l'authentification Kerberos pour fonctionner en toute sécurité de n'importe où sur le réseau .
- `kadmin.local` : doit être exécutée directement sur le KDC maître

Outre le fait que `kadmin` utilise Kerberos pour authentifier l'utilisateur, les capacités de ces deux versions sont identiques. La version locale est nécessaire pour vous permettre de configurer suffisamment de la base de données pour pouvoir utiliser la version distante.

De plus, la version Oracle Solaris fournit l'outil SEAM, `gkadmin`, une interface graphique interactive, qui propose globalement les mêmes possibilités que la commande `kadmin`. Pour plus d'informations, reportez-vous à la section “Outil SEAM ” à la page 514.

Outil SEAM

L'outil SEAM (gkadmin) est une interface graphique interactive qui permet de mettre à jour les principaux et les stratégies de Kerberos. Cet outil fournit globalement les mêmes fonctions que la commande `kadmin`. Toutefois, il ne prend pas en charge la gestion des fichiers keytab. Vous devez utiliser la commande `kadmin` pour gérer les fichiers keytab, ce qui est décrit dans “Administration des fichiers keytab” à la page 546.

Similaire à la commande `kadmin`, l'Outil SEAM utilise l'authentification Kerberos et le RPC chiffré pour fonctionner en toute sécurité de n'importe où sur le réseau. L'Outil SEAM permet d'effectuer les opérations suivantes :

- Créer des principaux basés sur les valeurs par défaut ou des principaux existants.
- Créer des stratégies basées sur des stratégies existantes.
- Ajouter des commentaires pour les principaux.
- Définir des valeurs par défaut pour la création de principaux.
- Se connecter en tant qu'un autre principal sans quitter l'outil.
- Imprimer ou enregistrer des listes de principaux et des listes de stratégies.
- Afficher ou rechercher des listes de principaux et des listes de stratégies.

L'Outil SEAM fournit également une aide contextuelle et une aide en ligne générale.

La liste des tâches suivante fournit des indications sur les différentes tâches réalisables avec l'Outil SEAM :

- “Gestion des principaux de Kerberos (liste des tâches)” à la page 518
- “Administration des stratégies Kerberos (liste des tâches)” à la page 532

En outre, reportez-vous à la section “Descriptions des panneaux de l'Outil SEAM ” à la page 541 pour obtenir les descriptions de tous les attributs de principaux et de stratégies que vous pouvez spécifier ou afficher dans l'outil SEAM.

Équivalents de ligne de commande de l'Outil SEAM

Cette section répertorie les commandes `kadmin` qui fournissent les mêmes fonctionnalités que l'Outil SEAM . Ces commandes peuvent être utilisées sans exécuter un système X Window System. Même si la plupart des procédures de ce chapitre utilisent l'Outil SEAM , plusieurs procédures fournissent également des exemples qui utilisent les équivalents de ligne de commande.

TABLEAU 25–1 Équivalents de ligne de commande de l'Outil SEAM

Procédure de l'outil SEAM	Équivalent de la commande `kadmin`
Affichage de la liste de principaux.	`list_principals` ou `get_principals`
Affichage des attributs d'un principal.	`get_principal`
Création d'un principal.	`add_principal`
Duplication d'un principal.	Pas d'équivalent de ligne de commande
Modification d'un principal.	`modify_principal` ou `change_password`
Suppression d'un principal.	`delete_principal`
Définition des valeurs par défaut pour la création de principaux.	Pas d'équivalent de ligne de commande
Affichage de la liste des stratégies.	`list_policies` ou `get_policies`
Affichage des attributs d'une stratégie.	`get_policy`
Création d'une stratégie.	`add_policy`
Duplication d'une stratégie.	Pas d'équivalent de ligne de commande
Modification d'une stratégie.	`modify_policy`
Suppression d'une stratégie.	`delete_policy`

Seul fichier modifié par l'Outil SEAM

Le seul fichier modifié par l'Outil SEAM est le fichier `$HOME/.gkadmin` . Ce fichier contient les valeurs par défaut pour la création de principaux. Vous pouvez mettre à jour ce fichier en choisissant Properties (Propriétés) dans le menu Edit (Édition).

Fonctions d'impression et d'aide en ligne de l'Outil SEAM

L'Outil SEAM fournit des fonctions d'impression et d'aide en ligne. Depuis le menu Print (Imprimer), vous pouvez envoyer les éléments suivants vers une imprimante ou un fichier :

- liste des principaux disponibles sur le KDC maître spécifié ;
- liste des stratégies disponibles sur le KDC maître spécifié ;
- principal actuellement sélectionné ou chargé.
- La stratégie actuellement sélectionnée ou chargée.

Dans le menu d'aide, vous pouvez accéder à l'aide contextuelle et à l'aide générale. Lorsque vous choisissez l'option d'aide contextuelle dans le menu d'aide, la fenêtre d'aide contextuelle s'affiche et l'outil passe en mode d'aide. En mode d'aide, lorsque vous cliquez sur les champs, les étiquettes ou les boutons de la fenêtre, l'aide de ces éléments est affichée dans la fenêtre d'aide. Pour revenir au mode normal, cliquez sur Dismiss (Fermer) dans la fenêtre d'aide.

Vous pouvez également utiliser le sommaire de l'aide, qui s'ouvre dans un navigateur HTML et fournit des indications sur la présentation générale et les informations sur les tâches de ce chapitre.

Utilisation de grandes listes dans l'Outil SEAM

Quand votre site commence à accumuler un grand nombre de principaux et de stratégies, le temps qu'il faut à l'outil SEAM pour charger et afficher les listes de principaux et de stratégies s'allonge. Par conséquent, votre productivité avec l'outil baisse. Il existe plusieurs façons de remédier à ce problème.

Tout d'abord, vous pouvez éliminer totalement le temps de chargement des listes en empêchant l'outil SEAM de les charger. Pour définir cette option, choisissez Properties dans le menu Edit, puis désactivez l'option Show Lists (Afficher les listes). Bien entendu, lorsque l'outil ne charge pas les listes, il ne peut pas les afficher et vous ne pouvez plus utiliser les panneaux de listes pour sélectionner des principaux et des stratégies. Au lieu de cela, vous devez saisir un nom de principal ou de stratégie dans le nouveau champ de nom qui est fourni, puis sélectionner l'opération que vous souhaitez effectuer. Dans les faits, la saisie d'un nom est équivalente à la sélection d'un élément dans la liste.

Une autre façon de travailler avec de grandes listes est de les mettre en cache. En fait, la mise en cache des listes pour une période limitée est définie comme le comportement par défaut pour l'outil SEAM. L'outil SEAM doit toujours initialement charger les listes dans le cache. Mais après cela, l'outil peut utiliser le cache plutôt que d'extraire les listes à nouveau. Cette option supprime la nécessité de continuer à charger les listes à partir du serveur, ce qui est très long.

Vous pouvez paramétrer la mise en cache de listes en sélectionnant Properties dans le menu Edit. Il existe deux paramètres de mise en cache. Vous pouvez choisir de mettre en cache la liste indéfiniment ou de spécifier une limite dans le temps lorsque l'outil doit recharger les listes à partir du serveur dans le cache.

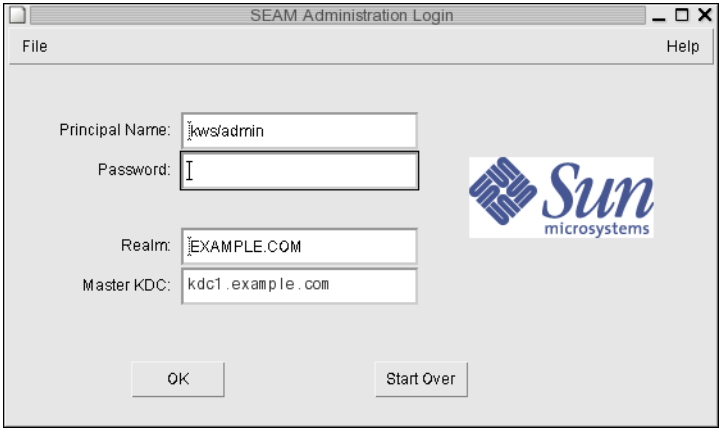
La mise en cache des listes vous permet toujours d'utiliser les panneaux de listes pour sélectionner des principaux et des stratégies, de sorte qu'il n'y a pas d'incidence sur la manière dont vous utilisez l'Outil SEAM comme avec la première option. En outre, même si la mise cache ne vous permet pas de voir les modifications d'autres utilisateurs, vous pouvez toujours voir les dernières informations relatives à la liste en fonction de vos modifications, car celles-ci mettent à jour les listes sur le serveur et dans le cache. Et, si vous souhaitez mettre à jour le cache pour voir d'autres modifications et récupérer la dernière copie des listes, vous pouvez utiliser le menu Refresh (Actualiser) chaque fois que vous le souhaitez pour actualiser le cache depuis le serveur.

▼ Procédure de démarrage de l'Outil SEAM

1 **Démarrez l'Outil SEAM en utilisant la commande `gkadmin`.**

```
$ /usr/sbin/gkadmin
```

La fenêtre de connexion d'administration SEAM s'affiche.



2 **Si vous ne souhaitez pas utiliser les valeurs par défaut, spécifiez de nouvelles valeurs par défaut.**

La fenêtre est automatiquement renseignée avec des valeurs par défaut. Le nom de principal par défaut est déterminé en prenant votre identité en cours à partir de la variable d'environnement `USER` et en lui ajoutant `/admin` (*username* `/admin`). Les champs de domaine et de KDC maître par défaut sont sélectionnés à partir du fichier `/etc/krb5/krb5.conf`. Si vous souhaitez récupérer les valeurs par défaut, cliquez sur Start Over.

Remarque – Les opérations d'administration que chaque nom de principal peut effectuer sont déterminées par le fichier ACL Kerberos, `/etc/krb5/kadm5.acl` . Pour plus d'informations sur les privilèges limités, reportez-vous à la section "Utilisation de l'Outil SEAM avec privilèges d'administration Kerberos limités" à la page 544.

3 **Saisissez un mot de passe pour le nom de principal spécifié.**

4 **Cliquez sur OK.**

Une fenêtre contenant tous les principaux s'affiche.

Gestion des principaux de Kerberos

Cette section fournit des instructions détaillées permettant d'administrer les principaux à l'aide de l'Outil SEAM . Elle fournit également des exemples d'équivalents de lignes de commande, le cas échéant.

Gestion des principaux de Kerberos (liste des tâches)

Tâche	Description	Voir
Affichage de la liste de principaux.	Affichez la liste des principaux en cliquant sur l'onglet Principals (Principaux).	"Affichage de la liste des principaux Kerberos" à la page 520
Affichage des attributs d'un principal.	Affichez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier).	"Affichage des attributs d'un principal Kerberos " à la page 522
Création d'un principal.	Créez un principal en cliquant sur le bouton Create New (Créer) dans le panneau Principal List (Liste de principaux).	"Création d'un principal Kerberos" à la page 524
Duplication d'un principal.	Dupliquez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Duplicate (Dupliquer).	"Duplication d'un principal Kerberos" à la page 527
Modification d'un principal.	Modifiez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify. Notez que vous ne pouvez pas modifier le nom d'un principal. Pour renommer un principal, vous devez le dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancien principal.	"Modification d'un principal Kerberos" à la page 528

Tâche	Description	Voir
Suppression d'un principal.	Supprimez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Delete (Supprimer).	"Suppression d'un principal Kerberos " à la page 529
Définition des valeurs par défaut pour la création de principaux.	Définissez des valeurs par défaut pour la création de principaux en sélectionnant Properties dans le menu Edit.	"Paramétrage des valeurs par défaut pour la création de principaux Kerberos" à la page 529
Modification des privilèges d'administration Kerberos (fichier `kadm5.acl`).	*Ligne de commande uniquement.* Les privilèges d'administration Kerberos déterminent quelles opérations un principal peut effectuer sur la base de données Kerberos, comme l'ajout et la modification. Vous devez modifier le fichier `/etc/krb5/kadm5.acl` pour modifier les privilèges d'administration Kerberos pour chaque principal.	"Modification des privilèges d'administration Kerberos" à la page 530

Automatisation de la création de principaux Kerberos

Même si l'Outil SEAM offre une certaine facilité d'utilisation, il ne propose pas de moyen d'automatiser la création de principaux. L'automatisation est particulièrement utile si vous avez besoin d'ajouter 10 ou même 100 nouveaux principaux dans un court laps de temps. Toutefois, en utilisant la commande `kadmin.local` dans un script Bourne shell, vous pouvez le faire.

La ligne de script shell suivante illustre une manière d'automatiser la création de nouveaux principaux :

```
awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |
        time /usr/sbin/kadmin.local> /dev/null
```

Cet exemple est réparti sur deux lignes pour une meilleure lisibilité. Le script lit un fichier appelé `princnames` contenant les noms de principaux et leurs mots de passe, et les ajoute à la base de données Kerberos. Vous devez créer le fichier `princnames` contenant un nom de principal et son mot de passe sur chaque ligne, séparés par un ou plusieurs espaces. L'option `+needchange` configure le principal afin que l'utilisateur soit invité à saisir un nouveau mot de passe lors de la première connexion avec le principal. Cette pratique permet de s'assurer que les mots de passe dans le fichier `princnames` ne représentent pas un risque pour la sécurité.

Vous pouvez construire des scripts plus élaborés. Par exemple, le script peut utiliser les informations contenues dans le service de noms pour obtenir la liste des noms d'utilisateur pour les noms de principaux. Ce que vous faite et la manière dont vous le faites est déterminé par les besoins de votre site et votre expérience en script.

▼ Affichage de la liste des principaux Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

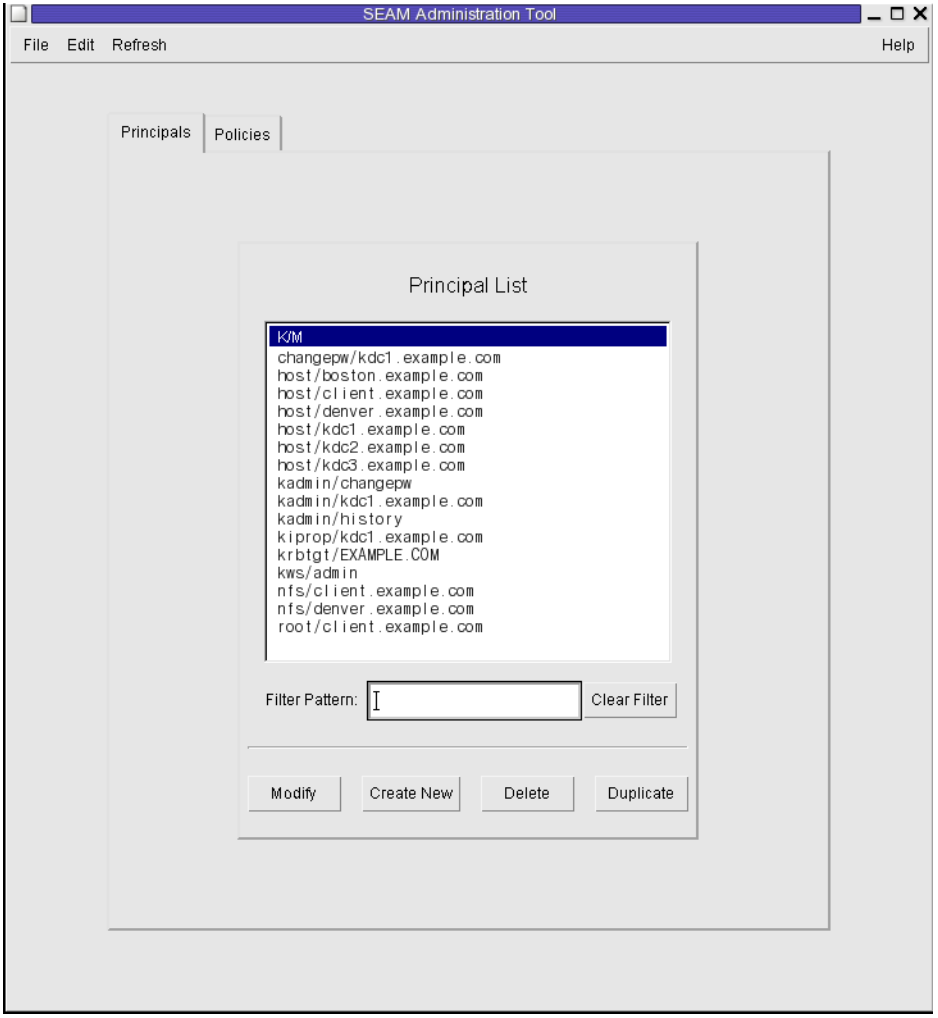
1 Si nécessaire, démarrez l'Outil SEAM .

Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

```
$ /usr/sbin/gkadmin
```

2 Cliquez sur l'onglet Principals (Principaux).

La liste de principaux s'affiche.



3 Affichez un principal spécifique ou une sous-liste de principaux.

Saisissez une chaîne dans le champs de filtre et appuyez sur la touche Entrée. Si le filtre fonctionne, la liste de principaux qui lui correspond s'affiche.

La chaîne du filtre doit être composée d'un ou plusieurs caractères. Notez bien que le mécanisme de filtrage respecte la casse et qu'il vous faut utiliser les majuscules et minuscules appropriées. Par exemple, si vous entrez la chaîne `ge`, le mécanisme de filtrage affiche uniquement les principaux contenant la chaîne `ge` (par exemple, `george` ou `edge`).

Si vous souhaitez afficher l'intégralité de la liste de principaux, cliquez sur Clear Filter (Supprimer le filtre).

Exemple 25–1 Affichage de la liste de principaux Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `list_principals` de `kadmin` est utilisée pour obtenir la liste de tous les principaux correspondant à `kadmin*`. Les caractères génériques peuvent être utilisés avec la commande `list_principals` .

```
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.con@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
kadmin: quit
```

▼ Affichage des attributs d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Principals (Principaux).**

3. **Sélectionnez le principal dans la liste que vous souhaitez afficher, puis cliquez sur Modify (Modifier).**

   Le panneau Principal Basics (Informations de base du principal) contenant certains attributs du principal s'affiche.

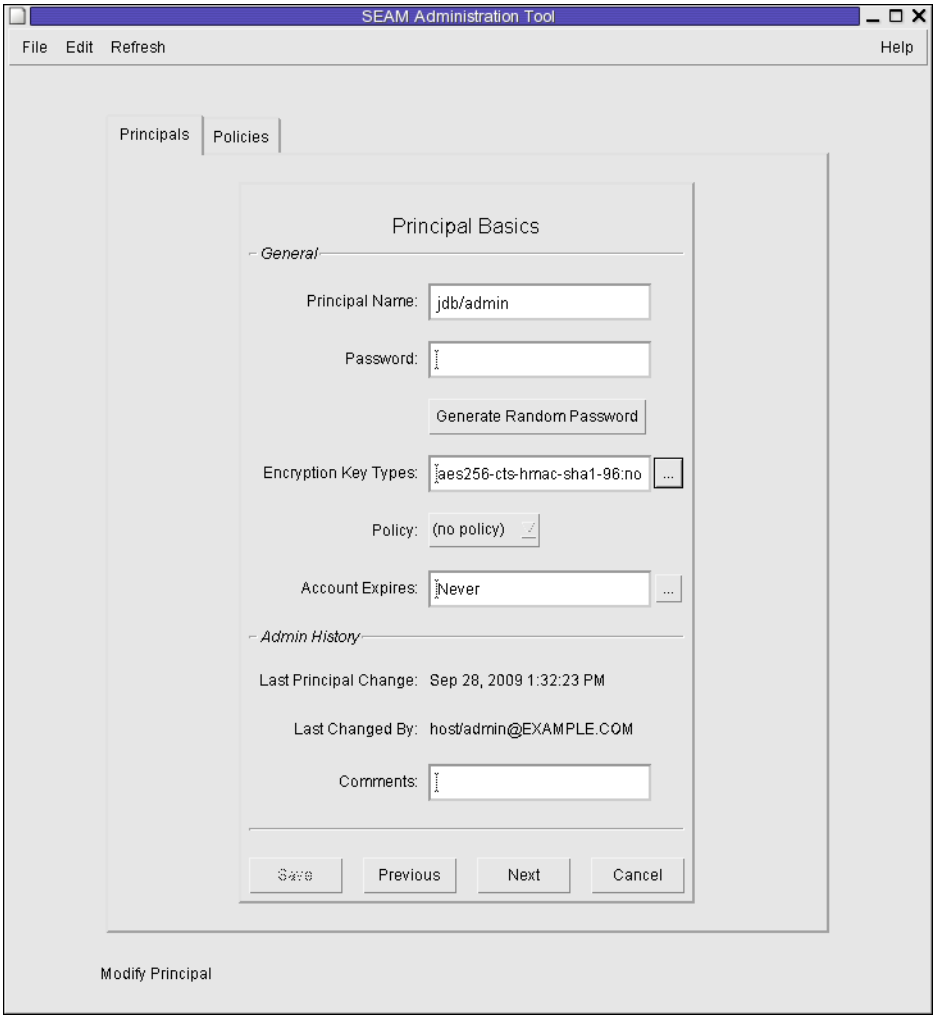
4. **Continuez à cliquer sur Next (Suivant) pour afficher tous les attributs du principal.**

   Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section “Descriptions des panneaux de l'Outil SEAM ” à la page 541.

5. **Lorsque vous avez fini de consulter ces informations, cliquez sur Cancel (Annuler).**

Exemple 25–2 Affichage des attributs d'un principal Kerberos

L'exemple suivant montre la première fenêtre lorsque vous visualisez le principal `jdb/admin`.



Exemple 25–3 Affichage des attributs d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `get_principal` de `kadmin` est utilisée pour afficher les attributs du principal `jdb/admin`.

```
kadmin: getprinc jdb/admin
Principal: jdb/admin@EXAMPLE.COM

Expiration date: [never]
Last password change: [never]

Password expiration date: Wed Apr 14 11:53:10 PDT 2011
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
```

```
Last modified: Mon Sep 28 13:32:23 PST 2009 (host/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 1
Key: vno 1, AES-256 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, AES-128 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, Triple DES with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

▼ Création d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1 Si nécessaire, démarrez l'Outil SEAM .

Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

Remarque – Si vous voulez créer un principal qui nécessite une nouvelle stratégie, vous devriez d'abord créer cette stratégie. Reportez-vous à la section “Création d'une stratégie Kerberos” à la page 537.

```
$ /usr/sbin/gkadmin
```

2 Cliquez sur l'onglet Principals (Principaux).

3 Cliquez sur New (Nouveau).

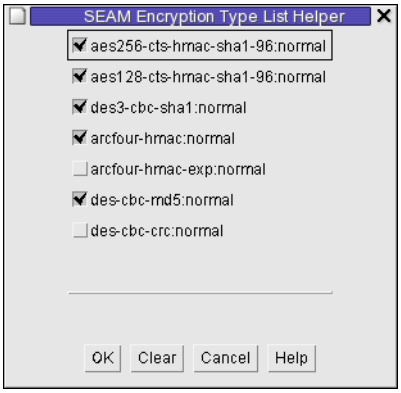
Le panneau Principal Basics contenant certains attributs du principal s'affiche.

4 Indiquez un nom de principal et un mot de passe.

Les deux sont obligatoires.

5 **Spécifiez les types de chiffrement pour le principal.**

Cliquez sur la boîte située à droite du champ de type de clé de chiffrement pour ouvrir une nouvelle fenêtre qui affiche l'ensemble des types de clés de chiffrement disponibles. Cliquez sur OK après avoir sélectionné les types de chiffrement requis.



6 **Spécifiez la stratégie pour le principal.**

7 **Spécifiez des valeurs pour les attributs du principal et continuez d'appuyer sur Next pour en spécifier d'autres.**

Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section "Descriptions des panneaux de l'Outil SEAM " à la page 541.

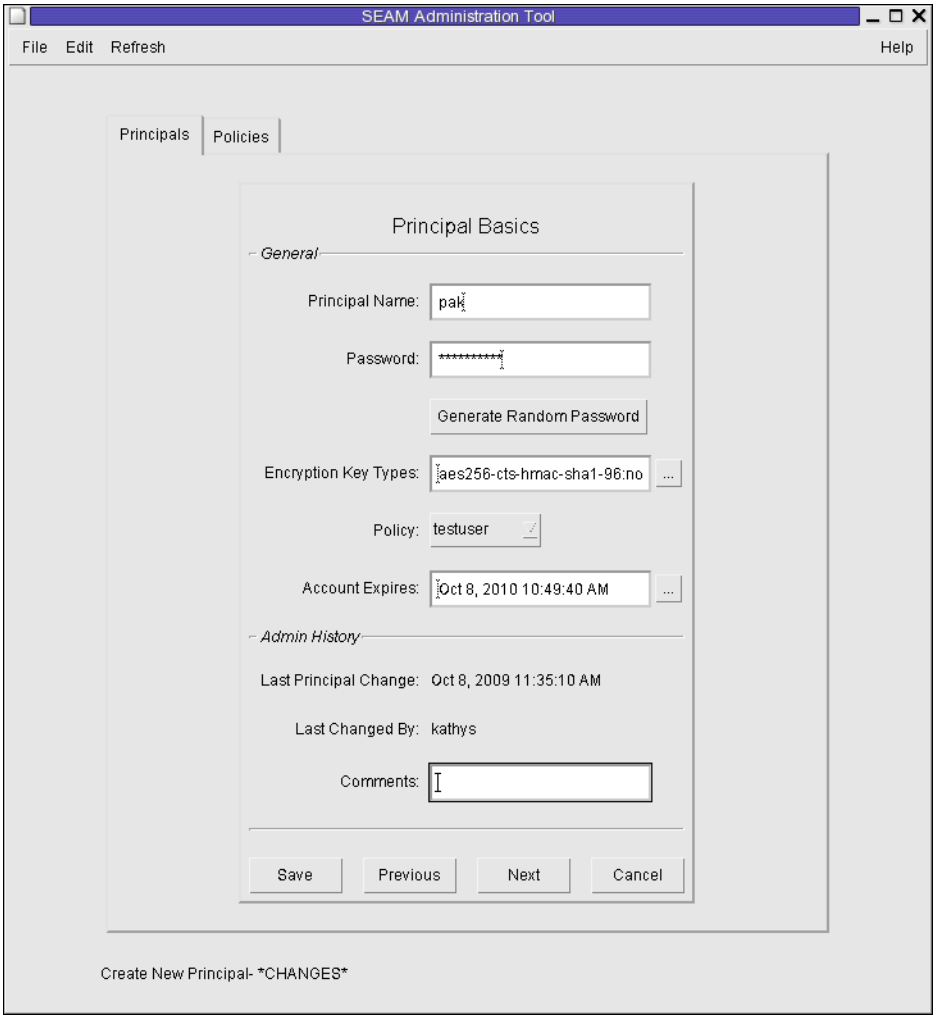
8 **Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.**

9 **Si nécessaire, configurez les privilèges d'administration de Kerberos pour le nouveau principal dans le fichier `/etc/krb5/kadm5.acl`.**

Pour plus d'informations, reportez-vous à la section "Modification des privilèges d'administration Kerberos" à la page 530.

Exemple 25–4 Création d'un principal Kerberos

L'exemple suivant montre le panneau Principal Basics lorsqu'un principal appelée `pak` est créé. La stratégie est définie sur `testuser`.



Exemple 25–5 Création d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `add_principal` de `kadmin` est utilisée pour créer un principal appelé `pak`. La stratégie du principal est définie sur `testuser`.

```
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": <Type the password>
Re-enter password for principal "pak@EXAMPLE.COM": <Type the password again>
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```

▼ Duplication d'un principal Kerberos

Cette procédure explique comment utiliser tout ou partie des attributs d'un principal existant pour en créer un nouveau. Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Principals (Principaux).**

3. **Sélectionnez le principal dans la liste que vous souhaitez dupliquer, puis cliquez sur Duplicate.**

   Le panneau Principal Basics s'affiche. Tous les attributs du principal sélectionné sont dupliqués, sauf les champs de nom et de mot de passe, qui sont vides.

4. **Indiquez un nom de principal et un mot de passe.**

   Les deux sont obligatoires. Pour effectuer une copie exacte du principal que vous avez sélectionné, cliquez sur Save et passez à l'Étape 7.

5. **Spécifiez des valeurs différentes pour les attributs du principal et continuez d'appuyer sur Next pour en spécifier d'autres.**

   Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section “Descriptions des panneaux de l'Outil SEAM ” à la page 541.

6. **Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.**

7. **Si nécessaire, configurez les privilèges d'administration de Kerberos pour le principal dans le fichier `/etc/krb5/kadm5.acl`.**

   Pour plus d'informations, reportez-vous à la section “Modification des privilèges d'administration Kerberos” à la page 530.

▼ Modification d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section "Procédure de démarrage de l'Outil SEAM " à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Principals (Principaux).**

3. **Sélectionnez le principal dans la liste que vous souhaitez modifier, puis cliquez sur Modify.**

   Le panneau Principal Basics contenant certains attributs du principal s'affiche.

4. **Modifiez les attributs du principal et continuez d'appuyer sur Next pour en modifier d'autres.**

   Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section "Descriptions des panneaux de l'Outil SEAM " à la page 541.

   Remarque – Vous ne pouvez pas modifier le nom d'un principal. Pour renommer un principal, vous devez le dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancien principal.

   ---

5. **Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.**

6. **Modifiez les privilèges d'administration Kerberos pour le principal dans le fichier `/etc/krb5/kadm5.acl`.**

   Pour plus d'informations, reportez-vous à la section "Modification des privilèges d'administration Kerberos" à la page 530.

Exemple 25–6 Modification du mot de passe d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `change_password` de `kadmin` est utilisée pour modifier le mot de passe du principal `jdb`. La commande `change_password` ne vous permet pas de réutiliser un mot de passe qui se trouve dans l'historique des mots de passe du principal.

```
kadmin: change_password jdb
Enter password for principal "jdb": <Type the new password>
Re-enter password for principal "jdb": <Type the password again>
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Pour modifier d'autres attributs d'un principal, vous devez utiliser la commande `modify_principal` de `kadmin`.

Suppression d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Principals (Principaux).**

3. **Sélectionnez le principal dans la liste que vous souhaitez supprimer, puis cliquez sur Delete.**

   Après avoir confirmé la suppression, le principal est supprimé.

4. **Supprimez le principal du fichier de liste de contrôle d'accès (ACL) de Kerberos, `/etc/krb5/kadm5.acl`.**

   Pour plus d'informations, reportez-vous à la section “Modification des privilèges d'administration Kerberos” à la page 530.

Exemple 25–7 Suppression d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `delete_principal` de `kadmin` est utilisée pour supprimer le principal `jdb`.

```
kadmin: delete_principal pak
Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): yes
Principal "pak@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
kadmin: quit
```

Paramétrage des valeurs par défaut pour la création de principaux Kerberos

Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

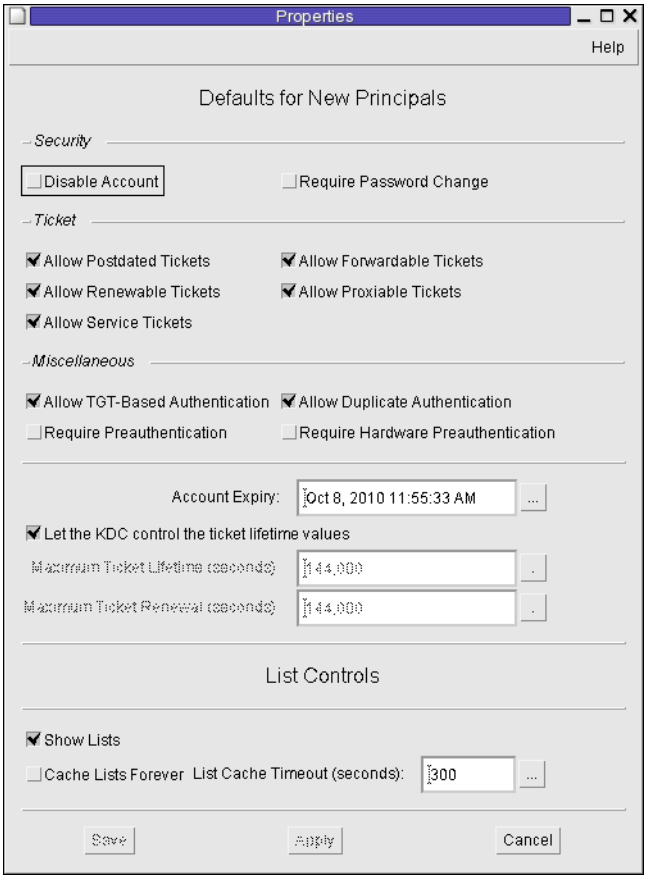
1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2 **Choisissez Properties (Propriétés) dans le menu Edit (Editer).**

La fenêtre Properties s'affiche.



3 **Sélectionnez les valeurs par défaut que vous souhaitez utiliser lorsque vous créez des principaux.**

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre.

4 **Cliquez sur Save (Enregistrer).**

▼ Modification des privilèges d'administration Kerberos

Même si votre site dispose probablement de nombreux principaux d'utilisateurs, en général, vous souhaitez que seul un petit nombre d'utilisateurs soit capable d'administrer la base de données Kerberos. Les privilèges d'administration de la base de données Kerberos sont

déterminés par le fichier ACL de Kerberos, `kadm5.acl`. Le fichier `kadm5.acl` vous permet d'autoriser ou d'interdire l'ajout de privilèges aux principaux individuels. Ou bien, vous pouvez utiliser le caractère générique « * » dans le nom du principal pour spécifier les privilèges pour les groupes de principaux.

1 Connectez-vous en tant que superutilisateur au KDC maître.

2 Modifiez le fichier `/etc/krb5/kadm5.acl` .

Une entrée dans le fichier `kadm5.acl` doit avoir le format suivant :

principal privileges [*principal-target*]

principal — Spécifie le principal auquel les privilèges sont accordés. N'importe quelle partie du nom du principal peut inclure le caractère générique « * », ce qui est utile pour fournir les mêmes privilèges pour un groupe de principaux. Par exemple, si vous voulez spécifier tous les principaux avec l'instance `admin` , vous devez utiliser `*/admin@` *realm*.

Notez qu'une utilisation commune d'une instance `admin` consiste à accorder des privilèges séparés (tels que l'accès à l'administration de la base de données Kerberos) à un principal Kerberos. Par exemple, l'utilisateur `jdb` peut avoir un principal pour son utilisation administrative, appelé `jdb/admin`. De cette façon, l'utilisateur `jdb` obtient les tickets de `jdb/admin` uniquement lorsqu'il a réellement besoin d'utiliser ces privilèges.

privileges — Spécifie les opérations qui peuvent être effectuées ou non par le principal. Ce champ est constitué d'une chaîne de caractères de la liste suivante de caractères ou de leur équivalent majuscule. Si le caractère est majuscule (ou non spécifié), alors l'opération n'est pas autorisée. Si le caractère est minuscule, l'opération est autorisée.

`a`	Autorise ou interdit l'ajout de principaux ou de stratégies.
`d`	Autorise ou interdit la suppression de principaux ou de stratégies.
`m`	Autorise ou interdit la modification de principaux ou de stratégies.
`c`	Autorise ou interdit la modification des mots de passe des principaux.
`i`	Autorise ou interdit la consultation de la base de données Kerberos.
`l`	Autorise ou interdit les liste de principaux ou de stratégies dans la base de données Kerberos.
`x` ou *	Autorise tous les privilèges (`admcil`).

principal-target — Lorsqu'un principal est indiqué dans ce champ, les *privilèges* s'appliquent au *principal* uniquement lorsque le *principal* fonctionne sur la *principal-target*. N'importe quelle partie du nom du principal peut inclure le caractère générique « * », ce qui est utile pour un groupe de principaux.

Exemple 25–8 Modification des privilèges d'administration de Kerberos

L'entrée suivante dans le fichier `kadm5.acl` accorde à tout principal dans le domaine `EXAMPLE.COM` avec l'instance `admin` tous les privilèges de la base de données Kerberos :

```
*/admin@EXAMPLE.COM *
```

L'entrée suivante dans le fichier `kadm5.acl` donne au principal `jdb@example.com` les privilèges d'ajouter, de répertorier et de consulter tous les principaux qui ont l'instance `root`.

```
jdb@EXAMPLE.COM ali */root@EXAMPLE.COM
```

Administration des stratégies Kerberos

Cette section fournit les instructions détaillées permettant d'administrer les stratégies à l'aide de l'Outil SEAM . Elle fournit également des exemples d'équivalents de lignes de commande, le cas échéant.

Administration des stratégies Kerberos (liste des tâches)

Tâche	Description	Voir
Affichage de la liste des stratégies.	Affichez la liste des stratégies en cliquant sur l'onglet Policies (Stratégies).	"Affichage de la liste des stratégies Kerberos" à la page 533
Affichage des attributs d'une stratégie.	Affichez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier).	"Affichage des attributs d'une stratégie Kerberos" à la page 535
Création d'une stratégie.	Créez une stratégie en cliquant sur le bouton Create New (Créer) dans le panneau Policy List (Liste de stratégies).	"Création d'une stratégie Kerberos" à la page 537
Duplication d'une stratégie.	Dupliquez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Duplicate (Dupliquer).	"Duplication d'une stratégie Kerberos" à la page 539
Modification d'une stratégie.	Modifiez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier). Notez que vous ne pouvez pas modifier le nom d'une stratégie. Pour renommer une stratégie, vous devez la dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancienne.	"Modification d'une stratégie Kerberos" à la page 539

Tâche	Description	Voir
Suppression d'une stratégie.	Supprimez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Delete (Supprimer).	"Suppression d'une stratégie Kerberos " à la page 540

▼ Affichage de la liste des stratégies Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

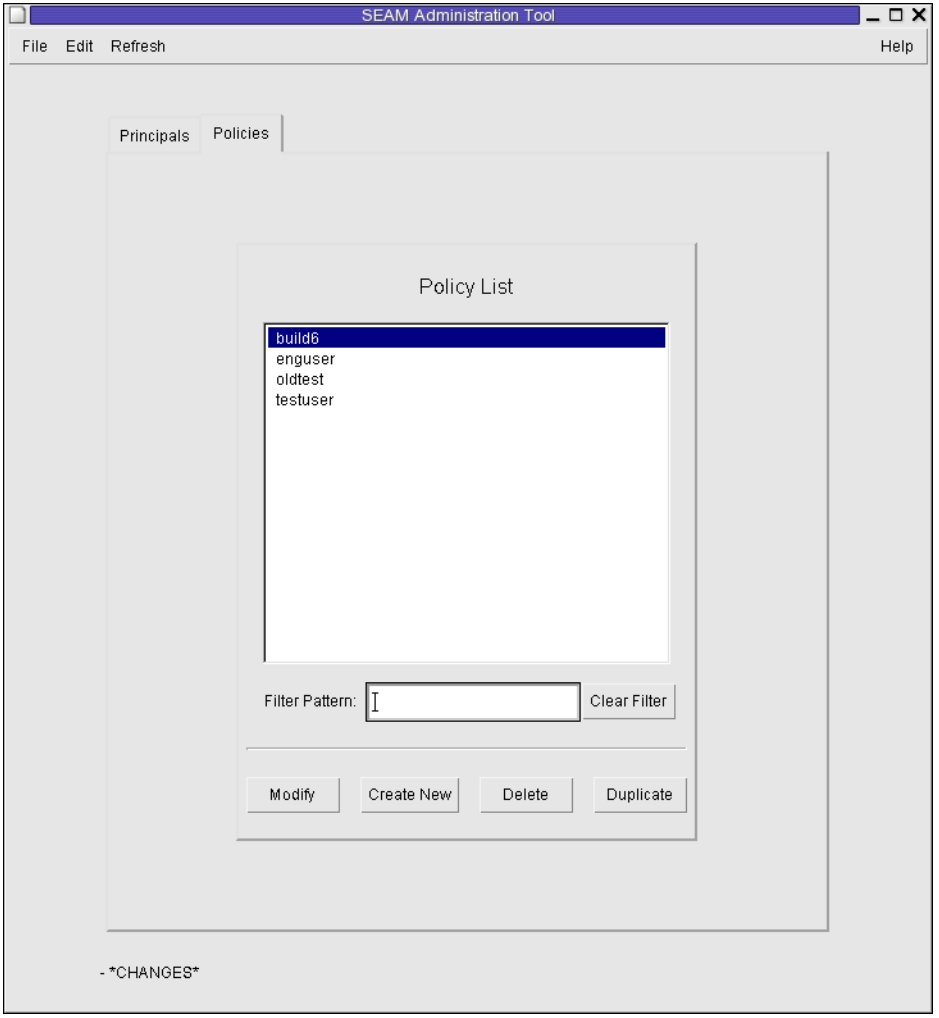
1 Si nécessaire, démarrez l'Outil SEAM .

Pour plus d'informations, reportez-vous à la section "Procédure de démarrage de l'Outil SEAM " à la page 517.

```
$ /usr/sbin/gkadmin
```

2 Cliquez sur l'onglet Policies (Stratégies).

La liste des stratégies s'affiche.



3 Affichez une stratégie spécifique ou une sous-liste de stratégies.

Saisissez une chaîne de filtrage dans le champ correspondant, puis appuyez sur la touche Entrée. Si le filtre fonctionne, la liste de stratégies qui lui correspond s'affiche.

La chaîne du filtre doit être composée d'un ou plusieurs caractères. Notez bien que le mécanisme de filtrage respecte la casse et qu'il vous faut utiliser les majuscules et minuscules appropriées. Par exemple, si vous entrez la chaîne `ge`, le mécanisme de filtrage affiche uniquement les stratégies contenant la chaîne `ge` (par exemple, `george` ou `edge`).

Si vous souhaitez afficher l'intégralité de la liste de stratégies, cliquez sur Clear Filter (Supprimer le filtre).

Exemple 25–9 Affichage de la liste de stratégies Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `list_policies` de `kadmin` est utilisée pour obtenir la liste de toutes les stratégies correspondant à `*user*`. Les caractères génériques peuvent être utilisés avec la commande `list_policies`.

```
kadmin: list_policies *user*
testuser
enguser
kadmin: quit
```

▼ Affichage des attributs d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Policies (Stratégies).**

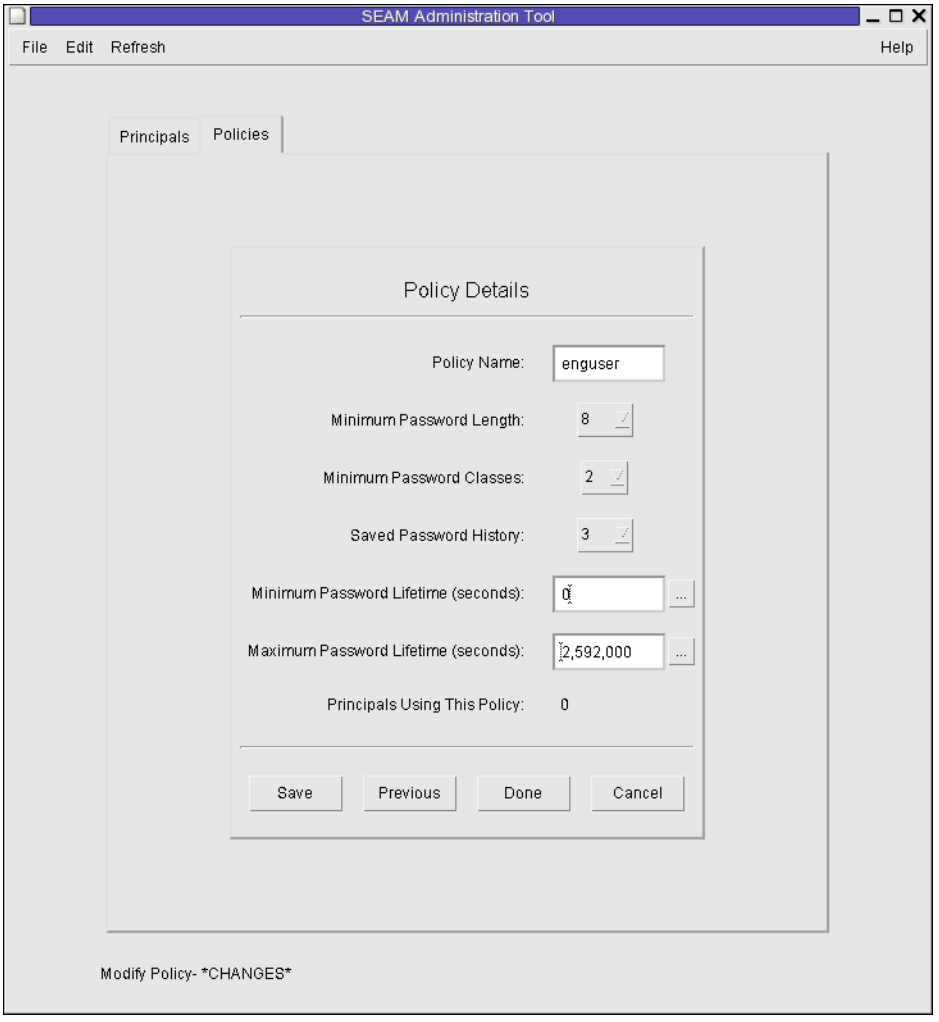
3. **Sélectionnez la stratégie dans la liste que vous souhaitez afficher, puis cliquez sur Modify.**

   Le panneau Policy Details (Détails de la stratégie) s'affiche.

4. **Lorsque vous avez fini de consulter ces informations, cliquez sur Cancel (Annuler).**

Exemple 25–10 Affichage des attributs d'une stratégie Kerberos

L'exemple suivant montre le panneau Policy Details (Détails de la stratégie) lorsque vous visualisez la stratégie `test`.



Exemple 25–11 Affichage des attributs d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `get_policy` de `kadmin` est utilisée pour afficher les attributs de la stratégie `enguser`.

```
kadmin: get_policy enguser
Policy: enguser
Maximum password life: 2592000
Minimum password life: 0
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 0
kadmin: quit
```

Le nombre de références est le nombre de principaux qui utilisent cette stratégie.

▼ Création d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Policies (Stratégies).**

3. **Cliquez sur New (Nouveau).**

   Le panneau Policy Details (Détails de la stratégie) s'affiche.

4. **Spécifiez un nom pour la stratégie dans le champ correspondant.**

   Le nom de stratégie est obligatoire.

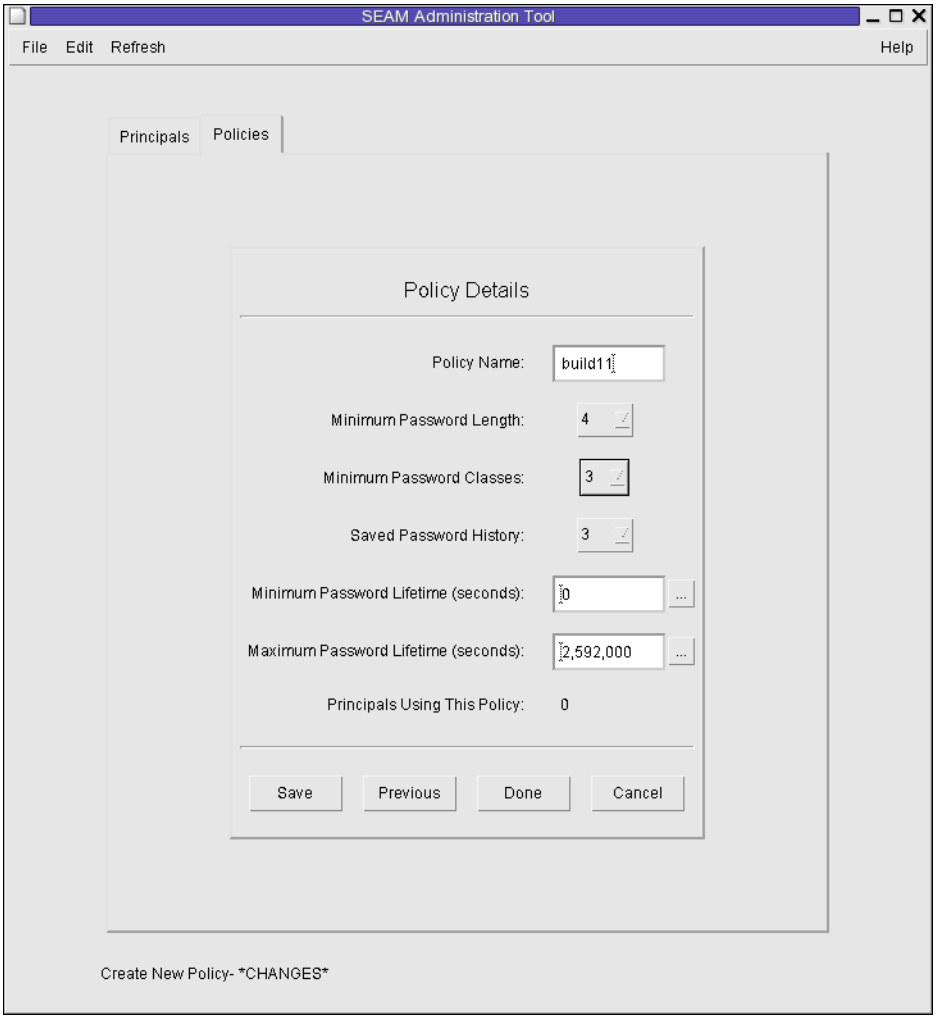
5. **Spécifiez les valeurs des attributs de la stratégie.**

   Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au Tableau 25–5 pour toutes les descriptions des attributs de stratégies.

6. **Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).**

Exemple 25–12 Création d'une stratégie Kerberos

Dans l'exemple suivant, une stratégie appelée `build11` est créée. Les classes de mot de passe minimales sont définies sur 3.



Exemple 25–13 Création d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `add_policy` de `kadmin` est utilisée pour créer la stratégie `build11`. Cette stratégie requiert au moins trois classes de caractères dans le mot de passe.

```
$ kadmin
kadmin: add_policy -minclasses 3 build11
kadmin: quit
```

Duplication d'une stratégie Kerberos

Cette procédure explique comment utiliser tout ou partie des attributs d'une stratégie existante pour créer une nouvelle stratégie. Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Policies (Stratégies).**

3. **Sélectionnez la stratégie dans la liste que vous souhaitez dupliquer, puis cliquez sur Duplicate (Dupliquer).**

   Le panneau Policy Details (Détails de la stratégie) s'affiche. Tous les attributs de la stratégie sélectionnée sont dupliqués, sauf le champ de nom, qui est vide.

4. **Spécifiez un nom pour la stratégie dupliquée dans le champ correspondant.**

   Le nom de stratégie est obligatoire. Pour effectuer une copie exacte de la stratégie que vous avez sélectionnée, cliquez sur Save et passez à l'Étape 6.

5. **Spécifiez des valeurs différentes pour les attributs de la stratégie.**

   Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au Tableau 25–5 pour toutes les descriptions des attributs de stratégies.

6. **Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).**

Modification d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

1. **Si nécessaire, démarrez l'Outil SEAM .**

   Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

   ```
   $ /usr/sbin/gkadmin
   ```

2. **Cliquez sur l'onglet Policies (Stratégies).**

3. **Sélectionnez la stratégie dans la liste que vous souhaitez modifier, puis cliquez sur Modify.**

   Le panneau Policy Details (Détails de la stratégie) s'affiche.

4 **Modifiez les attributs de la stratégie.**

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au Tableau 25–5 pour toutes les descriptions des attributs de stratégies.

Remarque – Vous ne pouvez pas modifier le nom d'une stratégie. Pour renommer une stratégie, vous devez la dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancienne.

---

5 **Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).**

Exemple 25–14 Modification d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `modify_policy` de `kadmin` est utilisée pour modifier la longueur minimale d'un mot de passe de cinq caractères pour la stratégie `build11`.

```
$ kadmin
kadmin: modify_policy -minlength 5 build11
kadmin: quit
```

▼ Suppression d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

Remarque – Avant de supprimer une stratégie, vous devez annuler la stratégie à partir de tous les principaux qui l'utilisent actuellement. Pour ce faire, vous devez modifier les attributs de stratégie des principaux. La stratégie ne peut pas être supprimée si un principal l'utilise.

---

1 **Si nécessaire, démarrez l'Outil SEAM .**

Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'Outil SEAM ” à la page 517.

```
$ /usr/sbin/gkadmin
```

2 **Cliquez sur l'onglet Policies (Stratégies).**

3 **Sélectionnez la stratégie dans la liste que vous voulez supprimer, puis cliquez sur Delete.**

Après avoir confirmé la suppression, la stratégie est supprimée.

Exemple 25–15 Suppression d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `delete_policy` de `kadmin` est utilisée pour supprimer la stratégie `build11`.

```
kadmin: delete_policy build11
Are you sure you want to delete the policy "build11"? (yes/no): yes
kadmin: quit
```

Avant de supprimer une stratégie, vous devez annuler la stratégie à partir de tous les principaux qui l'utilisent actuellement. Pour ce faire, vous devez utiliser la commande `modify_principal -policy` de `kadmin` sur les principaux affectés. La commande `delete_policy` échoue si la stratégie est en cours d'utilisation par un principal.

Référence de l'Outil SEAM

Cette section fournit les descriptions de chaque panneau de l'Outil SEAM . En outre, des d'informations sur l'utilisation de privilèges limités avec l'Outil SEAM sont fournies.

Descriptions des panneaux de l'Outil SEAM

Cette section fournit des descriptions pour chaque attribut de principal et de stratégie que vous pouvez spécifier ou afficher dans l'outil SEAM. Les attributs sont organisés par le panneau dans lequel ils sont affichés.

TABLEAU 25–2 Attributs pour le panneau Principal Basics de l'Outil SEAM

Attribut	Description
Nom du principal	Nom du principal (qui est la partie *primary*/ *instance* d'un nom complet de principal). Un principal est une identité unique à laquelle le KDC peut affecter les tickets. Si vous modifiez un principal, vous ne pouvez pas modifier son nom.
Password (Mot de passe)	Mot de passe du principal. Vous pouvez utiliser le bouton Generate Random Password (Générer un mot de passe aléatoire) pour créer un mot de passe aléatoire pour le principal.
Policy (Stratégie)	Menu des stratégies disponibles pour le principal.
Account Expires (Expiration du compte)	Date et heure d'expiration du compte principal. Lorsque le compte expire, le principal ne peut plus obtenir un ticket d'octroi de tickets (TGT) et peut être incapable de se connecter.
Last Principal Change (Dernière modification de principal)	Date à laquelle les informations du principal ont été modifiées pour la dernière fois. (Lecture seule)
Last Changed By (Dernière modification par)	Nom du principal qui a modifié en dernier le compte de ce principal. (Lecture seule)
Comments (Commentaires)	Commentaires liés au principal (par exemple, « compte temporaire »).

TABLEAU 25–3 Attributs pour le panneau Principal Details de l'Outil SEAM

Attribut	Description
Last Success (Dernier succès)	Date et heure de la dernière connexion réussie du principal. (Lecture seule)
Last Failure (Dernier échec)	Date et heure du dernier échec de connexion du principal. (Lecture seule)
Failure Count (Nombre d'échecs)	Nombre de fois où une erreur de connexion s'est produite pour le principal. (Lecture seule)
Last Password Change (Dernière modification du mot de passe)	Date et heure auxquelles le mot de passe du principal a été modifié pour la dernière fois. (Lecture seule)
Password Expires (Date d'expiration du mot de passe)	Date et heure auxquelles le mot de passe actuel du principal expire.
Key Version (Version de la clé)	Numéro de version de la clé pour le principal. Cet attribut n'est généralement modifié que quand le mot de passe est compromis.
Maximum Lifetime (seconds) (Durée de vie maximale (en secondes))	Durée maximale pour laquelle un ticket peut être accordé au principal (sans renouvellement).
Maximum Renewal (seconds) (Renouvellement maximal (en secondes))	Durée maximale pendant laquelle un ticket peut être renouvelé pour le principal.

TABLEAU 25–4 Attributs du panneau Principal Flags (Indicateur de principal) de l'Outil SEAM

Attribut (boutons radio)	Description
Disable Account (Désactiver un compte)	Lorsqu'elle est sélectionnée, cette option empêche le principal de se connecter. Cet attribut fournit un moyen facile de geler temporairement un compte principal.
Require Password Change (Exiger la modification du mot de passe)	Lorsque cette option est sélectionnée, l'option fait expirer le mot de passe en cours du principal, ce qui oblige l'utilisateur à utiliser la commande `kpasswd` pour créer un nouveau mot de passe. Cet attribut est utile si une violation de la sécurité se produit et que vous devez vous assurer que les anciens mots de passe sont remplacés.
Allow Postdated Tickets (Autoriser les tickets postdatés)	Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets postdatés. Par exemple, vous pouvez avoir besoin d'utiliser des tickets postdatés pour les tâches de `cron` qui doivent s'exécuter après les heures de bureau, mais vous ne pouvez pas obtenir de tickets en avance en raison de courtes durées de vie de tickets.
Allow Forwardable Tickets (Autoriser les tickets transmissibles)	Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets transmissibles. Les tickets transmissibles sont des tickets qui sont transmis à l'hôte distant pour fournir une session à connexion unique. Par exemple, si vous utilisez des tickets transmissibles et que vous authentifiez via `ftp` ou `rsh`, d'autres services, tels que les services NFS, sont alors disponibles sans que vous soyez invité à saisir un autre mot de passe.

TABLEAU 25–4 Attributs du panneau Principal Flags (Indicateur de principal) de l'Outil SEAM *(Suite)*

Attribut (boutons radio)	Description
Allow Renewable Tickets (Autoriser les tickets renouvelables)	Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets renouvelables. Un principal peut étendre automatiquement la date d'expiration ou le temps qu'un ticket peut être renouvelable (plutôt que d'avoir à obtenir un nouveau ticket une fois que le premier ticket arrive à expiration). Actuellement, le service NFS est le service de ticket qui peut renouveler les tickets.
Allow Proxiable Tickets (Autoriser les tickets utilisables avec proxy)	Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets utilisables avec proxy. Un ticket utilisable avec proxy est un ticket qui peut être utilisé par un service pour le compte d'un client afin d'effectuer une opération pour ce dernier. Avec un ticket utilisable avec proxy, un service peut prendre l'identité d'un client et obtenir un ticket pour un autre service. Toutefois, le service ne peut pas obtenir de ticket d'octroi de tickets (TGT).
Allow Service Tickets (Autoriser les tickets de service)	Lorsqu'elle est sélectionnée, cette option permet aux tickets de service d'être émis pour le principal. Vous ne devez pas autoriser les tickets de service à être émis pour les principaux `kadmin/`*hostname* et `changepw/` *hostname*. Cette pratique permet de s'assurer que seuls ces principaux peuvent mettre à jour la base de données KDC.
Allow TGT-Based Authentication (Autoriser l'authentification par TGT)	Lorsque cette option est sélectionnée, le principal de service est autorisé à fournir des services à un autre principal. Plus précisément, cet attribut autorise le KDC à émettre un ticket de service pour le service principal. Cet attribut est uniquement valable pour les principaux de service. Lorsque ce bouton n'est pas coché, les tickets de service ne peuvent pas être émis pour le principal de service.
Allow Duplicate Authentication (Autoriser la duplication d'authentification)	Lorsqu'elle est sélectionnée, cette option autorise le principal d'utilisateur à obtenir des tickets de service pour d'autres principaux d'utilisateur. Cet attribut est uniquement valide pour les principaux d'utilisateur. Si cette option n'est pas sélectionnée, le principal d'utilisateur peut toujours obtenir des tickets de service pour les principaux de service, mais pas pour d'autres principaux d'utilisateur.
Required Preauthentication (Pré-authentification requise)	Lorsque cette option est sélectionnée, le KDC n'envoie pas le ticket d'octroi de tickets (TGT) demandé au principal jusqu'à ce que le KDC puisse authentifier (par le biais d'un logiciel) que le principal est bien celui qui demande le ticket. Cette pré-authentification est généralement effectuée par le biais d'un mot de passe supplémentaire, par exemple, à partir d'une carte DES. Si elle n'est pas sélectionnée, le KDC n'a pas besoin de pré-authentifier le principal avant que le KDC lui envoie un TGT demandé.
Required Hardware Authentication (Authentification matérielle requise)	Lorsque cette option est sélectionnée, le KDC n'envoie pas le ticket d'octroi de tickets (TGT) demandé au principal jusqu'à ce que le KDC puisse authentifier (par le biais d'un matériel) que le principal est bien celui qui demande le ticket. La pré-authentification matérielle peut se produire, par exemple, sur un lecteur d'anneau Java. Si elle n'est pas sélectionnée, le KDC n'a pas besoin de pré-authentifier le principal avant que le KDC lui envoie un TGT demandé.

TABLEAU 25–5 Attributs pour le panneau Policy Basics de l'Outil SEAM

Attribut	Description
Nom de la stratégie	Nom de la stratégie. Une stratégie est un ensemble de règles qui régissent le mot de passe et les tickets d'un principal. Si vous modifiez une stratégie, vous ne pouvez pas modifier son nom.
Minimum Password Length (Longueur minimale de mot de passe)	Longueur minimale du mot de passe du principal.
Minimum Password Classes (Nombre minimal de classes de mot de passe)	Nombre minimal de types de caractères différents qui sont requis dans le mot de passe du principal. Par exemple, une valeur de classes minimales de 2 signifie que le mot de passe doit comporter au moins deux types de caractères différents, tels que des lettres et des chiffres (hi2mom). Une valeur de 3 signifie que le mot de passe doit comporter au moins trois types de caractères différents, comme des lettres, des chiffres et des signes de ponctuation (hi2mom!). Et ainsi de suite... Une valeur de 1 définit signifie l'absence de restriction sur le nombre de types de caractères de mot de passe.
Saved Password History (Historique de mots de passe enregistrés)	Nombre de mots de passe précédents qui ont été utilisés par le principal et liste des mots de passe précédents ne pouvant plus être utilisés.
Minimum Password Lifetime (seconds) (Durée de vie minimale du mot de passe (en secondes))	Période minimale pendant laquelle le mot de passe doit être utilisé avant de pouvoir être changé.
Maximum Password Lifetime (seconds) (Durée de vie maximale du mot de passe (en secondes))	Période maximale pendant laquelle le mot de passe peut être utilisé avant de devoir être changé.
Principals Using This Policy (Principaux utilisant cette stratégie)	Nombre de principaux auquel cette stratégie s'applique actuellement. (Lecture seule)

Utilisation de l'Outil SEAM avec privilèges d'administration Kerberos limités

Toutes les fonctions de l'outil SEAM sont disponibles si votre principal `admin` dispose de tous les privilèges d'administration de la base de données Kerberos. Cependant, il se peut que vous ayez des privilèges limités, tels qu'être seulement autorisé à consulter la liste des principaux ou à modifier le mot de passe d'un principal. Avec des privilèges d'administration Kerberos limités, vous pouvez toujours utiliser l'outil SEAM. Cependant, diverses parties de l'outil SEAM

changent en fonction des privilèges d'administration Kerberos dont vous ne disposez pas. Tableau 25–6 montre comment l'outil SEAM change en fonction de vos privilèges d'administration Kerberos.

Le changement le plus visible de l'outil SEAM se produit lorsque vous ne disposez pas du privilège de liste. Sans le privilège de liste, les panneaux de listes n'affichent pas la liste des principaux et les stratégies à manipuler. Au lieu de cela, vous devez utiliser le champ de nom dans les panneaux de listes pour spécifier un principal ou une stratégie que vous voulez manipuler.

Si vous vous connectez à l'outil SEAM et que vous ne disposez pas de privilèges suffisants pour effectuer des tâches avec lui, le message suivant s'affiche et vous êtes renvoyé à la fenêtre de connexion d'administration SEAM :

```
Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal.
```

Pour modifier les privilèges d'un principal afin qu'il puisse administrer la base de données Kerberos, reportez-vous à la section "Modification des privilèges d'administration Kerberos" à la page 530.

TABLEAU 25–6 Utilisation de l'outil SEAM avec des privilèges d'administration Kerberos limités

Privilège non autorisé	Changements de l'outil SEAM
`a` (ajouter)	Les boutons Create New et Duplicate ne sont pas disponibles dans les panneaux Principal List et Policy List. Sans le privilège d'ajout, vous ne pouvez pas créer de principaux ou de stratégies, ni les dupliquer.
`d` (supprimer)	Le bouton Delete n'est pas disponible dans les panneaux Principal List et Policy List. Sans le privilège de suppression, vous ne pouvez pas supprimer de principaux ou de stratégies.
`m` (modifier)	Le bouton Modify n'est pas disponible dans les panneaux Principal List et Policy List. Sans le privilège de modification, vous ne pouvez pas modifier de principaux ou de stratégies. En outre, avec le bouton Modify non disponible, vous ne pouvez pas modifier le mot de passe d'un principal, même si vous avez le privilège de modification de mot de passe.
`c` (modifier un mot de passe)	Le champ Password du panneau Principal Basics est en lecture seule et ne peut pas être modifié. Sans le privilège de changement de mot de passe, vous ne pouvez pas modifier le mot de passe d'un principal. Notez que même si vous avez le privilège changement de mot de passe, vous devez également avoir le privilège de modification pour modifier le mot de passe d'un principal.

TABLEAU 25–6 Utilisation de l'outil SEAM avec des privilèges d'administration Kerberos limités *(Suite)*

Privilège non autorisé	Changements de l'outil SEAM
`i` (consultation de base de données)	Les boutons Modify et Duplicate ne sont pas disponibles dans les panneaux Principal List et Policy List. Sans le privilège de consultation, vous ne pouvez pas modifier ou dupliquer de principaux ou de stratégies. En outre, avec le bouton Modify non disponible, vous ne pouvez pas modifier le mot de passe d'un principal, même si vous avez le privilège de modification de mot de passe.
`l` (liste)	La liste des principaux et des stratégies dans les panneaux de liste est indisponible. Au lieu de cela, vous devez utiliser le champ de nom dans les panneaux de listes pour spécifier un principal ou une stratégie que vous voulez manipuler.

Administration des fichiers keytab

Tous les hôtes qui fournissent un service doivent disposer d'un fichier local, appelé un *keytab* (abréviation de « key table » (table des clés). Le fichier keytab contient le principal pour le service approprié, appelé *clé de service*. Une clé de service est utilisée par un service pour s'authentifier auprès du KDC et est uniquement connue de Kerberos et du service lui-même. Par exemple, si vous avez un serveur NFS utilisant Kerberos, le serveur doit avoir un fichier keytab qui contient son principal de service `nfs`.

Pour ajouter une clé de service à un fichier keytab, vous ajoutez le principal de service approprié à un fichier keytab de l'hôte à l'aide de la commande `ktadd` de `kadmin`. Comme vous êtes en train d'ajouter un principal de service à un fichier keytab, le principal doit exister dans la base de données Kerberos afin que `kadmin` puisse vérifier son existence. Sur le KDC maître, le fichier keytab est situé sous `/etc/krb5/kadm5.keytab`, par défaut. Sur les serveurs d'applications qui fournissent des services utilisant Kerberos, le fichier keytab est situé à `/etc/krb5/krb5.keytab`, par défaut.

Un fichier keytab est comparable à un mot de passe d'utilisateur. Tout comme il est important pour les utilisateurs de protéger leurs mots de passe, il est tout aussi important pour les serveurs d'applications de protéger leurs fichiers keytab. Vous devez toujours stocker les fichiers keytab sur un disque local et les rendre lisibles uniquement par l'utilisateur `root`. En outre, vous ne devez jamais envoyer un fichier keytab par le biais d'un réseau non sécurisé.

Il existe également une instance spéciale dans laquelle ajouter un principal `root` au fichier keytab d'un hôte. Si vous souhaitez qu'un utilisateur sur le client Kerberos monte des systèmes de fichiers NFS utilisant Kerberos, qui nécessitent un accès équivalent au root, vous devez ajouter le principal `root` du client à son fichier keytab. Dans le cas contraire, les utilisateurs doivent utiliser la commande `kinit` en tant que `root` pour obtenir des informations

d'identification pour le principal `root` du client lorsqu'ils souhaitent monter un système de fichiers NFS utilisant Kerberos avec accès `root`, même lorsqu'ils utilisent l'agent de montage automatique.

Remarque – Lorsque vous configurez un KDC maître, vous devez ajouter les principaux `kadmind` et `changepw` au fichier `kadm5.keytab` .

Une autre commande que vous pouvez utiliser pour administrer les fichiers keytab est la commande `ktutil`. Cette commande interactive vous permet de gérer le fichier keytab d'un hôte local sans disposer de privilèges d'administration Kerberos, car `ktutil` n'interagit pas avec la base de données Kerberos comme le fait `kadmin`. Par conséquent, après l'ajout d'un principal à un fichier keytab, vous pouvez utilisez `ktutil` pour visualiser la liste de clés dans le fichier keytab ou pour désactiver temporairement l'authentification d'un service.

Remarque – Lorsque vous modifiez un principal dans un fichier keytab à l'aide de la commande `ktadd` dans `kadmin`, une nouvelle clé est générée et ajoutée au fichier keytab.

Administration des fichiers keytab (liste des tâches)

Tâche	Description	Voir
Ajout d'un principal de service à un fichier keytab	Utilisez la commande `ktadd` de `kadmin` pour ajouter un principal de service dans un fichier keytab.	"Ajout d'un principal de service Kerberos à un fichier keytab" à la page 548
Suppression d'un principal de service d'un fichier keytab	Utilisez la commande `ktremove` de `kadmin` pour supprimer un principal de service d'un fichier keytab.	"Suppression d'un principal de service d'un fichier keytab " à la page 549
Affichage de la liste de clés (liste des principaux) dans un fichier keytab	Utilisez la commande `ktutil` pour afficher la liste de clés dans un fichier keytab.	"Affichage de la liste de clés (principaux) dans un fichier keytab" à la page 550
Désactivation temporaire de l'authentification d'un service sur un hôte	Cette procédure est un moyen rapide de désactiver temporairement l'authentification d'un service sur un hôte sans disposer des privilèges `kadmin`. Avant d'utiliser `ktutil` pour supprimer le principal de service du fichier keytab du serveur, copiez le fichier keytab d'origine vers un emplacement temporaire. Au moment de réactiver le service, copiez le fichier keytab d'origine à son emplacement correct.	"Désactivation temporaire de l'authentification d'un service sur un hôte" à la page 551

▼ Ajout d'un principal de service Kerberos à un fichier keytab

1 **Assurez-vous que le principal existe déjà dans la base de données Kerberos.**

Pour plus d'informations, reportez-vous à la section "Affichage de la liste des principaux Kerberos" à la page 520.

2 **Connectez-vous en tant que superutilisateur à l'hôte qui a besoin qu'un principal soit ajouté à son fichier keytab.**

3 **Démarrez la commande `kadmin`.**

```
# /usr/sbin/kadmin
```

4 **Ajoutez un principal à un fichier keytab en utilisant la commande `ktadd`.**

`kadmin:` **`ktadd`** `[`**`-e`** *enctype*`] [`**`-k`** *keytab*`] [`**`-q`**`] [`*principal* | **`-glob`** *principal-exp*`]`

`-e` *enctype*	Ignore la liste des types de chiffrement définie dans le fichier `krb5.conf`.
`-k` *keytab*	Spécifie le fichier keytab. Par défaut, `/etc/krb5/krb5.keytab` est utilisé.
`-q`	Affiche des informations moins détaillées.
principal	Spécifie le principal à ajouter au fichier keytab. Vous pouvez ajouter les principaux de service suivants : `host`, `root`, `nfs` et `ftp`.
`-glob` *principal-exp*	Spécifie les expressions de principal. Tous les principaux qui correspondent à *principal-exp* sont ajoutés au fichier keytab. Les règles qui régissent l'expression de principal sont les mêmes que pour la commande `list_principals` de `kadmin`.

5 **Quittez la commande `kadmin`.**

`kadmin:` **`quit`**

Exemple 25–16 Ajout d'un principal de service dans un fichier keytab

Dans l'exemple suivant, les principaux `kadmin/kdc1.example.com` et `changepw/kdc1.example.com` sont ajoutés à un fichier keytab de KDC maître. Dans cet exemple, le fichier keytab doit être le fichier spécifié dans le fichier `kdc.conf`.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com changepw/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
```

```
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
          mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: quit
```

Dans l'exemple suivant, le principal d'`host` de `denver` est ajouté au fichier keytab de `denver` de sorte que le KDC peut authentifier les services de réseau de `denver`.

```
denver # /usr/sbin/kadmin
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS
          mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
          with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc mode
          with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
          with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
          with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

▼ Suppression d'un principal de service d'un fichier keytab

1. **Connectez-vous en tant que superutilisateur sur l'hôte avec un principal de service qui doit être supprimé de son fichier keytab.**

2. **Démarrez la commande `kadmin`.**

   ```
   # /usr/sbin/kadmin
   ```

3. **(Facultatif) Pour afficher la liste actuelle des principaux (clés) dans le fichier keytab, utilisez la commande `ktutil`.**

   Pour obtenir des instructions détaillées, reportez-vous à la section "Affichage de la liste de clés (principaux) dans un fichier keytab" à la page 550.

4 Supprimez une identité du fichier keytab à l'aide de la commande `ktremove` commande.

```
kadmin: ktremove [-k keytab] [-q] principal [kvno | all | old ]
```

`-k` *keytab*	Spécifie le fichier keytab. Par défaut, `/etc/krb5/krb5.keytab` est utilisé.
`-q`	Affiche des informations moins détaillées.
principal	Spécifie le principal à supprimer du fichier keytab.
kvno	Supprime toutes les entrées pour le principal spécifié dont le numéro de version de clé correspond à *kvno*.
`all`	Supprime toutes les entrées pour le principal spécifié.
`old`	Supprime toutes les entrées pour le principal spécifié, à l'exception des principaux avec les numéros de version de clé les plus élevés.

5 Quittez la commande `kadmin`.

```
kadmin: quit
```

Exemple 25–17 Suppression d'un principal de service d'un fichier keytab.

Dans l'exemple suivant, le principal d'`host` de `denver` est supprimé du fichier keytab de `denver`.

```
denver # /usr/sbin/kadmin
kadmin: ktremove host/denver.example.com@EXAMPLE.COM
kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3
  removed from keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

▼ Affichage de la liste de clés (principaux) dans un fichier keytab

1 Connectez-vous en tant que superutilisateur sur l'hôte avec le fichier keytab.

Remarque – Bien qu'il soit possible de créer des fichiers keytab qui sont détenus par d'autres utilisateurs, l'utilisation de l'emplacement par défaut pour le fichier keytab requiert la propriété `root`.

---

2 Démarrez la commande `ktutil`.

```
# /usr/bin/ktutil
```

3 Lisez le fichier keytab dans le tampon de la liste de clés à l'aide de la commande `read_kt`.

```
ktutil: read_kt keytab
```

4 Affichez le tampon de la liste de clés en utilisant la commande `list`.

```
ktutil: list
```

Le tampon de la liste de clés actuel s'affiche.

5 Quittez la commande `ktutil`.

```
ktutil: quit
```

Exemple 25–18 Affichage de la liste de clés (principaux) dans un fichier keytab

L'exemple suivant affiche la liste de clés dans le fichier `/etc/krb5/krb5.keytab` sur l'hôte `denver` hôte.

```
denver # /usr/bin/ktutil
    ktutil: read_kt /etc/krb5/krb5.keytab
    ktutil: list
slot KVNO Principal
---- ---- ---------------------------------------
   1    5 host/denver@EXAMPLE.COM
    ktutil: quit
```

▼ Désactivation temporaire de l'authentification d'un service sur un hôte

Parfois, il peut s'avérer nécessaire de désactiver temporairement le mécanisme d'authentification d'un service, tel que `rlogin` ou `ftp` , sur un serveur d'applications réseau. Par exemple, si vous le souhaitez, vous pouvez empêcher les utilisateurs de se connecter à un système pendant que vous êtes en train d'effectuer des procédures de maintenance. La commande `ktutil` permet d'accomplir cette tâche en supprimant le principal de service à partir du fichier keytab du serveur, sans nécessiter de privilèges `kadmin`. Pour réactiver l'authentification, il vous suffit de copier le fichier keytab d'origine que vous avez enregistré jusqu'à son emplacement d'origine.

Remarque – Par défaut, la plupart des services sont configurés de façon à exiger l'authentification. Si un service n'est pas configuré pour demander l'authentification, le service fonctionne toujours, même si vous désactivez l'authentification pour le service.

---

1 Connectez-vous en tant que superutilisateur sur l'hôte avec le fichier keytab.

Remarque – Bien qu'il soit possible de créer des fichiers keytab qui sont détenus par d'autres utilisateurs, l'utilisation de l'emplacement par défaut pour le fichier keytab requiert la propriété `root`.

---

2. **Enregistrez le fichier keytab actuel dans un fichier temporaire.**

3. **Démarrez la commande `ktutil`.**

   ```
   # /usr/bin/ktutil
   ```

4. **Lisez le fichier keytab dans le tampon de la liste de clés à l'aide de la commande `read_kt`.**

   ```
   ktutil: read_kt keytab
   ```

5. **Affichez le tampon de la liste de clés en utilisant la commande `list`.**

   ```
   ktutil: list
   ```

   Le tampon de la liste de clés actuel s'affiche. Notez le numéro d'emplacement du service que vous voulez désactiver.

6. **Pour désactiver temporairement un service d'hôte, supprimez le principal de service du tampon de la liste de clés à l'aide de la commande `delete_entry`.**

   ```
   ktutil: delete_entry slot-number
   ```

   Où *slot-number* indique le numéro d'emplacement du principal de service à supprimer, ce qui est affiché par la commande `list`.

7. **Écrivez le tampon de la liste de clés sur un nouveau fichier keytab à l'aide de la commande `write_kt`.**

   ```
   ktutil: write_kt new-keytab
   ```

8. **Quittez la commande `ktutil`.**

   ```
   ktutil: quit
   ```

9. **Déplacez le nouveau fichier keytab.**

   ```
   # mv new-keytab keytab
   ```

10. **Lorsque vous souhaitez réactiver le service, copiez le fichier keytab temporaire (d'origine) vers son emplacement d'origine.**

Exemple 25–19 Désactivation temporaire d'un service sur un hôte

Dans l'exemple suivant, le service `host` sur l'hôte `denver` est temporairement désactivé. Pour réactiver le service d'hôte sur `denver`, vous devez copier le fichier `krb5.keytab.temp` vers le fichier `/etc/krb5/krb5.keytab` .

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp
denver # /usr/bin/ktutil
    ktutil:read_kt /etc/krb5/krb5.keytab
    ktutil:list
slot KVNO Principal
---- ---- ---------------------------------------
```

```
   1    8 root/denver@EXAMPLE.COM
   2    5 host/denver@EXAMPLE.COM
    ktutil:delete_entry 2
    ktutil:list
slot KVNO Principal
---- ---- -------------------------------------
   1    8 root/denver@EXAMPLE.COM
    ktutil:write_kt /etc/krb5/new.krb5.keytab
    ktutil: quit
denver # cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab
```

◆ ◆ ◆ CHAPITRE 26

Utilisation des applications Kerberos (tâches)

Ce chapitre est destiné à tout utilisateur d'un système sur lequel le service Kerberos est configuré. Ce chapitre explique comment utiliser les commandes utilisant Kerberos et les services qui sont fournis. Vous devez être déjà familiarisé avec ces commandes (dans leurs versions n'incluant pas l'utilisation de Kerberos) avant de lire les descriptions ci-après.

Étant donné que ce chapitre est destiné à l'utilisateur standard, il inclut des informations sur les tickets : obtention, affichage et destruction. Ce chapitre inclut également des informations sur la sélection ou la modification d'un mot de passe Kerberos.

Les informations contenues dans ce chapitre sont répertoriées ci-après :

Pour une présentation du produit Kerberos Oracle Solaris, reportez-vous au Chapitre 21, "Introduction au service Kerberos".

Gestion des tickets Kerberos

Cette section explique comment obtenir, afficher et détruire les tickets. Pour une présentation des tickets, reportez-vous à la section "Fonctionnement du service Kerberos" à la page 398.

Avez-vous besoin de vous soucier des tickets ?

Avec l'une des versions SEAM ou les versions Oracle Solaris installées, Kerberos est intégré dans la commande `login`, et vous obtenez des tickets automatiquement lorsque vous vous connectez. Les commandes utilisant Kerberos `rsh`, `rcp`, `rdist`, `telnet` et `rlogin` sont généralement configurées pour fournir des copies de vos tickets aux autres machines, de sorte que vous n'avez pas à demander explicitement des billets pour obtenir l'accès à ces machines. Votre

configuration peut ne pas inclure ce transfert automatique, mais il s'agit du comportement par défaut. Reportez-vous aux sections “Présentation des commandes utilisant Kerberos” à la page 565 et “Transfert des tickets Kerberos ” à la page 567 pour plus d'informations sur le transfert de tickets.

Pour plus d'informations sur les durées de vie des tickets, reportez-vous à la section “Durée de vie des tickets” à la page 578.

Création d'un ticket Kerberos

Normalement, si le PAM est configuré correctement, un ticket est créé automatiquement lorsque vous vous connectez, et vous n'avez pas besoin d'effectuer une action spécifique pour obtenir un ticket. Cependant, vous devrez peut-être créer un ticket si votre ticket arrive à expiration. En outre, vous devrez peut-être utiliser un autre principal en plus de votre principal par défaut, par exemple, si vous utilisez `rlogin - l` pour vous connecter à un ordinateur sous l'identité d'un autre utilisateur.

Pour créer un ticket, utilisez la commande `kinit`.

```
% /usr/bin/kinit
```

La commande `kinit` vous invite à saisir votre mot de passe. Pour la syntaxe complète de la commande `kinit`, reportez-vous à la page de manuel `kinit(1)`.

EXEMPLE 26–1 Création d'un ticket Kerberos

Cet exemple illustre un utilisateur, `jennifer`, créant un ticket sur son propre système.

```
% kinit
Password for jennifer@ENG.EXAMPLE.COM:       <Type password>
```

Ici, l'utilisateur `david` crée un ticket qui est valide pendant trois heures avec l'option `-l`.

```
% kinit -l 3h david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG:       <Type password>
```

L'exemple affiche l'utilisateur `david` créant un ticket transmissible (avec l'option `-f`) pour lui-même. Avec ce ticket transmissible, il peut, par exemple, se connecter à un autre système, puis se connecter via Internet ou un réseau local (`telnet`) à un système tiers.

```
% kinit -f david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG:          <Type password>
```

EXEMPLE 26–1 Création d'un ticket Kerberos *(Suite)*

Pour plus d'informations sur la façon dont le transfert de tickets fonctionne, reportez-vous aux sections “Transfert des tickets Kerberos ” à la page 567 et “Types de tickets” à la page 576.

Affichage des tickets Kerberos

Tous les tickets ne sont pas similaires. Un seul ticket peut, par exemple, être *transmissible*. Un autre ticket peut être *postdaté*. Un troisième ticket peut être à la fois transmissible et postdaté. Vous pouvez voir les billets que vous avez, ainsi que leurs attributs, en utilisant la commande `klist` avec l'option `-f` :

```
% /usr/bin/klist -f
```

Les symboles suivants indiquent les attributs qui sont associés à chaque ticket, tel qu'affiché par `klist` :

A Préauthentifié (Preauthenticated)

D Postdatable

d Postdaté (Postdated)

F Transmissible (Forwardable)

f Transmis (Forwarded)

I Initial

i Non valide (Invalid)

P Utilisable avec proxy (Proxiable)

p Proxy

R Renouvelable (Renewable)

La section “Types de tickets” à la page 576 décrit les différents attributs qu'un ticket peut avoir.

EXEMPLE 26–2 Affichage des tickets Kerberos

Cet exemple montre que l'utilisateur `jennifer` a un ticket *initial*, qui est *transmissible* (F) et *postdaté* (d), mais il n'a pas encore été validé (i).

```
% /usr/bin/klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: jennifer@EXAMPLE.COM

Valid starting                Expires                Service principal
09 Mar 04 15:09:51  09 Mar 04 21:09:51  nfs/EXAMPLE.COM@EXAMPLE.COM
```

EXEMPLE 26–2 Affichage des tickets Kerberos *(Suite)*

```
        renew until 10 Mar 04 15:12:51, Flags: Fdi
```

L'exemple suivant montre que l'utilisateur `david` a deux tickets qui ont été *transmis* (f) à son hôte à partir d'un autre hôte. Les tickets sont également *transmissibles* (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting                 Expires                 Service principal
07 Mar 04 06:09:51  09 Mar 04 23:33:51  host/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 17:09:51, Flags: fF

Valid starting                 Expires                 Service principal
08 Mar 04 08:09:51  09 Mar 04 12:54:51  nfs/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 15:22:51, Flags: fF
```

L'exemple suivant montre comment afficher les types de chiffrement de la clé de session et du ticket en utilisant l'option `-e`. L'option `-a` est utilisée pour mapper l'adresse de l'hôte à un nom d'hôte si le service de noms peut faire la conversion.

```
% klist -fea
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting                 Expires                 Service principal
07 Mar 04 06:09:51  09 Mar 04 23:33:51  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 10 Mar 04 17:09:51, Flags: FRIA
        Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32
        Addresses: client.example.com
```

Destruction des tickets Kerberos

Si vous souhaitez détruire tous les tickets Kerberos acquis au cours de votre session en cours, utilisez la commande `kdestroy`. La commande détruit votre cache des informations d'identification, ce qui détruit toutes vos informations d'identification et tous les tickets. Bien que ce ne soit pas généralement nécessaire, l'exécution de `kdestroy` réduit le risque de compromettre le cache des informations d'identification pendant que vous n'êtes pas connecté.

Pour détruire vos tickets, utilisez la commande `kdestroy`.

```
% /usr/bin/kdestroy
```

La commande `kdestroy` détruit vos tickets *all*. Vous ne pouvez pas utiliser cette commande pour détruire sélectivement un ticket donné.

Si vous allez vous éloigner de votre système et êtes inquiet qu'un intrus puisse utiliser vos autorisations, vous devez utiliser `kdestroy` ou un économiseur d'écran qui verrouille l'écran.

Gestion des mots de passe Kerberos

Avec le service Kerberos configuré, vous avez maintenant deux mots de passe : votre mot de passe Solaris normal et un mot de passe Kerberos. Vous pouvez faire en sorte que les deux mots de passe soient le même, ou ils peuvent être différents.

Conseils sur le choix d'un mot de passe

Votre mot de passe peut inclure presque n'importe quel caractère que vous pouvez taper. Les principales exceptions sont les touches Ctrl et Entrée. Un bon mot de passe est un mot de passe facile à retenir, mais qu'aucune autre personne ne peut deviner facilement. Voici quelques exemples de mauvais mots de passe :

- Les mots qui peuvent être trouvés dans un dictionnaire.
- N'importe quel nom commun ou populaire.
- Le nom d'une personne ou d'un personnage célèbre.
- Votre nom ou nom d'utilisateur sous la forme de votre choix (par exemple : votre nom écrit à l'envers, répété deux fois et ainsi de suite).
- Nom du conjoint, d'un enfant ou d'un animal de compagnie.
- Votre date de naissance ou la date de naissance d'un parent.
- Votre numéro de sécurité sociale, numéro de permis de conduire, numéro de passeport ou autre numéro d'identification.
- Tout exemple de mot de passe apparaissant dans ce manuel ou n'importe quel autre manuel.

Un bon mot de passe est un mot de passe d'au moins huit caractères. En outre, un mot de passe doit inclure une combinaison de caractères, tels que des lettres majuscules et minuscules, des chiffres et des signes de ponctuation. Exemples de mots de passe qui seraient convenables s'ils ne figuraient pas dans ce manuel :

- Acronymes, tels que "I2LMHinSF" (dont on se souvient sous la forme "I too left my heart in San Francisco" (J'ai moi aussi eu le cœur brisé à San Francisco))
- Mots dénués de sens faciles à prononcer, tels que "WumpaBun" ou "WangDangdoodle!"
- Expressions délibérément mal orthographiées, telles que "6o'cluck" ou "RrriotGrrrlsRrrule!"

Attention – N'utilisez pas ces exemples. Les mots de passe qui figurent dans des manuels sont les premiers mots de passe qu'un intrus va essayer.

Modification de votre mot de passe

Si le PAM est correctement configuré, vous pouvez modifier votre mot de passe Kerberos de deux manières :

- Avec la commande `passwd` UNIX habituelle. Avec le service Kerberos configuré, la commande `passwd` vous invite également automatiquement à entrer un nouveau mot de passe Kerberos.

  L'avantage d'utiliser `passwd` au lieu de `kpasswd` est que vous pouvez définir les deux mots de passe Kerberos et UNIX en même temps. Cependant, en règle générale,*il n'est pas nécessaire* de modifier les deux mots de passe avec `passwd`. Souvent, vous pouvez uniquement modifier le mot de passe UNIX et laisser le mot de passe Kerberos inchangé, ou vice-versa.

  Remarque – Le comportement de `passwd` dépend de la façon dont le module PAM est configuré. Vous pouvez être amené à modifier les deux mots de passe dans certaines configurations. Pour certains sites, le mot de passe UNIX doit être modifié, alors que d'autres sites nécessitent la modification du mot de passe Kerberos.

- Avec la commande `kpasswd`. `kpasswd` est très similaire à `passwd`. Une différence est que `kpasswd` ne change que les mots de passe Kerberos. Vous devez utiliser `passwd` si vous souhaitez modifier votre mot de passe UNIX.

  Une autre différence est que `kpasswd` peut modifier un mot de passe pour un principal Kerberos qui n'est pas un utilisateur UNIX valide. Par exemple, `david/admin` est un principal Kerberos, mais n'est pas un utilisateur UNIX réel. Par conséquent, vous devez utiliser `kpasswd` au lieu de `passwd`.

Une fois que vous avez modifié votre mot de passe, un certain temps s'écoule avant que le changement ne se propage sur l'ensemble d'un système (en particulier sur un réseau de grande taille). En fonction de la configuration de votre système, ce délai peut prendre de quelques minutes à une heure ou plus. Si vous avez besoin d'obtenir de nouveaux tickets Kerberos peu de temps après avoir modifié votre mot de passe, essayez d'abord le nouveau mot de passe. Si le nouveau mot de passe ne fonctionne pas, essayez de nouveau à l'aide de l'ancien mot de passe.

Le protocole Kerberos V5 permet aux administrateurs système de définir des critères relatifs aux mots de passe autorisés pour chaque utilisateur. Ces critères sont définis par la *politique*

définie pour chaque utilisateur (ou par une politique par défaut). Reportez-vous à la section "Administration des stratégies Kerberos" à la page 532 pour plus d'informations sur les politiques.

Par exemple, supposons que la stratégie de l'utilisateur `jennifer` (appelons-la `jenpol`) demande que les mots de passe contiennent au moins huit lettres et incluent un mélange de deux types de caractères. `kpasswd` rejettera donc une tentative d'utiliser "sloth" comme mot de passe.

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:        <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'sloth'>
New password (again):       <Jennifer re-types 'sloth'>
kpasswd: New password is too short.
Please choose a password which is at least 4 characters long.
```

Ici, `jennifer` utilise "slothrop49" comme mot de passe. "Slothrop49" répond aux critères, car il contient plus de huit lettres et contient deux types différents de caractères (chiffres et lettres minuscules).

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:       <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:       <Jennifer types 'slothrop49'>
New password (again):       <Jennifer re-types 'slothrop49'>
Kerberos password changed.
```

EXEMPLE 26–3 Modification de votre mot de passe

Dans l'exemple suivant, l'utilisateur `david` modifie ses deux mots de passe UNIX et Kerberos avec `passwd`.

```
% passwd
    passwd:  Changing password for david
    Enter login (NIS+) password:                <Type the current UNIX password>
    New password:                           <Type the new UNIX password>
    Re-enter password:                      <Confirm the new UNIX password>
```

EXEMPLE 26–3 Modification de votre mot de passe *(Suite)*

```
    Old KRB5 password:                  <Type the current Kerberos password>
    New KRB5 password:                  <Type the new Kerberos password>
    Re-enter new KRB5 password:         <Confirm the new Kerberos password>
```

Notez que `passwd` demande à la fois le mot de passe UNIX et le mot de passe Kerberos. Ce comportement est établi par la configuration par défaut. Dans ce cas, l'utilisateur `david` doit utiliser `kpasswd` pour définir son mot de passe Kerberos sur une autre valeur, comme indiqué ci-après.

Cet exemple illustre l'utilisateur `david` changeant seulement son mot de passe Kerberos avec `kpasswd` .

```
% kpasswd
kpasswd: Changing password for david@ENG.EXAMPLE.COM.
Old password:               <Type the current Kerberos password>
New password:               <Type the new Kerberos password>
New password (again):       <Confirm the new Kerberos password>
Kerberos password changed.
```

Dans cet exemple, l'utilisateur `david` modifie le mot de passe pour le principal Kerberos `david/admin` (qui n'est pas un utilisateur UNIX valide). Il doit utiliser `kpasswd`.

```
% kpasswd david/admin
kpasswd:  Changing password for david/admin.
Old password:               <Type the current Kerberos password>
New password:               <Type the new Kerberos password>
New password (again):       <Type the new Kerberos password>
Kerberos password changed.
```

Octroi de l'accès à votre compte

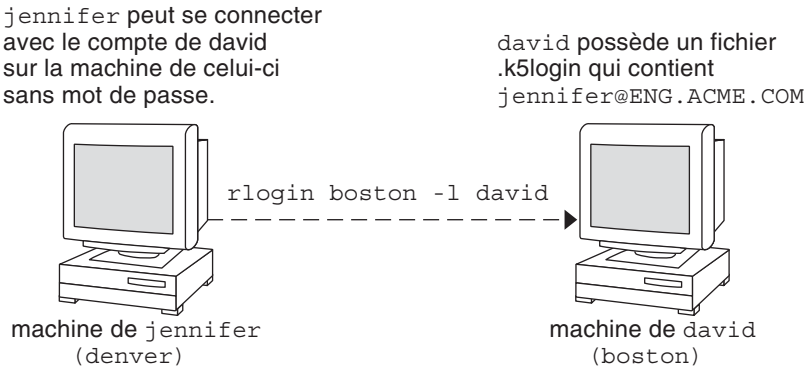
Si vous avez besoin d'autoriser quelqu'un à se connecter à votre compte (sous votre identité), vous pouvez le faire via Kerberos, sans révéler votre mot de passe, en insérant un fichier `.k5login` dans votre répertoire personnel. Un fichier `.k5login` est une liste d'un ou plusieurs principaux Kerberos correspondant à chaque personne à laquelle vous souhaitez accorder l'accès. Chaque principal doit figurer sur une ligne distincte.

Supposons que l'utilisateur `david` conserve un fichier `.k5login` dans son répertoire personnel qui se présente comme suit :

```
jennifer@ENG.EXAMPLE.COM
joe@EXAMPLE.ORG
```

Ce fichier permet aux utilisateurs `jennifer` et `joe` d'endosser l'identité de `david`, à condition qu'ils aient déjà des tickets Kerberos dans leurs domaines respectifs. Par exemple, jennifer peut se connecter à distance à la machine de `david`(`boston`), en tant que david, sans avoir à donner son mot de passe.

FIGURE 26–1 Utilisation du fichier `.k5login` pour accorder l'accès à votre compte



Dans le cas de figure où le répertoire personnel de `david` est monté sur NFS, à l'aide de protocoles Kerberos V5, à partir d'une autre (troisième) machine, `jennifer` doit avoir un ticket transmissible pour accéder à son répertoire personnel. Reportez-vous à la section “Création d'un ticket Kerberos ” à la page 556 pour obtenir un exemple d'utilisation d'un ticket transmissible.

Si vous devez vous connecter à d'autres ordinateurs sur un réseau, vous devrez inclure vos propres principaux Kerberos dans les fichiers `.k5login` sur ces machines.

L'utilisation d'un fichier `.k5login` est plus sûre que de donner votre mot de passe à un autre utilisateur, pour les raisons suivantes :

- Vous pouvez annuler l'accès à n'importe quel moment en supprimant le principal de votre fichier `.k5login`.
- Les principaux d'utilisateurs nommés dans le fichier `.k5login` dans votre répertoire d'accueil disposent d'un accès complet à votre compte sur cette machine (ou des ensembles de machines, si le fichier `.k5login` est partagé, par exemple, sur NFS). Toutefois, les services utilisant Kerberos autoriseront l'accès en fonction de l'identité de cet utilisateur, pas de la vôtre. Par conséquent, `jennifer` peut se connecter à la machine de `joe` et y effectuer des tâches. Toutefois, si elle utilise un programme utilisant Kerberos, tel que `ftp` ou `rlogin`, elle le fait sous sa propre identité.

- Kerberos conserve un journal des utilisateurs qui obtiennent des tickets. C'est pourquoi un administrateur système peut savoir, si nécessaire, qui est capable d'utiliser votre identité d'utilisateur à un moment donné.

Une méthode commune d'utiliser le fichier `.k5login` est de le placer dans le répertoire personnel de `root`, octroyant ainsi l'accès `root` pour cette machine aux principaux Kerberos répertoriés. Cette configuration permet aux administrateurs système de devenir `root` localement, ou de se connecter à distance en tant que `root`, sans avoir à communiquer le mot de passe `root`, et sans qu'il soit nécessaire pour quiconque de taper le mot de passe `root` sur le réseau.

EXEMPLE 26–4 Utilisation du fichier `.k5login` pour accorder l'accès à votre compte

Supposons que `jennifer` décide de se connecter à l'ordinateur `boston.example.com` en tant que `root`. Parce qu'elle a une entrée pour son nom de principal dans le fichier `.k5login` dans le répertoire personnel de `root` sur `boston.example.com`, elle n'a de nouveau pas besoin de taper son mot de passe.

```
% rlogin boston.example.com -l root -x
This rlogin session is using DES encryption for all data transmissions.
Last login: Thu Jun 20 16:20:50 from daffodil
SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998
boston[root]%
```

Commandes utilisateur Kerberos

Le produit Kerberos V5 est un système *à connexion unique*, ce qui signifie que vous n'avez à saisir votre mot de passe qu'une seule fois. Les programmes de Kerberos V5 effectuent l'authentification (et éventuellement le chiffrement) pour vous, car Kerberos a été intégré dans une suite de programmes réseau existants et connus. Les applications de Kerberos V5 sont des versions de programmes réseau UNIX existants auxquels des fonctions Kerberos ont été ajoutées.

Par exemple, lorsque vous utilisez un programme utilisant Kerberos pour vous connecter à un hôte distant, le programme, le KDC et l'hôte distant effectuent un ensemble de négociations rapides. Lorsque ces négociations sont terminées, le programme a prouvé votre identité en votre nom à l'hôte distant, et l'hôte distant vous a accordé l'accès.

Notez que les commandes utilisant Kerberos tentent de s'authentifier auprès de Kerberos en premier lieu. Si l'authentification Kerberos échoue, une erreur se produit ou l'authentification UNIX est tentée, en fonction des options qui ont été utilisées avec la commande. Reportez-vous à la section `Kerberos Security` dans chaque page de manuel des commandes Kerberos pour obtenir des informations plus détaillées.

Présentation des commandes utilisant Kerberos

Les services réseau utilisant Kerberos sont des programmes qui se connectent à une autre machine quelque part sur Internet. Ces programmes sont les suivants :

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Ces programmes ont des fonctionnalités qui utilisent de façon transparente vos tickets Kerberos pour négocier l'authentification et le chiffrement optionnel avec l'hôte distant. Dans la plupart des cas, vous remarquerez uniquement que vous n'avez plus à saisir votre mot de passe pour les utiliser, car Kerberos fournira une preuve de votre identité pour vous.

Les programmes réseau Kerberos V5 comprennent des options qui vous permettent de réaliser les opérations suivantes :

- Transférer vos billets à un autre hôte (si vous avez préalablement obtenu des tickets transmissibles).
- Chiffrer les données transférées entre vous et l'hôte distant.

Remarque – Cette section part du principe que vous êtes déjà familiarisé avec les versions non Kerberos de ces programmes, et met en évidence les fonctionnalités Kerberos ajoutées par le package Kerberos V5. Pour obtenir des descriptions détaillées des commandes décrites ici, reportez-vous à leurs pages de manuel respectives.

Les options Kerberos suivantes ont été ajoutées à `ftp`, `rcp`, `rlogin`, `rsh` et `telnet` :

`-a` Tente la connexion automatique à l'aide de vos tickets existants. Utilise le nom d'utilisateur tel que renvoyé par `getlogin()`, sauf si le nom est différent de l'ID utilisateur en cours. Reportez-vous à la page de manuel `telnet`(1) pour plus de détails.

`-f` Transfert un ticket *non transmissible* à un hôte distant. Cette option est mutuellement exclusive avec l'option `-F`. Elles ne peuvent pas être utilisées ensemble dans la même commande.

Vous voudrez transmettre un ticket si vous avez des raisons de croire que vous aurez besoin de vous authentifier auprès d'autres services basés sur Kerberos sur un troisième hôte. Par exemple, vous pouvez être amené à vous

connecter à distance à un autre ordinateur, puis à vous connecter à distance à partir de celui-ci à une troisième machine.

Vous devez absolument utiliser un ticket transmissible si votre répertoire personnel sur l'hôte distant est monté sur NFS à l'aide du mécanisme Kerberos V5. Dans le cas contraire, vous ne pourrez pas accéder à votre répertoire personnel. En d'autres termes, supposons que vous vous connectiez d'abord au système 1 (System 1). À partir du système 1, vous vous connectez à distance sur votre machine, System 2, qui permet de monter votre répertoire personnel du système 3 (System 3). Sauf si vous avez utilisé l'option `-f` ou `-F` avec `rlogin`, vous ne pourrez pas accéder à votre répertoire personnel car votre ticket ne peut pas être transmis au système 3.

Par défaut, `kinit` obtient des tickets d'octroi de tickets transmissibles (TGT, ticket-granting ticket). Cependant, votre configuration peut varier à cet égard.

Pour plus d'informations sur le transfert de tickets, reportez-vous à la section “Transfert des tickets Kerberos ” à la page 567.

`-F` Transfère une copie *retransmissible* de votre TGT à un système distant. Elle est similaire à `-f`, mais elle permet d'accéder à une autre machine (par exemple, une quatrième ou une cinquième). L'option `-F` peut donc être considérée comme étant un surensemble de l'option `-f`. L'option `-F` est mutuellement exclusive avec l'option `-f`. Elles ne peuvent pas être utilisées ensemble dans la même commande.

Pour plus d'informations sur le transfert de tickets, reportez-vous à la section “Transfert des tickets Kerberos ” à la page 567.

`-k` *realm* Demande des tickets pour l'hôte distant dans le domaine (*realm*) spécifié, au lieu de déterminer le domaine lui-même à l'aide du fichier `krb5.conf`.

`-K` Utilise vos billets pour l'authentification auprès de l'hôte distant, mais n'effectue pas la connexion automatiquement.

`-m` *mechanism* Spécifie le mécanisme de sécurité GSS-API à utiliser, comme indiqué dans le fichier `/etc/gss/mech`. La valeur par défaut est `kerberos_v5`.

`-x` Chiffre cette session.

`-X` *auth-type* Désactive le type d'authentification *auth-type*.

Le tableau suivant présente les commandes offrant des options spécifiques. Un "X" indique que la commande a une option de ce type.

TABLEAU 26–1 Options Kerberos pour les commandes réseau

	ftp	rcp	rlogin	rsh	telnet
-a					X
-f	X		X	X	X
-F			X	X	X
-k		X	X	X	X
-K					X
-m	X				
-x	X	X	X	X	X
-X					X

En outre, `ftp` permet la définition du niveau de protection d'une session à son invite :

clear (Annuler) Définit le niveau de protection sur "clear" (aucune protection). Ce niveau de protection est la valeur par défaut.

private (Privé) Définit le niveau de protection sur "private". La confidentialité et l'intégrité des transmissions de données sont protégées par chiffrement. Toutefois, le service de confidentialité peut ne pas être disponible pour tous les utilisateurs Kerberos.

safe (Sécurisé) Définit le niveau de protection sur "safe". L'intégrité des transmissions de données est protégée par contrôle cryptographique.

Vous pouvez également définir le niveau de protection à l'invite `ftp` en tapant `protect` suivi par l'un des niveaux de protection indiqués ci-dessus (`clear`, `private` ou `safe`).

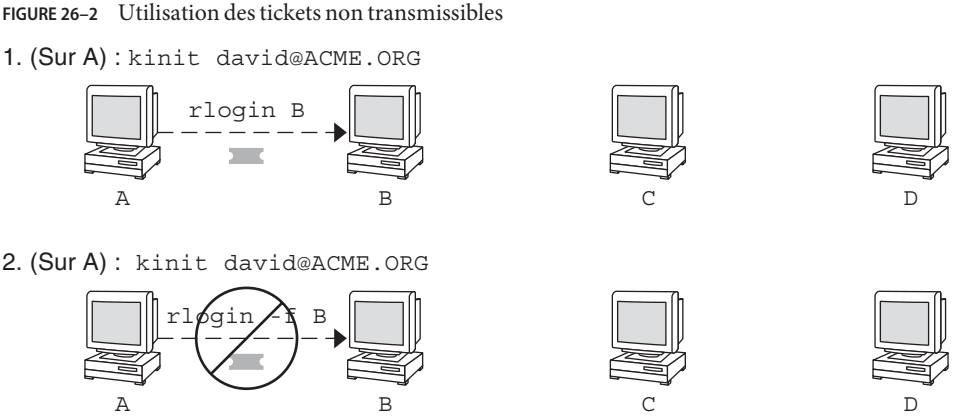
Transfert des tickets Kerberos

Comme décrit dans la section “Présentation des commandes utilisant Kerberos” à la page 565, certaines commandes vous permettent de transférer les tickets à l'aide de l'option `-f` ou `-F`. Le transfert des billets vous permet de "chaîner" vos transactions réseau. Vous pouvez, par exemple, vous connecter à distance sur un seul ordinateur, puis vous connecter à distance à partir de celui-ci à une autre machine. L'option `-f` vous permet de transférer un ticket, tandis que l'option `-F` vous permet de retransférer un ticket transmis.

Dans la Figure 26–2, l'utilisateur `david` obtient un ticket d'octroi de tickets (TGT) non transmissible avec `kinit`. Le ticket est non transmissible car il n'a pas spécifié l'option `-f`. Dans

le scénario 1, il est en mesure de se connecter à distance à la machine B, mais il ne peut aller plus loin. Dans le scénario 2, la commande `rlogin -f` échoue car il tente de transférer un ticket qui est non transmissible.

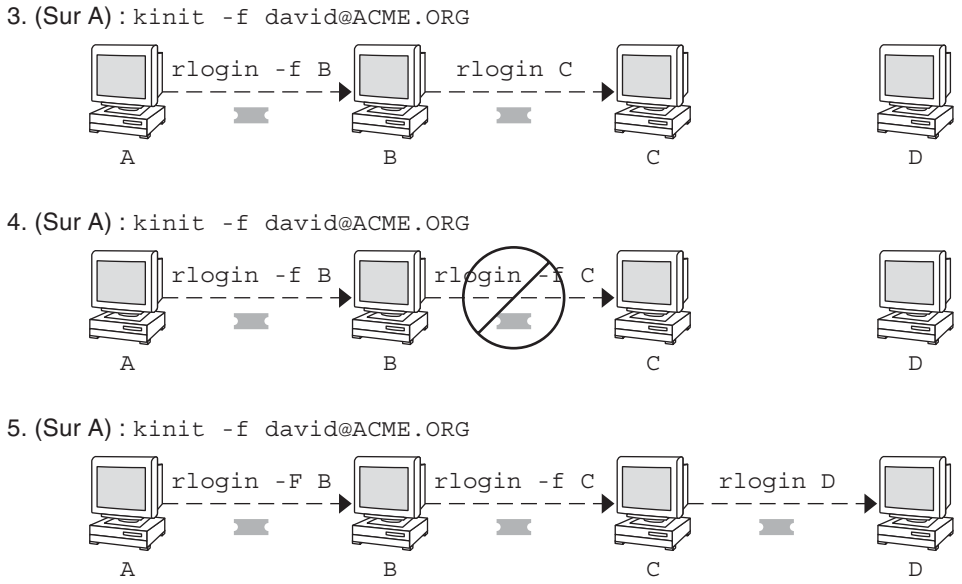
FIGURE 26–2 Utilisation des tickets non transmissibles



En réalité, les fichiers de configuration Kerberos sont définis de sorte que `kinit` obtient des tickets transmissibles par défaut. Cependant, votre configuration peut être différente. Pour des raisons d'explication, supposons que `kinit` *n'obtienne pas* de TGT transmissibles sauf si elle est appelée avec `kinit -f`. Notez d'ailleurs que `kinit` n'a pas d'option `-F`. Les TGT sont soit transmissibles ou non.

Dans la Figure 26–3, l'utilisateur `david` obtient des TGT transmissibles avec `kinit -f`. Dans le scénario 3, il est en mesure d'atteindre la machine C, car il utilise un ticket transmissible avec la commande `rlogin`. Dans le scénario 4, la deuxième commande `rlogin` échoue parce que le ticket n'est pas retransférable. En utilisant l'option `-F` à la place, comme dans le scénario 5, la deuxième `rlogin` réussit et le ticket peut être retransféré à l'ordinateur D.

FIGURE 26–3 Utilisation de tickets transmissibles



Utilisation de commandes utilisant Kerberos (exemples)

Les exemples suivants montrent comment les options des commandes utilisant Kerberos fonctionnent.

EXEMPLE 26–5 Utilisation des options `-a`, `-f` et `-x` avec `telnet`

Dans cet exemple, l'utilisateur `david` s'est déjà connecté et souhaite se connecter via Internet ou un réseau local (`telnet`) à la machine `denver.example.com`. Il utilise l'option `-f` pour transférer ses tickets existants, l'option `-x` pour chiffrer la session et l'option `-a` pour effectuer la connexion automatique. Dans la mesure où il n'a pas l'intention d'utiliser les services d'un troisième hôte, il peut utiliser `-f` au lieu de `-F`.

```
% telnet -a -f -x denver.example.com
Trying 128.0.0.5...
Connected to denver.example.com. Escape character is '^]'.
[ Kerberos V5 accepts you as "david@eng.example.com" ]
[ Kerberos V5 accepted forwarded credentials ]
SunOS 5.9: Tue May 21 00:31:42 EDT 2004  Welcome to SunOS
%
```

Vous remarquerez que l'ordinateur de `david` a utilisé Kerberos pour l'authentifier auprès de `denver.example.com` et l'a connecté automatiquement sous son identité. Il a eu une session chiffrée, une copie de ses tickets déjà en attente, et il n'a jamais eu à entrer son mot de passe. S'il

EXEMPLE 26–5 Utilisation des options `-a`, `-f` et `-x` avec `telnet` *(Suite)*

avait utilisé une version non Kerberos de `telnet` , il aurait été invité à saisir son mot de passe, lequel aurait été envoyé sur le réseau, non chiffré. Si un intrus avait analysé le trafic réseau à ce moment-là, il aurait connu le mot de passe de `david`.

Si vous transférez vos tickets Kerberos, `telnet` (ainsi que les autres commandes abordées ici) les détruit lorsqu'elle s'arrête.

EXEMPLE 26–6 Utilisation de `rlogin` avec l'option `-F`

Ici, l'utilisateur `jennifer` veut se connecter à sa propre machine, `boston.example.com`. Elle transmet ses tickets existants avec l'option `-F`, et chiffre la session à l'aide de l'option `-x`. Elle choisit `-F` plutôt que `-f` car une fois qu'elle s'est connectée à `boston`, elle peut vouloir effectuer d'autres transactions réseau nécessitant le retransfert des tickets. En outre, dans la mesure où elle transfère ses tickets existants, elle n'a pas à saisir son mot de passe.

```
% rlogin boston.example.com -F -x
This rlogin session is using encryption for all transmissions.
Last login Mon May 19 15:19:49 from daffodil
SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003
%
```

EXEMPLE 26–7 Définition du niveau de protection dans `ftp`

Supposons que `joe` veuille utiliser `ftp` pour obtenir son courrier à partir du répertoire `~joe/MAIL` de la machine `denver.example.com`, en chiffrant la session. L'échange se présente comme suit :

```
% ftp -f denver.example.com
Connected to denver.example.com
220 denver.example.org FTP server (Version 6.0) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded Name (daffodil.example.org:joe)
232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe
230 User joe logged in.
Remote system type is UNIX.
Using BINARY mode to transfer files.
ftp> protect private
200 Protection level set to Private
ftp> cd ~joe/MAIL
250 CWD command successful.
ftp> get RMAIL
227 Entering Passive Mode (128,0,0,5,16,49)
150 Opening BINARY mode data connection for RMAIL (158336 bytes).
226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)
ftp> quit
%
```

Pour chiffrer la session, `joe` définit le niveau de protection sur `private`.

◆ ◆ ◆ CHAPITRE 27

Service Kerberos (référence)

Ce chapitre présente un grand nombre de fichiers, de commandes et de démons faisant partie du produit Kerberos. En outre, ce chapitre fournit des informations détaillées sur le fonctionnement de l'authentification Kerberos.

La liste suivante répertorie les informations contenues dans ce chapitre :

Fichiers Kerberos

TABLEAU 27–1 Fichiers Kerberos

Nom du fichier	Description
`~/.gkadmin`	Valeurs par défaut pour la création de principaux dans l'outil SEAM.
`~/.k5login`	Liste de principaux permettant l'accès à un compte Kerberos.
`/etc/krb5/kadm5.acl`	Fichier ACL de Kerberos incluant les noms de principaux des administrateurs KDC et leurs privilèges d'administration Kerberos.

TABLEAU 27–1 Fichiers Kerberos *(Suite)*

Nom du fichier	Description
`/etc/krb5/kadm5.keytab`	Fichier keytab pour le service `kadmin` sur le KDC maître
`/etc/krb5/kdc.conf`	Fichier de configuration du KDC.
`/etc/krb5/kpropd.acl`	Fichier de configuration de propagation de la base de données Kerberos.
`/etc/krb5/krb5.conf`	Fichier de configuration du domaine Kerberos.
`/etc/krb5/krb5.keytab`	Fichier keytab pour les serveurs d'application réseau.
`/etc/krb5/warn.conf`	Fichier de configuration de renouvellement automatique et d'avertissement d'expiration des tickets Kerberos.
`/etc/pam.conf`	PAM, fichier de configuration
`/tmp/krb5cc_`*uid*	Cache d'informations d'identification par défaut, où *uid* est l'UID décimal de l'utilisateur.
`/tmp/ovsec_adm.`*xxxxxx*	Cache d'informations d'identification pour la durée de vie des opérations de modification de mot de passe, où *xxxxxx* est une chaîne aléatoire.
`/var/krb5/.k5.`*REALM*	Fichier stash KDC contenant une copie de la clé principale de KDC.
`/var/krb5/kadmin.log`	Fichier journal de `kadmind`.
`/var/krb5/kdc.log`	Fichier journal du KDC.
`/var/krb5/principal`	Base de données de principaux Kerberos.
`/var/krb5/principal.kadm5`	Base de données d'administration Kerberos contenant des informations de stratégie.
`/var/krb5/principal.kadm5.lock`	Fichier de verrouillage de la base de données d'administration Kerberos.
`/var/krb5/principal.ok`	Fichier d'initialisation de la base de données de principaux Kerberos, créé lors de l'initialisation réussie de la base de données Kerberos.
`/var/krb5/principal.ulog`	Fichier journal de mise à jour Kerberos contenant des mises à jour pour la propagation incrémentielle.
`/var/krb5/slave_datatrans`	Fichier de sauvegarde du KDC utilisé par le script `kprop_script` pour la propagation.
`/var/krb5/slave_datatrans_`*slave*	Fichier de vidage temporaire créé lors des mises à jour complètes sur le *slave* spécifié.

Commandes Kerberos

Cette section présente quelques commandes incluses dans le produit Kerberos.

TABLEAU 27–2 Commandes Kerberos

Commande	Description
`/usr/bin/ftp`	Programme FTP.
`/usr/bin/kdestroy`	Détruit les tickets Kerberos.
`/usr/bin/kinit`	Obtient et met en cache les tickets d'octroi de tickets Kerberos.
`/usr/bin/klist`	Affiche les tickets Kerberos actuels.
`/usr/bin/kpasswd`	Modifie un mot de passe Kerberos.
`/usr/bin/ktutil`	Gère les fichiers keytab Kerberos.
`/usr/bin/rcp`	Programme de copie de fichiers à distance.
`/usr/bin/rdist`	Programme de distribution de fichiers à distance.
`/usr/bin/rlogin`	Programme de connexion à distance.
`/usr/bin/rsh`	Programme de shell à distance.
`/usr/bin/telnet`	Programme `telnet` utilisant Kerberos.
`/usr/lib/krb5/kprop`	Programme de propagation de base de données Kerberos.
`/usr/sbin/gkadmin`	Programme d'interface graphique d'administration de base de données Kerberos utilisé pour gérer les principaux et les stratégies.
`/usr/sbin/gsscred`	Gère les entrées de tableau gsscred.
`/usr/sbin/kadmin`	Programme d'interface graphique d'administration de base de données Kerberos à distance (utilisé avec l'authentification Kerberos), utilisé pour gérer les principaux, les stratégies, et les fichiers keytab.
`/usr/sbin/kadmin.local`	Programme d'interface graphique d'administration de base de données Kerberos local (utilisé sans l'authentification Kerberos et devant être exécuté sur le KDC maître), utilisé pour gérer les principaux, les stratégies et les fichiers keytab.
`/usr/sbin/kclient`	Script d'installation du client Kerberos utilisé avec ou sans profil d'installation.
`/usr/sbin/kdb5_ldap_util`	Crée des conteneurs LDAP pour les bases de données Kerberos.
`/usr/sbin/kdb5_util`	Crée des bases de données Kerberos et des fichiers stash.

TABLEAU 27–2 Commandes Kerberos *(Suite)*

Commande	Description
`/usr/sbin/kgcmgr`	Configure les KDC maître et esclave Kerberos.
`/usr/sbin/kproplog`	Présente un récapitulatif des entrées de mise à jour dans le journal de mise à jour.

Démons Kerberos

La table suivante répertorie les démons utilisés par les produits Kerberos.

TABLEAU 27–3 Démons Kerberos

Démon	Description
`/usr/sbin/in.ftpd`	Démon de FTP.
`/usr/lib/krb5/kadmind`	Démon d'administration de base de données Kerberos.
`/usr/lib/krb5/kpropd`	Démon de propagation de base de données Kerberos.
`/usr/lib/krb5/krb5kdc`	Démon de traitement des tickets Kerberos.
`/usr/lib/krb5/ktkt_warnd`	Démon de renouvellement automatique et d'avertissement d'expiration des tickets Kerberos.
`/usr/sbin/in.rlogind`	Démon de connexion à distance.
`/usr/sbin/in.rshd`	Démon de shell à distance.
`/usr/sbin/in.telnetd`	Démon `telnet` et Kerberos.

Terminologie Kerberos

La section suivante présente les termes Kerberos et leurs définitions. Ces termes sont utilisés dans la documentation Kerberos. Une bonne compréhension de ces termes est essentielle pour appréhender les concepts Kerberos.

Terminologie spécifique à Kerberos

Vous devez comprendre les termes de cette section pour pouvoir administrer les KDC.

Le *Centre de distribution des clés (Key Distribution Center)* ou *KDC* est le composant de Kerberos responsable de l'émission d'informations d'identification. Ces informations d'identification sont créées à l'aide des informations stockées dans la base de données KDC. Chaque domaine a besoin d'au moins deux KDC, un maître et au moins un esclave. Tous les

KDC génèrent des informations d'identification, mais seul le KDC maître gère toutes les modifications apportées à la base de données KDC.

Un *fichier stash* contient la clé principale du KDC. Cette clé est utilisée lorsqu'un serveur est redémarré pour authentifier automatiquement le KDC avant qu'il ne démarre les commandes `kadmind` et `krb5kdc`. Étant donné que ce fichier inclut la clé principale, ce fichier et toutes ses sauvegardes doivent être sécurisés. Le fichier est créé avec des autorisations en lecture seule pour `root`. Pour garder le fichier sécurisé, vous ne devez pas modifier les autorisations. Si le fichier est compromis, la clé peut être utilisée pour accéder à la base de données KDC ou la modifier.

Terminologie spécifique à l'authentification

Vous devez connaître les termes de cette section pour comprendre le processus d'authentification. Les programmeurs et les administrateurs système doivent être familiarisés avec ces termes.

Un *client* est un logiciel qui s'exécute sur le poste de travail d'un utilisateur. Le logiciel Kerberos qui s'exécute sur le client effectue de nombreuses demandes au cours de ce processus. Par conséquent, il est important de différencier les actions de ce logiciel de celles de l'utilisateur.

Les termes *server* et *service* sont souvent interchangeables. Pour clarifier, le terme *server* est utilisé pour définir le système physique sur lequel le logiciel Kerberos est en cours d'exécution. Le terme *service* correspond à une fonction particulière prise en charge sur un serveur (par exemple, `ftp` ou `nfs`). Dans la plupart des cas, la documentation mentionne les serveurs dans le cadre d'un service, mais cette définition obscurcit la signification des termes. Par conséquent, le terme *server* fait référence au système physique. Le terme *service* désigne le logiciel.

Le produit Kerberos utilise deux types de clés. Un type de clé est dérivé du mot de passe. Chaque principal d'utilisateur reçoit une clé dérivée du mot de passe qui n'est connue que du KDC et de l'utilisateur. L'autre type de clé utilisé par le produit Kerberos est une clé aléatoire qui n'est pas associée à un mot de passe et donc n'est pas adapté à l'utilisation par les principaux d'utilisateur. Les clés aléatoires sont généralement utilisées pour les principaux de service qui ont des entrées dans un fichier keytab et les clés de session générées par le KDC. Les principaux de service peuvent utiliser des clés aléatoires étant donné que le service peut accéder à la clé dans le fichier keytab qui lui permet de fonctionner de manière non interactive. Les clés de session sont générées par le KDC (et partagées entre le client et le service) pour assurer la sécurité des transactions entre un client et un service.

Un *ticket* est un 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. Un ticket contient les informations suivantes :

- Nom du principal du service
- Nom du principal de l'utilisateur

- Adresse IP de l'hôte de l'utilisateur
- Horodatage
- Valeur définissant la durée de vie du ticket.
- Copie de la clé de session

Toutes ces données sont chiffrées dans la clé de service du serveur. Notez que le KDC émet le ticket incorporé dans des informations d'identification décrites ci-dessous. Une fois le ticket émis, il peut être réutilisé jusqu'à son expiration.

Les *informations d'identification* sont un paquet d'informations comprenant un ticket et la clé de session correspondante. Les informations d'identification sont chiffrées avec la clé du principal effectuant la demande. En règle générale, le KDC génère des informations d'identification en réponse à une requête de ticket d'un client.

Un *authentificateur* correspond à des informations utilisées par le serveur pour authentifier le principal de l'utilisateur du client. Un authentificateur inclut le nom du principal de l'utilisateur, un horodatage et d'autres données. À 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 partagée par le client et le serveur. En général, le client crée l'authentificateur et l'envoie à l'aide du ticket du serveur ou du service pour s'authentifier auprès du serveur ou du service.

Types de tickets

Les tickets ont des propriétés qui régissent la façon dont ils peuvent être utilisés. Ces propriétés sont assignées au ticket lors de sa création et peuvent être modifiées ultérieurement. Par exemple, un ticket peut passer de `transmissible` à `transmis`. Vous pouvez visualiser les propriétés de ticket à l'aide de la commande `klist`. Voir “Affichage des tickets Kerberos” à la page 557.

Les tickets peuvent être décrits par un ou plusieurs des termes suivants :

Transmissible/transmis (Forwardable/forwarded)
: Un ticket transmissible peut être envoyé à partir d'un hôte vers un autre hôte, supprimant la nécessité d'un client de se réauthentifier. Par exemple, si l'utilisateur `david` obtient un ticket transmissible sur la machine de l'utilisateur `jennifer`, il peut se connecter à sa propre machine sans devoir demander un nouveau ticket (et donc s'authentifier à nouveau). Pour consulter un exemple d'utilisation d'un ticket transmissible, reportez-vous à l'Exemple 26–1.

Initial
: Un ticket initial est un ticket émis directement, et non sur la base 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. 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.

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

Postdatable/postdaté (Postdatable/postdated)
: Un ticket postdaté est un ticket qui ne devient valide qu'après une période spécifiée 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 son heure de début soit dépassée, et que 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 est marqué comme renouvelable, sa durée de vie est normalement égale à la durée de vie entière du ticket d'octroi de tickets.

Utilisable avec proxy/proxy (Proxiable/proxy)
: Parfois, il est nécessaire à un principal de permettre à un service d'effectuer une opération en son nom. Le nom du principal du proxy doit être spécifié lorsque le ticket est créé. La version Oracle Solaris ne prend pas en charge les tickets utilisables avec proxy ou les tickets proxy.

  Un ticket utilisable avec proxy est similaire à un ticket transmissible, à ceci près qu'il n'est valide que pour un seul service, tandis qu'un ticket transmissible accorde l'utilisation complète de l'identité du client au service. Un ticket transmissible peut par conséquent être considéré comme une sorte de super-proxy.

Renouvelable (Renewable)
: Comme les tickets avec de très longues durées de vie impliquent un risque de sécurité, les tickets peuvent être désignés comme renouvelables. Un ticket renouvelable possède deux moments d'expiration : l'heure à laquelle l'instance courante du ticket expire et la durée de vie maximale de tout ticket (une semaine). 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 dans l'heure. Lorsqu'un ticket atteint sa durée de vie maximale (dix heures), celui-ci expire automatiquement et ne peut pas être renouvelé.

Pour plus d'informations sur la façon de visualiser les attributs de tickets, reportez-vous à la section "Affichage des tickets Kerberos" à la page 557.

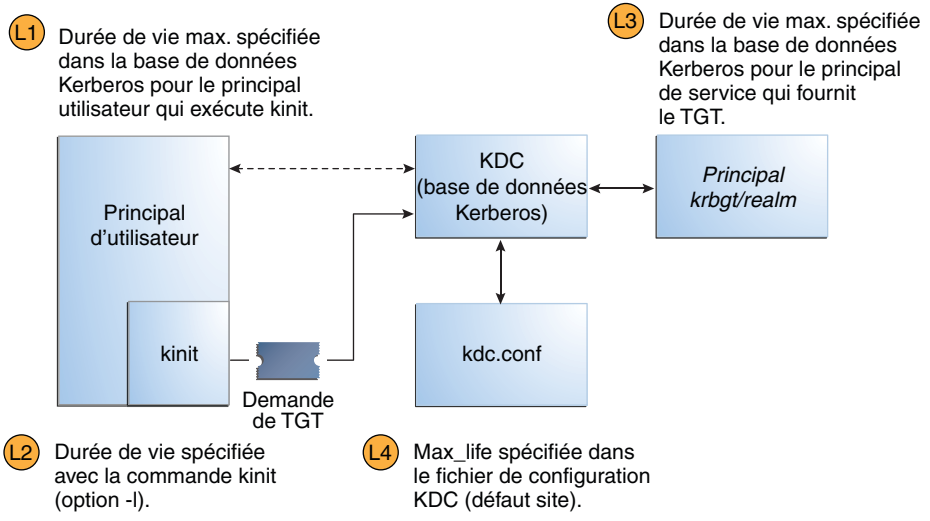
Durée de vie des tickets

Chaque fois qu'un principal obtient un ticket, y compris un ticket d'octroi de tickets (TGT), la durée de vie du ticket est définie comme la plus petite des valeurs de durée de vie suivantes :

- Valeur de durée de vie spécifiée par l'option `-l` de la commande `kinit`, si `kinit` est utilisée pour obtenir le ticket. Par défaut, `kinit` utilise la valeur de durée de vie maximale.
- Valeur de durée de vie maximale (`max_life`) spécifiée dans le fichier `kdc.conf`.
- Valeur de durée de vie maximale spécifiée dans la base de données Kerberos pour le principal de service fournissant le ticket. Dans le cas de `kinit`, le principal de service est `krbtgt/`*realm*.
- Valeur de durée de vie maximale spécifiée dans la base de données Kerberos pour le principal d'utilisateur demandant le ticket.

La Figure 27–1 montre comment la durée de vie d'un TGT est déterminée et d'où les quatre valeurs de durée de vie proviennent. Même si cette figure montre comment la durée de vie d'un TGT est déterminée, la même chose se produit globalement pour chaque obtention de ticket par un principal. La seule différence est que `kinit` n'offre pas une valeur de durée de vie et que le principal de service fournissant le ticket fournit une valeur de durée de vie maximale (au lieu du principal `krbtgt/` *realm*).

FIGURE 27–1 Détermination de la durée de vie d'un TGT



Durée de vie des tickets = valeur minimum de L1, L2, L3 et L4

La durée de vie d'un ticket renouvelable est également déterminée à partir de la plus basse de quatre valeurs, mais des valeurs de durée de vie renouvelables sont utilisées à la place, comme suit :

- Valeur de durée de vie renouvelable spécifiée par l'option `-r` de `kinit`, si `kinit` est utilisée pour obtenir ou renouveler le ticket.
- Valeur de durée de vie renouvelable maximale (`max_renewable_life`) spécifiée dans le fichier `kdc.conf`.
- Valeur de durée de vie renouvelable maximale spécifiée dans la base de données Kerberos pour le principal de service fournissant le ticket. Dans le cas de `kinit`, le principal de service est `krbtgt/`*realm*
- Valeur de durée de vie renouvelable maximale spécifiée dans la base de données Kerberos pour le principal d'utilisateur demandant le ticket.

Noms de principaux Kerberos

Chaque ticket est identifié par un nom de principal. Le nom de principal peut identifier un utilisateur ou un service. Voici des exemples de noms de principaux.

TABLEAU 27–4 Exemples de noms de principaux Kerberos

Nom du principal	Description
`changepw/kdc1.example.com@EXAMPLE.COM`	Principal pour le serveur KDC maître qui permet l'accès au KDC lorsque vous modifiez les mots de passe.
`clntconfig/admin@EXAMPLE.COM`	Principal utilisé par l'utilitaire d'installation `kclient`.
`ftp/boston.example.com@EXAMPLE.COM`	Principal utilisé par le service `ftp`. Ce principal peut être utilisé à la place d'un principal `host`.
`host/boston.example.com@EXAMPLE.COM`	Principal utilisé par des applications utilisant Kerberos (`klist` et `kprop`, par exemple) et des services (tels que `ftp` et `telnet`). Ce principal est appelé `host` ou principal de service. Le principal est utilisé pour authentifier les montages NFS. Ce principal est également utilisé par un client pour vérifier que le TGT émis au client provient du bon KDC.
`K/M@EXAMPLE.COM`	Nom de principal de la clé principale. Un nom de principal de clé principale est associé à chaque KDC maître.
`kadmin/history@EXAMPLE.COM`	Principal incluant une clé utilisée pour conserver l'historique des mots de passe d'autres principaux. Chaque KDC maître possède l'un de ces principaux.
`kadmin/kdc1.example.com@EXAMPLE.COM`	Principal pour le serveur KDC maître qui permet l'accès au KDC à l'aide de la commande `kadmind`.

TABLEAU 27–4 Exemples de noms de principaux Kerberos *(Suite)*

Nom du principal	Description
`kadmin/changepw.example.com@EXAMPLE.COM`	Principal utilisé pour accepter les demandes de modification de mot de passe émises par les clients qui n'exécutent pas une version d'Oracle Solaris.
`krbtgt/EXAMPLE.COM@EXAMPLE.COM`	Ce principal est utilisé lors de la génération d'un ticket d'octroi de tickets.
`krbtgt/EAST.EXAMPLE.COM@WEST.EXAMPLE.COM`	Ce principal est un exemple de ticket d'octroi de tickets inter-domaine.
`nfs/boston.example.com@EXAMPLE.COM`	Principal utilisé par le service NFS. Ce principal peut être utilisé à la place d'un principal `host`.
`root/boston.example.com@EXAMPLE.COM`	Principal associé au compte `root` sur un client. Ce principal est appelé principal `root` et fournit un accès `root` aux systèmes de fichiers montés NFS.
username`@EXAMPLE.COM`	Principal d'un utilisateur.
username`/admin@EXAMPLE.COM`	Principal `admin` pouvant être utilisé pour l'administration de la base de données KDC.

Fonctionnement du système d'authentification Kerberos

Des applications vous permettent de vous connecter à un système distant si vous pouvez fournir un ticket apportant la preuve de votre identité et un clé de session correspondante. La clé de session contient des informations spécifiques à l'utilisateur et au service en cours d'accès. Un ticket et une clé de session sont créés par le KDC pour tous les utilisateurs lors de leur première connexion. Le ticket et la clé de session correspondante constituent des informations d'identification. Lors de l'utilisation de plusieurs services réseau, un utilisateur peut obtenir de nombreuses informations d'identification. L'utilisateur doit disposer d'informations d'identification pour chaque service s'exécutant sur un serveur particulier. Par exemple, l'accès au service `ftp` sur un serveur nommé `boston` nécessite des informations d'identification. L'accès au service `ftp` sur un autre serveur nécessite ses propres informations d'identification.

Le processus de création et de stockage des informations d'identification est transparent. Les informations d'identification sont créées par le KDC, qui les envoie aux demandeurs. Une fois reçues, les informations d'identification sont stockées dans un cache d'informations d'identification.

Interaction du service Kerberos avec le DNS et le fichier `nsswitch.conf`

Le service Kerberos est compilé pour utiliser le DNS pour la résolution des noms d'hôte. Le fichier `nsswitch.conf` n'est pas du tout consulté lorsque la résolution de nom d'hôte est terminée.

Obtention de l'accès à un service à l'aide de Kerberos

Pour accéder à un service spécifique sur un serveur spécifique, l'utilisateur doit obtenir deux types d'informations d'identification. Le premier est pour le ticket d'octroi de tickets (aussi appelé TGT). Une fois que le service d'octroi de ticket a déchiffré ces informations d'identification, le service crée d'autres informations d'identification pour le serveur auquel l'utilisateur demande l'accès. Ces informations d'identification peuvent ensuite être utilisées pour demander l'accès à ce service sur le serveur. Une fois que le serveur a déchiffré ces informations d'identification, l'utilisateur obtient l'accès. Les sections suivantes décrivent le processus de manière plus détaillée.

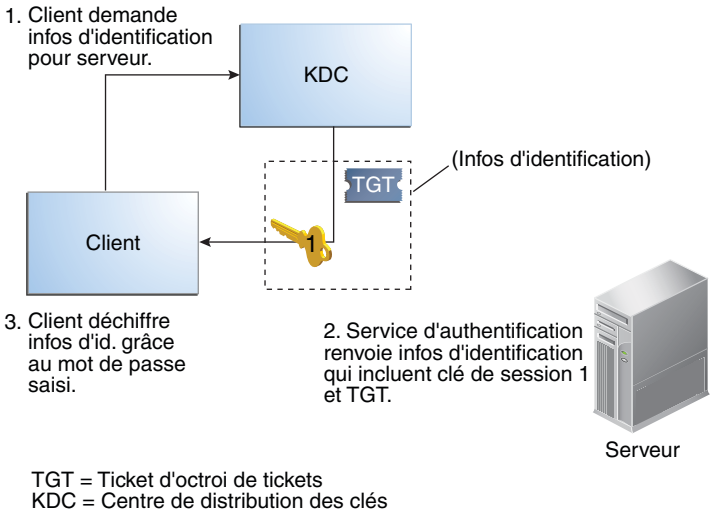
Obtention d'informations d'identification pour le service d'octroi de tickets

1. Pour démarrer le processus d'authentification, le client envoie une demande au serveur d'authentification pour un principal d'utilisateur spécifique. Cette demande est envoyée sans chiffrement. Aucune information sécurisée n'est incluse dans la demande, de sorte qu'il n'est pas nécessaire d'utiliser de chiffrement.
2. Lorsque la demande est reçue par le service d'authentification, le nom de principal de l'utilisateur est recherché dans la base de données KDC. Si un principal correspond à l'entrée dans la base de données, le service d'authentification obtient la clé privée pour ce principal. Le service d'authentification génère ensuite une clé de session utilisable par le client et le service d'octroi de tickets (appelez-la Session key 1) et un ticket pour le service d'octroi de tickets (Ticket 1). Ce ticket est également qualifié de *ticket d'octroi de tickets* (TGT). La clé de session et le ticket sont chiffrés à l'aide de la clé privée de l'utilisateur, et les informations sont renvoyées au client.
3. Le client utilise ces informations pour déchiffrer Session Key 1 et Ticket 1 à l'aide de la clé privée pour le principal de l'utilisateur. Comme la clé privée doit uniquement être connue de l'utilisateur et de la base de données KDC, les informations du paquet doivent être sécurisées. Le client stocke les informations dans le cache d'informations d'identification.

Au cours de ce processus, l'utilisateur est invité à saisir un mot de passe normalement. Si le mot de passe spécifié par l'utilisateur est le même que celui utilisé pour créer la clé privée stockée

dans la base de données KDC, alors le client peut déchiffrer les informations envoyées par le service d'authentification. Maintenant, le client dispose d'informations d'identification à utiliser avec le service d'octroi de tickets. Le client est prêt à demander des informations d'identification pour un serveur.

FIGURE 27–2 Obtention d'informations d'identification pour le service d'octroi de tickets



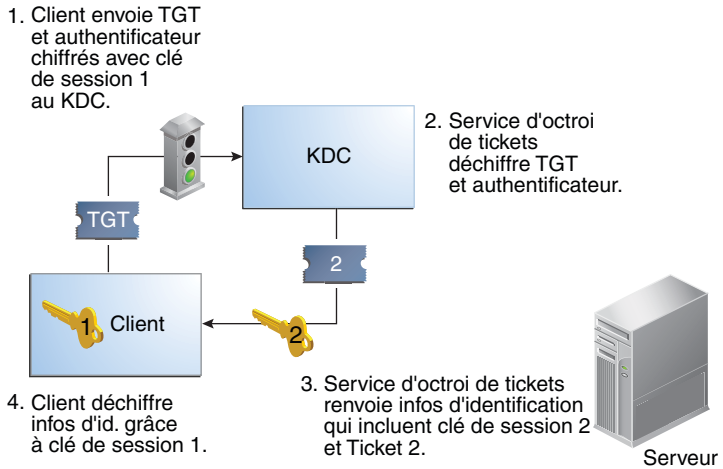
Obtention d'informations d'identification pour un serveur

1. Pour demander l'accès à un serveur spécifique, un client doit d'abord avoir obtenu des informations d'identification pour ce serveur à partir du service d'authentification. Reportez-vous à la section "Obtention d'informations d'identification pour le service d'octroi de tickets" à la page 581. Le client envoie ensuite une demande au service d'octroi de ticket, qui inclut le nom du principal de service, Ticket 1, et un authentificateur chiffré avec Session Key 1. Ticket 1 a été initialement chiffré par le service d'authentification à l'aide de la clé du service d'octroi de tickets.
2. Comme la clé de service du service d'octroi de tickets est connue du service d'octroi de tickets, Ticket 1 peut être déchiffré. Les informations de Ticket 1 comprennent Session Key 1, de sorte que le service d'octroi de tickets peut déchiffrer l'authentificateur. À ce stade, le principal de l'utilisateur est authentifié avec le service d'octroi de tickets.
3. Une fois l'authentification réussie, le service d'octroi de tickets génère une clé de session pour le principal de l'utilisateur et le serveur (Session Key 2), et un ticket pour le serveur (Ticket 2). Session Key 2 et Ticket 2 sont ensuite chiffrés à l'aide de Session Key 1. Étant

donné que Session Key 1 est uniquement connue du client et du service d'octroi de tickets, cette information est sécurisée et peut être envoyée sans problème sur le réseau.

4. Lorsque le client reçoit ce paquet d'informations, il déchiffre les informations en utilisant Session Key 1, qui était stockée dans le cache des informations d'identification. Le client dispose d'informations d'identification à utiliser avec le serveur. Maintenant, le client est prêt à demander l'accès à un service particulier sur ce serveur.

FIGURE 27–3 Obtention d'informations d'identification pour un serveur

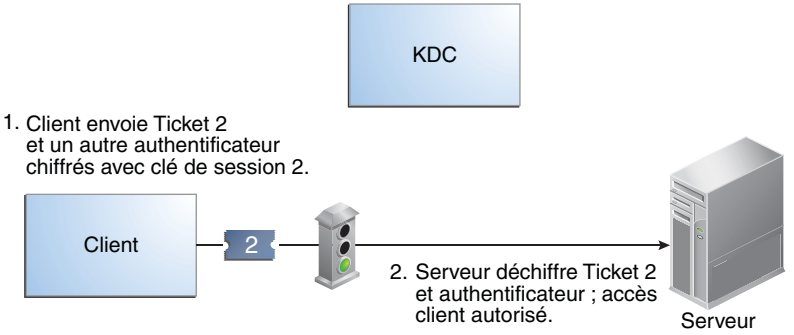


TGT = Ticket d'octroi de tickets
KDC = Centre de distribution des clés

Obtention de l'accès à un service donné

1. Pour demander l'accès à un service spécifique, le client doit d'abord avoir obtenu des informations d'identification pour le service d'octroi de tickets à partir du serveur d'authentification, et des informations d'identification de serveur à partir du service d'octroi de tickets. Reportez-vous aux sections "Obtention d'informations d'identification pour le service d'octroi de tickets" à la page 581 et "Obtention d'informations d'identification pour un serveur " à la page 582. Le client peut alors envoyer une demande au serveur en incluant Ticket 2 et un autre authentificateur. L'authentificateur est chiffré à l'aide de Session key 2.
2. Ticket 2 a été chiffré par le service d'octroi de tickets avec la clé de service pour le service. Étant donné que la clé de service est appelée par le principal de service, le service peut déchiffrer Ticket 2 et obtenir Session Key 2. Session Key 2 peut alors être utilisée pour déchiffrer l'authentificateur. Si l'authentificateur est correctement déchiffré, le client obtient l'accès au service.

FIGURE 27–4 Obtention de l'accès à un service donné



Utilisation des types de chiffrement Kerberos

Les types de chiffrement identifient les algorithmes cryptographiques et le mode à utiliser lors d'opérations cryptographiques. Les types de chiffrement `aes` , `des3-cbc-sha1` et `rc4–hmac` permettent de créer des clés à utiliser pour des opérations cryptographiques renforcées. Ces opérations renforcées améliorent la sécurité globale du service Kerberos.

Remarque – Dans les versions antérieures à la version Solaris 10 8/07, le type de chiffrement `aes256-cts-hmac-sha1-96` peut être utilisé avec le service Kerberos si les packages Strong Cryptographic non fournis en standard sont installés.

Lorsqu'un client demande un ticket au KDC, le KDC doit utiliser des clés dont le type de chiffrement est compatible à la fois avec le client et le serveur. Bien que le protocole Kerberos permette au client de demander à ce que le KDC utilise certains types de chiffrement pour la partie de réponse du ticket du client, le protocole n'autorise pas le serveur à spécifier des types de chiffrement au KDC.

Remarque – Si le KDC maître installé n'exécute pas la version Solaris10, le KDC esclave doit être mis à niveau vers la version Solaris10 avant de mettre à niveau le KDC maître. Un KDC maître Solaris10 utilise les nouveaux types de chiffrement, ce qu'un esclave plus ancien n'est pas en mesure de faire.

Le tableau suivant répertorie certains des problèmes à prendre en compte avant de modifier les types de chiffrement.

- Le KDC suppose que le premier key/enctype associé à l'entrée du serveur principal dans la base de données du principal est pris en charge par le serveur.

- Sur le KDC, vous devez vous assurer que les clés générées pour le principal sont compatibles avec les systèmes sur lesquels le principal sera authentifié. Par défaut, la commande `kadmin` crée des clés pour tous les types de chiffrement pris en charge. Si les systèmes sur lesquels le principal est utilisé ne prennent pas en charge cette configuration par défaut des types de chiffrement, vous devez restreindre les types de chiffrement lors de la création d'un principal. Vous pouvez limiter les types de chiffrement par l'intermédiaire de l'indicateur `-e` dans `kadmin addprinc` ou en définissant le paramètre `supported_enctypes` dans le fichier `kdc.conf` sur ce sous-ensemble. Le paramètre `supported_enctypes` doit être utilisé lorsque la plupart des systèmes d'un domaine Kerberos prennent en charge un sous-ensemble de l'ensemble par défaut des types de chiffrement. Le paramètre `supported_enctypes` spécifie l'ensemble par défaut des types de chiffrement utilisés par `kadmin addprinc` lorsqu'il crée un principal pour un domaine particulier. En règle générale, il est préférable de contrôler les types de chiffrement utilisés par Kerberos à l'aide de l'une de ces deux méthodes.
- Au moment de déterminer les types de chiffrement pris en charge par un système, pensez à la fois à la version de Kerberos exécutée sur le système et aux algorithmes cryptographiques pris en charge par l'application du serveur pour lequel un principal de serveur est en cours de création. Par exemple, lorsque vous créez un principal de service `nfs/hostname`, il est conseillé de limiter les types de chiffrement aux types pris en charge par le serveur NFS de l'hôte. Notez que dans la version Solaris10, tous les types de chiffrement Kerberos pris en charge le sont également par le serveur NFS.
- Le paramètre `master_key_enctype` dans le fichier `kdc.conf` peut être utilisé pour contrôler le type de chiffrement de la clé principale qui chiffre les entrées dans la base de données du principal. N'utilisez pas ce paramètre si la base de données du principal KDC a déjà été créée. Le paramètre `master_key_enctype` peut être utilisé au moment de la création de la base de données afin de faire passer le type de chiffrement de la clé principale par défaut de `des-cbc-crc` à un type de chiffrement supérieur. Assurez-vous que tous les KDC esclaves prennent en charge le type de chiffrement choisi et qu'ils ont la même entrée `master_key_enctype` dans leur `kdc.conf` lorsque vous configurez les KDC esclaves. Assurez-vous également que le paramètre `master_key_enctype` est défini sur l'un des types de chiffrement dans `supported_enctypes`, si `supported_enctypes` est défini dans `kdc.conf`. Si l'une ou l'autre de ces situations n'est pas gérée correctement, le KDC maître peut ne pas être en mesure de travailler avec le KDC esclave.
- Sur le client, vous pouvez contrôler les types de chiffrement demandés par le client lors de l'obtention de tickets du KDC par le biais de quelques paramètres dans `krb5.conf`. Le paramètre `default_tkt_enctypes` spécifie les types de chiffrement que le client est disposé à utiliser lorsqu'il demande un ticket d'octroi de tickets (TGT) au KDC. Le TGT est utilisé par le client pour acquérir d'autres tickets de serveur d'une manière plus efficace. L'effet du paramètre `default_tkt_enctypes` est de donner au client un contrôle sur les types de chiffrement utilisés pour protéger les communications entre le client et le KDC, lorsque le client demande un ticket de serveur via TGT (aussi appelé demande TGS). Notez que les types de chiffrement spécifiés dans `default_tkt_enctypes` doivent correspondre à au moins l'un des types de chiffrement de clé du principal dans la base de données du principal stockée sur le KDC. Dans le cas contraire, la demande TGS échoue. Dans la plupart des cas,

il est préférable de ne pas définir `default_tkt_enctypes` car ce paramètre peut être une source de problèmes d'interopérabilité. Par défaut, le code client demande tous les types de chiffrement pris en charge et le KDC choisit les types de chiffrement en fonction des clés que le KDC trouve dans la base de données du principal.

- Le paramètre `default_tgs_enctypes` restreint les types de chiffrement demandés par le client dans ses demandes TGS, qui sont utilisés pour l'acquisition de tickets de serveur. Ce paramètre restreint également les types de chiffrement utilisés par le KDC lors de la création de la clé de session partagée par le client et le serveur. Par exemple, si un client souhaite utiliser uniquement le chiffrement 3DES pour un NFS sécurisé, vous devez définir `default_tgs_enctypes` = `des3-cbc-sha1`. Assurez-vous que les principaux du client et du serveur ont une clé `des-3-cbc-sha1` dans la base de données du principal. Comme avec `default_tkt_enctype`, il est sans doute préférable dans la plupart des cas de ne pas définir ce paramètre, car il peut provoquer des problèmes d'interopérabilité si les informations d'identification ne sont pas configurées correctement sur le KDC et le serveur.
- Sur le serveur, vous pouvez contrôler les types de chiffrement acceptés par le serveur avec le paramètre `permitted_enctypes` de `kdc.conf`. De plus, vous pouvez spécifier les types de chiffrement utilisés lors de la création d'entrées `keytab`. Encore une fois, il est généralement préférable de ne pas utiliser l'une de ces méthodes pour contrôler les types de chiffrement et de laisser le KDC déterminer les types de chiffrement à utiliser, car le KDC ne communique pas avec l'application de serveur pour déterminer la clé ou le type de chiffrement à utiliser.

Utilisation de la table `gsscred`

La table `gsscred` est utilisée par un serveur NFS lorsque le serveur tente d'identifier un utilisateur Kerberos, si les mappages par défaut ne sont pas suffisants. Le service NFS utilise des ID UNIX pour identifier les utilisateurs. Ces ID ne font pas partie d'un principal ou d'informations d'identification d'utilisateur. La table `gsscred` assure le mappage supplémentaires d'informations d'identification GSS aux UID UNIX (à partir du fichier de mots de passe). La table doit être créée et administrée une fois que la base de données KDC est remplie. Pour plus d'informations, reportez-vous à la section “Mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 420.

Lorsqu'une demande de client arrive, le service NFS tente de faire correspondre le nom des informations d'identification avec un ID UNIX. Si le mappage échoue, la table `gsscred` vérifiée.

Différences notables entre Oracle Solaris Kerberos et MIT Kerberos

La version Solaris10 du service Kerberos est basée sur la version 1.2.1 de MIT Kerberos. Le tableau suivant répertorie les améliorations incluses dans la version Solaris10 et pas dans la version MIT 1.2.1:

- Prise en charge par Kerberos des applications distantes Oracle Solaris
- Propagation incrémentielle pour la base de données KDC
- Script de configuration client
- Messages d'erreur localisés
- Prise en charge des enregistrements d'audit BSM
- Utilisation à thread sécurisé de Kerberos par le biais de l'API GSS
- Utilisation de la structure de chiffrement pour la cryptographie

Cette version comprend également certaines corrections de bogues post-MIT 1.2.1. En particulier, les corrections de bogues btree 1.2.5 et l'ajout de la prise en charge du 1.3 TCP ont été ajoutés.

PARTIE VII

Audit Oracle Solaris

Cette section fournit des informations sur la configuration, la gestion et l'utilisation du sous-système d'audit Oracle Solaris.

◆ ◆ ◆ CHAPITRE 28

Audit Oracle Solaris (présentation)

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

Ce chapitre présente le fonctionnement de l'audit dans Oracle Solaris. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour obtenir des suggestions de planification, reportez-vous au Chapitre 29, "Planification de l'audit Oracle Solaris". Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au Chapitre 30, "Gestion de l'audit Oracle Solaris (tâches) ". Pour obtenir des informations de référence, reportez-vous au Chapitre 31, "Audit Oracle Solaris (référence) ".

Description de l'audit

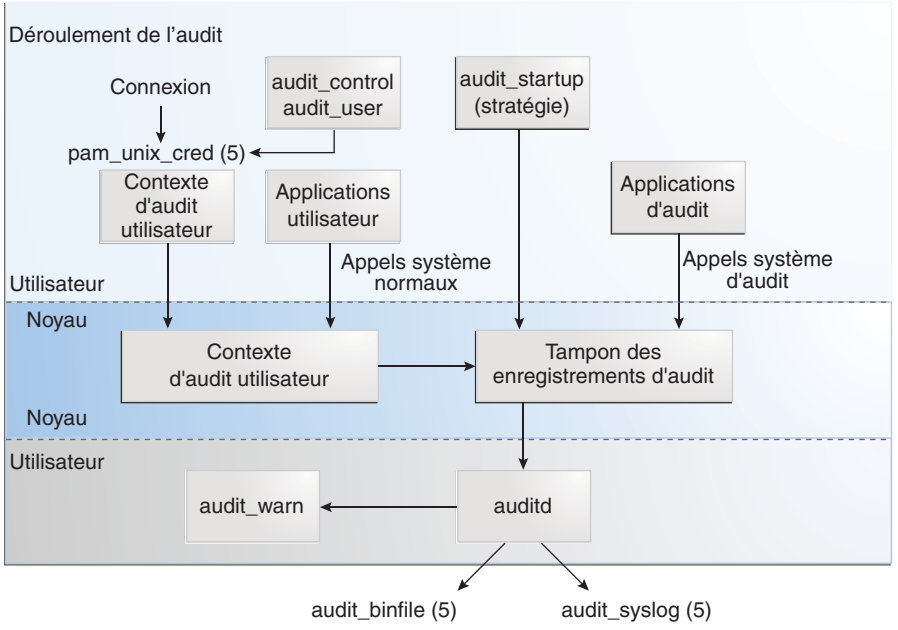
L'audit consiste à collecter des données sur l'utilisation des ressources système. Les données d'audit fournissent un enregistrement des événements système ayant trait à la sécurité. Ces données peuvent ensuite être utilisées pour déterminer la responsabilité quant aux actions survenant sur un hôte. Un audit réussi commence par deux fonctions de sécurité : identification et authentification. À chaque connexion, une fois qu'un utilisateur fournit un nom d'utilisateur et un mot de passe, un ID de session d'audit unique est généré et associé au processus de l'utilisateur. L'ID de session d'audit est hérité par tous les processus démarrés au cours de la session de connexion. Même si un utilisateur change d'identité au cours d'une session, toutes ses actions sont suivies avec le même ID de session d'audit. Pour plus d'informations sur le changement d'identité, reportez-vous à la page de manuel su(1M).

Le service d'audit effectue les opérations suivantes :

- Surveillance des événements liés à la sécurité survenant sur l'hôte
- Enregistrement des événements dans une piste d'audit à l'échelle du réseau
- Détection des utilisations inappropriées et des activités non autorisées
- Examen des modèles d'accès et des historiques d'accès des individus et des objets
- Identification des tentatives de contournement des mécanismes de protection
- Détection de l'utilisation étendue d'un privilège survenant lorsqu'un utilisateur change d'identité

Lors de la configuration du système, vous présélectionnez les classes d'enregistrements d'audit à surveiller. Vous pouvez également régler le degré de l'audit effectué pour chaque utilisateur. La figure ci-dessous présente les détails du flux d'audit Oracle Solaris.

FIGURE 28–1 Flux d'audit



Une fois les données d'audit collectées dans le noyau, les plug-ins distribuent les données aux emplacements appropriés. Par la suite, les outils de post-sélection vous permettent de réduire et d'examiner des parties intéressantes de la piste d'audit. Par exemple, vous pouvez choisir de passer en revue les enregistrements d'audit pour chaque utilisateur ou pour des groupes

spécifiques. Vous pouvez examiner tous les enregistrements d'un certain type d'événement un jour donné. Ou bien, vous pouvez sélectionner les enregistrements générés à une certaine heure de la journée.

Les systèmes qui installent des zones non globales peuvent auditer toutes les zones de la même façon que la zone globale. Ces systèmes peuvent également être configurés pour collecter différents enregistrements dans les zones non globales. Pour plus d'informations, reportez-vous à la section "Audit et zones Oracle Solaris" à la page 684.

Fonctionnement de l'audit

L'audit génère des enregistrements d'audit lorsque des événements donnés se produisent. Le plus souvent, les événements générant des enregistrements d'audit sont les suivants :

- Démarrage et arrêt du système
- Connexion et déconnexion
- Création ou destruction de processus et création ou destruction de threads
- Ouverture, fermeture, création, destruction, ou modification du nom d'objets
- Utilisation des capacités de privilège ou du contrôle d'accès basé sur les rôles (RBAC)
- Actions d'identification et d'authentification
- Modification d'autorisations par un processus ou un utilisateur
- Actions d'administration, telles que l'installation d'un package
- Applications spécifiques à un site

Les enregistrements d'audit sont générés à partir de trois sources :

- Par une application
- À la suite d'un événement d'audit asynchrone
- À la suite d'un appel système de processus

Une fois les informations de l'événement recueillies, elles sont formatées en un enregistrement d'audit. L'enregistrement est ensuite écrit dans les fichiers d'audit. Les enregistrements d'audit complets sont stockés au format binaire. Dans la version Solaris10, les enregistrements d'audit peuvent également être consignés par l'utilitaire `syslog`.

Les fichiers d'audit au format binaire peuvent être stockés dans un système de fichiers local. Les fichiers peuvent également être stockés sur des serveurs de fichiers montés via NFS. L'emplacement peut inclure plusieurs partitions sur le même système, des partitions sur des systèmes différents ou des partitions sur des systèmes basés sur des réseaux différents mais reliés. L'ensemble des fichiers d'audit liés est considéré comme une *piste d'audit*. Les enregistrements d'audit s'accumulent dans des fichiers d'audit dans l'ordre chronologique. Chaque enregistrement d'audit contient des informations qui identifient l'événement, la cause, l'heure et d'autres informations pertinentes.

Les enregistrements d'audit peuvent également être surveillés à l'aide de l'utilitaire `syslog`. Ces journaux d'audit peuvent être stockés localement. Ou, les journaux peuvent être envoyés à un système distant via le protocole UDP. Pour plus d'informations, reportez-vous à la section "Journaux d'audit" à la page 599.

Rapports entre l'audit et la sécurité

L'audit Oracle Solaris permet de détecter des violations de sécurité potentielles en révélant des modèles suspects ou anormaux d'utilisation du système. L'audit Oracle Solaris offre également un moyen de suivre des actions suspectes, permettant ainsi de remonter à un utilisateur particulier, ce qui a un effet dissuasif. Lorsque les utilisateurs savent que leurs activités sont auditées, ils sont moins susceptibles de tenter des activités malveillantes.

La protection d'un système informatique, en particulier d'un système sur réseau, requiert des mécanismes permettant de contrôler des activités avant que les processus système ou les processus utilisateur ne commencent. La sécurité nécessite des outils permettant de surveiller les activités lorsque celles-ci se produisent. La sécurité requiert également des rapports d'activités après que les activités ont eu lieu. La configuration initiale de l'audit Oracle Solaris requiert que les paramètres soient définis avant que les utilisateurs ne se connectent ou que des processus système ne commencent. La plupart des activités d'audit impliquent de surveiller des événements courants et d'établir des rapports sur les événements correspondant aux paramètres spécifiés. La manière dont l'audit Oracle Solaris surveille les événements et génère des rapports est traitée de manière détaillée dans le Chapitre 29, "Planification de l'audit Oracle Solaris" et le Chapitre 30, "Gestion de l'audit Oracle Solaris (tâches) ".

L'audit ne peut pas empêcher les pirates d'entrer dans le système de manière non autorisée. Cependant, le service d'audit permet par exemple de générer des rapports indiquant qu'un utilisateur spécifique a effectué certaines actions à une heure et une date données. Le rapport d'audit peut identifier l'utilisateur par le biais du chemin d'entrée et du nom de l'utilisateur. Ces informations peuvent être envoyées immédiatement à votre terminal et signalées dans un fichier pour une analyse ultérieure. Par conséquent, le service d'audit fournit des données permettant de déterminer les éléments suivants :

- La manière dont la sécurité du système a été compromise.
- Les brèches à combler pour assurer le niveau de sécurité souhaité.

Terminologie et concept de l'audit

Les termes suivants sont utilisés pour décrire le service d'audit. Certaines définitions incluent des pointeurs vers des descriptions plus complètes.

TABLEAU 28–1 Termes liés à l'audit Oracle Solaris

Terme	Définition
Classe d'audit	Groupe d'événements d'audit. Les classes d'audit permettent de sélectionner un groupe d'événements à auditer. Pour plus d'informations, reportez-vous à la section "Classes d'audit et présélection" à la page 597.
Répertoire d'audit	Référentiel de fichiers d'audit au format binaire. Pour une description des différents types de répertoires d'audit, reportez-vous à la section "Journaux d'audit" à la page 599.
Événement d'audit	Action du système ayant trait à la sécurité et faisant l'objet de l'audit. Pour faciliter la sélection, les événements sont regroupés en classes d'audit. Pour une description des actions pouvant être auditées, reportez-vous à la section "Événements d'audit" à la page 596.
Stratégie d'audit	Ensemble d'options d'audit que vous pouvez activer ou désactiver sur votre site. Ces options permettent notamment d'indiquer si certains types de données d'audit doivent être enregistrées ou pas. Les options permettent aussi de préciser si les actions auditables doivent être suspendues ou pas lorsque la piste d'audit est pleine. Pour plus d'informations, reportez-vous à la section "Détermination de la stratégie d'audit" à la page 611.
Enregistrement d'audit	Données d'audit stockées dans les fichiers d'audit. Un enregistrement d'audit décrit un événement d'audit unique. Chaque enregistrement d'audit est constitué de jetons d'audit. Pour plus d'informations sur les enregistrements d'audit, reportez-vous à la section "Enregistrements d'audit et jetons d'audit" à la page 598.
Jeton d'audit	Champ d'un enregistrement ou événement d'audit. Chaque jeton d'audit décrit un attribut d'un événement d'audit, tel qu'un utilisateur, un programme ou un autre objet. Pour une description de tous les jetons d'audit, reportez-vous à la section "Formats de jeton d'audit " à la page 692.
Piste d'audit	Ensemble composé d'un ou plusieurs fichiers d'audit et stockant les données d'audit de tous les systèmes exécutant le service d'audit. Pour plus d'informations, reportez-vous à la section "Piste d'audit " à la page 689.
Présélection	La présélection consiste à sélectionner les classes d'audit à surveiller avant d'activer le service d'audit. Les événements d'audit des classes d'audit présélectionnées apparaissent dans la piste d'audit. Les classes d'audit non présélectionnées ne sont pas auditées. Les événements correspondants n'apparaissent donc pas dans la piste d'audit. Un outil de postsélection, la commande `auditreduce`, sélectionne des enregistrements dans la piste d'audit. Pour plus d'informations, reportez-vous à la section "Classes d'audit et présélection" à la page 597.
Objets publics	Un objet public est un fichier appartenant à l'utilisateur `root` et lisible par tout le monde. Par exemple, les fichiers des répertoires `/etc` et `/usr/bin` sont des objets publics. Les objets publics ne font plus l'objet d'audit pour des événements en lecture seule. Par exemple, même si la classe d'audit `file_read` (`fr`) est présélectionnée, la lecture des objets publics n'est pas auditée. Vous pouvez remplacer la valeur par défaut en modifiant l'option de stratégie d'audit `public`.

TABLEAU 28–1 Termes liés à l'audit Oracle Solaris *(Suite)*

Terme	Définition
Plug-ins d'audit	Modules transférant les enregistrements d'audit dans la file d'attente du noyau vers un emplacement indiqué. Le plug-in `audit_binfile.so` crée des fichiers d'audit binaires (la piste d'audit). Le plug-in `audit_syslog.so` filtre les enregistrements d'audit sélectionnés dans les journaux `syslog`. Pour plus d'informations, reportez-vous à la section "Modules plug-in d'audit " à la page 599.

Événements d'audit

Les actions système ayant trait à la sécurité peuvent être auditées. Ces actions auditables sont qualifiées d'*événements d'audit*. Les événements d'audit sont répertoriés dans le fichier `/etc/security/audit_event` . Chaque événement d'audit est défini dans le fichier par un numéro, un nom symbolique, une brève description et l'ensemble des classes d'audit auxquelles il appartient. Pour plus d'informations sur le fichier `audit_event`, reportez-vous à la page de manuel `audit_event(4)`.

Par exemple, l'entrée suivante définit l'événement d'audit pour l'appel système `exec()` :

```
7:AUE_EXEC:exec(2):ps,ex
```

Lorsque vous présélectionnez la classe d'audit `ps` ou `ex` pour l'audit, les appels système `exec()` sont enregistrés dans la piste d'audit.

L'audit Oracle Solaris gère les événements *attribuables* et *non attribuables* . La stratégie d'audit répartit les événements en événements *synchrones* et *asynchrones* de la manière suivante :

- **Événements attribuables** : événements pouvant être attribués à un utilisateur. L'appel système `exec()` peut être attribué à un utilisateur, de sorte que l'appel est considéré comme un événement attribuable. Tous les événements attribuables sont des événements synchrones.
- **Événements non attribuables** : événements se produisant au niveau d'interruption du noyau ou avant l'authentification d'un utilisateur. La classe d'audit `na` gère les événements d'audit non attribuables. Par exemple, l'initialisation du système est un événement non attribuable. La plupart des événements non attribuables sont des événements asynchrones. Cependant, les événements non attribuables dotés de processus associés, tels qu'un échec de connexion, sont des événements synchrones.
- **Événements synchrones** : événements associés à un processus dans le système. Les événements synchrones constituent la majorité des événements système.
- **Événements asynchrones** : événements associés à aucun processus, de sorte qu'aucun processus ne peut être bloqué puis réactivé ultérieurement. Le démarrage système initial et les événements d'entrée et de sortie PROM sont des exemples d'événements asynchrones.

Lorsque la classe à laquelle un événement d'audit appartient est présélectionnée pour l'audit, l'événement est enregistré dans la piste d'audit. Par exemple, lorsque vous présélectionnez les classes d'audit `ps` et `na` pour l'audit, les appels système `exec()` et les actions d'initialisation du système, entre autres événements, sont enregistrés dans la piste d'audit.

Outre les événements d'audit définis par le service d'audit Oracle Solaris, des événements d'audit peuvent également être générés par des applications tierces. Les numéros d'événements d'audit compris entre 32768 et 65535 sont disponibles pour les applications tierces.

Classes d'audit et présélection

Chaque événement d'audit appartient à une ou plusieurs *classes d'audit*. Les classes d'audit sont des conteneurs pratiques pour les grands nombres d'événements d'audit. Lorsque vous *présélectionnez* une classe à auditer, vous spécifiez que tous les événements de cette classe doivent être enregistrés dans la piste d'audit. Vous pouvez effectuer une présélection pour des événements sur un système et pour des événements initiés par un utilisateur particulier. Une fois le service d'audit en cours d'exécution, vous pouvez ajouter de façon dynamique des classes d'audit à la présélection, ou en supprimer.

- **Présélection système** : spécifie des valeurs par défaut à l'échelle du système pour l'audit des lignes `flags`, `naflags` et `plugin` du fichier `audit_control`. Le fichier `audit_control` est décrit à la section "Fichier `audit_control`" à la page 678. Reportez-vous également à la page de manuel `audit_control(4)`.
- **Présélection utilisateur** : spécifie des ajouts aux valeurs par défaut du contrôle système pour des utilisateurs individuels dans la base de données `audit_user`.

  Le masque de présélection d'audit détermine les classes d'événements auditées pour un utilisateur. Le masque de présélection d'audit de l'utilisateur est une combinaison de valeurs système par défaut et de classes d'audit spécifiées pour l'utilisateur. Pour plus d'informations, reportez-vous à la section "Caractéristiques de l'audit des processus" à la page 689.

  La base de données `audit_user` peut être gérée localement ou par un service de nommage. La console de gestion Solaris fournit l'interface graphique pour l'administration de la base de données. Pour plus d'informations, reportez-vous à la page de manuel `audit_user(4)`.
- **Présélection dynamique** : spécifie des classes d'audit en tant qu'arguments à la commande `auditconfig` pour ajouter ou supprimer ces classes d'audit d'un processus ou d'une session. Pour plus d'informations, reportez-vous à la page de manuel `auditconfig(1M)`.

Une commande de postsélection, `auditreduce`, vous permet de sélectionner des enregistrements parmi les enregistrements d'audit présélectionnés. Pour plus d'informations, reportez-vous à la section "Examen de la piste d'audit" à la page 601 et à la page de manuel `auditreduce(1M)`.

Les classes d'audit sont définies dans le fichier `/etc/security/audit_class`. Chaque entrée contient le masque d'audit pour la classe, le nom de la classe et un nom descriptif de la classe. Par exemple, les définitions de classe `ps` et `na` s'affichent dans le fichier `audit_class` comme suit :

```
0x00100000:ps:process start/stop
0x00000400:na:non-attribute
```

Il existe 32 classes d'audit possibles. Les classes comprennent les deux classes globales : `all` et `no`. Les classes d'audit sont décrites à la page de manuel `audit_class(4)`.

Le mappage entre les événements d'audit et les classes peut être configuré. Vous pouvez supprimer des événements à partir d'une classe, ajouter des événements à une classe et créer une nouvelle classe destinée à contenir des événements sélectionnés. Pour plus d'informations sur cette procédure, reportez-vous à la section "Modification de l'appartenance à une classe d'un événement d'audit" à la page 629.

Enregistrements d'audit et jetons d'audit

Chaque *enregistrement d'audit* consigne l'occurrence d'un seul événement audité. L'enregistrement inclut des informations telles que l'auteur de l'action, les fichiers affectés, l'action tentée, ainsi que l'endroit et l'heure à laquelle l'action s'est produite. L'exemple suivant montre un enregistrement d'audit `login` :

```
header,81,2,login - local,,2003-10-13 11:23:31.050 -07:00
subject,root,root,other,root,other,378,378,0 0 example_system
text,successful login
return,success,0
```

Le type d'informations enregistrées pour chaque événement d'audit est défini par un ensemble de *jetons d'audit*. Chaque fois qu'un enregistrement d'audit est créé pour un événement, l'enregistrement contient certains ou tous les jetons définis pour l'événement. La nature de l'événement détermine quels jetons sont enregistrés. Dans l'exemple ci-dessus, chaque ligne commence par le nom du jeton d'audit. Le contenu du jeton d'audit suit le nom. Ensemble, les quatre jetons d'audit comprennent l'enregistrement d'audit `login`.

Pour une description détaillée de la structure de chaque jeton d'audit avec un exemple de sortie `praudit`, reportez-vous à la section "Formats de jeton d'audit " à la page 692. Pour une description du flux binaire des jetons d'audit, reportez-vous à la page de manuel `audit.log(4)`.

Modules plug-in d'audit

Vous pouvez spécifier des modules plug-in d'audit pour gérer les enregistrements placés par votre présélection dans la file d'attente d'audit. Les plug-ins sont des entrées du fichier `audit_control`.

- Plug-in `audit_binfile.so` : gère la distribution de la file d'attente d'audit aux fichiers d'audit binaires. Dans le fichier `audit_control`, si aucun plug-in n'est spécifié et l'entrée `dir` a une valeur, alors le démon d'audit utilise ce plug-in.
- Plug-in `audit_syslog.so` : gère la distribution d'enregistrements sélectionnés de la file d'attente d'audit aux journaux `syslog`.

La syntaxe du fichier `audit_control` est décrite à la page de manuel `audit_control(4)`. Pour consulter des exemples, reportez-vous aux tâches dans la section "Configuration des fichiers d'audit (liste des tâches) " à la page 620.

Pour plus d'informations sur les plug-ins, reportez-vous aux pages de manuel `audit_binfile(5)`, `audit_syslog(5)` et `audit_control(4)`.

Journaux d'audit

Les enregistrements d'audit sont collectés dans des journaux d'audit. L'audit Oracle Solaris fournit deux modes de sortie pour les journaux d'audit. Les journaux appelés *fichiers d'audit* stockent des enregistrements d'audit au format binaire. L'ensemble des fichiers d'audit d'un système ou d'un site constitue un enregistrement d'audit complet. L'enregistrement d'audit complet est appelé la *piste d'audit*.

L'utilitaire `syslog` collecte et stocke des résumés d'enregistrements d'audit en version texte. Un enregistrement `syslog` n'est pas complet. L'exemple suivant montre une entrée `syslog` pour un d'enregistrement d'audit `login` :

```
Oct 13  11:24:11 example_system auditd: [ID 6472 audit.notice] \
        login - login ok session 378 by root as root:other
```

Un site peut stocker des enregistrements d'audit dans les deux formats. Vous pouvez configurer les systèmes de votre site afin d'utiliser le mode binaire, le mode `syslog` ou les deux modes. Le tableau suivant compare les enregistrements d'audit binaires et les enregistrements `syslog`.

TABLEAU 28–2 Comparaison d'enregistrements d'audit binaires aux enregistrements d'audit `syslog`.

Fonctionnalité	Enregistrements binaires	Enregistrements `syslog`
Protocole	Écrit dans le système de fichiers	Utilise UDP pour la connexion à distance
Type de données	Binaire	Texte

TABLEAU 28–2 Comparaison d'enregistrements d'audit binaires aux enregistrements d'audit `syslog`. *(Suite)*

Fonctionnalité	Enregistrements binaires	Enregistrements `syslog`
Longueur d'enregistrement	Aucune limite	Jusqu'à 1024 caractères par enregistrement d'audit
Emplacement	Stockés sur le disque local et dans les répertoires montés à l'aide de NFS	Stockés dans un emplacement spécifié dans le fichier `syslog.conf`
Configuration	Modifie le fichier `audit_control` et protège et monte les répertoires d'audit via NFS	Modifie le fichier `audit_control` et le fichier `syslog.conf`
Lecture	En règle générale, en mode batch Sortie navigateur en XML	En temps réel, ou recherché par des scripts que vous avez créés pour `syslog` Sortie en texte brut
Exhaustivité	Exhaustivité garantie et affichage dans l'ordre approprié	Exhaustivité non garantie
Horodatage	Heure moyenne de Greenwich (GMT)	Heure du système audité

Des enregistrements binaires offrent la plus grande sécurité et la meilleure couverture. La sortie binaire répond aux exigences de certifications de sécurité, telles que les critères communs du profil de protection Accès contrôlé (CAPP). Les enregistrements sont écrits dans un système de fichiers protégé contre le vol. Sur un seul système, tous les enregistrements binaires sont collectés et affichés dans l'ordre. L'horodatage GMT dans les journaux binaires permet une comparaison exacte lorsque des systèmes d'une piste d'audit sont répartis entre différents fuseaux horaires. La commande `praudit -x` vous permet de visualiser les enregistrements dans un navigateur au format XML. Vous pouvez également utiliser des scripts pour analyser la sortie XML.

En revanche, les enregistrements `syslog` garantissent une plus grande commodité et flexibilité. Par exemple, vous pouvez collecter les données `syslog` à partir de plusieurs sources. En outre, lorsque vous surveillez des événements `audit.notice` dans le fichier `syslog.conf`, l'utilitaire `syslog` consigne un résumé des enregistrements d'audit avec l'horodatage actuel. Vous pouvez utiliser les mêmes outils d'analyse et de gestion que vous avez développés pour les messages `syslog` à partir de plusieurs sources, y compris les stations de travail, serveurs, pare-feux et routeurs. Les enregistrements peuvent être affichés en temps réel et stockés sur un système distant.

En utilisant `syslog.conf` pour stocker des enregistrements d'audit à distance, vous protégez les données du journal contre toute altération ou suppression malveillante. D'autre part, lorsque les enregistrements d'audit sont stockés à distance, ceux-ci sont susceptibles de faire l'objet d'attaques réseau, telles que le déni de service et l'usurpation d'adresses source. En outre, UDP peut couper des paquets ou les distribuer dans le désordre. Le nombre limite de caractères pour les entrées `syslog` est de 1024, de sorte que certains enregistrements d'audit peuvent être

tronqués dans le journal. Sur un système, tous les enregistrements d'audit ne sont pas collectés. Les enregistrements peuvent ne pas s'afficher dans l'ordre. Dans la mesure où chaque enregistrement d'audit est indiqué avec la date et l'heure du système local, vous ne pouvez pas vous baser sur l'horodatage pour construire une piste d'audit pour plusieurs systèmes.

Pour plus d'informations sur les journaux d'audit, reportez-vous à :

- la page de manuel `audit_syslog`(5)
- la page de manuel `audit.log`(4)
- "Configuration des journaux d'audit `syslog` " à la page 623

Stockage de la piste d'audit

Un *répertoire d'audit* contient des fichiers d'audit au format binaire. L'installation standard utilise de nombreux répertoires d'audit. Le contenu de tous les répertoires d'audit constitue la *piste d'audit*. Les enregistrements d'audit sont stockés dans des répertoires d'audit selon l'ordre suivant :

- **Répertoire d'audit principal** : répertoire dans lequel les fichiers d'audit d'un système sont placés dans des conditions normales d'utilisation.
- **Répertoire d'audit secondaire** : répertoire dans lequel les fichiers d'audit d'un système sont placés si le répertoire d'audit principal est plein ou pas disponible.
- **Répertoire de dernier recours** : répertoire d'audit local utilisé si le répertoire d'audit principal et tous les répertoires d'audit secondaires ne sont pas disponibles.

Les répertoires sont spécifiés dans le fichier `audit_control`. Un répertoire n'est pas utilisé tant qu'un répertoire occupant une position supérieure dans la liste n'est pas plein. Pour obtenir un fichier `audit_control` annoté avec une liste des entrées de répertoire, reportez-vous à l'Exemple 30–3.

Placer les fichiers d'audit dans le répertoire root d'audit par défaut facilite la tâche du réviseur lors de l'examen de la piste d'audit. La commande `auditreduce` utilise le répertoire root d'audit pour rechercher tous les fichiers de la piste d'audit. Le répertoire root d'audit par défaut est `/etc/security/audit`. Ce répertoire est symboliquement lié à `/var/audit`. Les fichiers d'audit se trouvant dans les répertoires nommés `/var/audit/` *hostname*`/files` sont facilement localisés par la commande `auditreduce`. Pour plus d'informations, reportez-vous à la section "Commande `auditreduce`" à la page 673.

Examen de la piste d'audit

Le service d'audit fournit des commandes pour combiner et réduire les fichiers de la piste d'audit. La commande `auditreduce` peut fusionner des fichiers d'audit de la piste d'audit. La commande peut également filtrer les fichiers pour localiser des événements particuliers. La commande `praudit` lit les fichiers binaires. Les options de la commande `praudit` fournissent une sortie adaptée pour l'écriture de scripts et l'affichage dans le navigateur.

Audit sur un système à zones Oracle Solaris

Une zone non globale représente un environnement virtualisé du système d'exploitation, créé dans une seule instance du SE Oracle Solaris. Le service d'audit contrôle le système dans sa totalité, y compris les activités dans les zones. Un système doté de zones non globales peut exécuter un service d'audit pour contrôler toutes les zones de manière identique. Il peut également configurer un service d'audit par zone, incluant la zone globale.

Les sites remplissant les conditions suivantes peuvent exécuter un service d'audit unique :

- Le site nécessite une piste d'audit à image unique.
- Les zones non globales sont utilisées en tant que conteneurs d'applications. Les zones font partie d'un même domaine d'administration. C'est-à-dire qu'aucune zone non globale ne dispose de fichiers de service de nommage personnalisé.

  Si toutes les zones d'un système se trouvent à l'intérieur d'un domaine d'administration, la stratégie d'audit `zonename` peut être utilisée afin de distinguer les événements d'audit s'exécutant dans différentes zones.
- Les administrateurs d'audit souhaitent maintenir un temps système d'audit faible. L'administrateur de la zone globale audite toutes les zones de manière identique. En outre, le démon d'audit de la zone globale dessert toutes les zones du système.

Les sites remplissant les conditions suivantes peuvent exécuter un service d'audit par zone :

- Le site ne nécessite pas de piste d'audit à image unique.
- Les zones non globales disposent de fichiers de service de nommage personnalisé. Ces différents domaines administratifs fonctionnent généralement comme des serveurs.
- Des administrateurs de zones particulières souhaitent contrôler l'audit dans les zones qu'ils gèrent. En procédant à un audit par zone, les administrateurs de zones peuvent décider d'activer ou de désactiver l'audit de la zone qu'ils gèrent.

Les avantages de l'audit par zone sont la fourniture d'une piste d'audit personnalisée pour chaque zone et la possibilité de désactiver l'audit en fonction de la zone. En revanche, ces avantages peuvent impliquer un temps système d'administration. L'administrateur de zone personnalise chaque fichier de configuration d'audit. Chaque zone exécute son propre démon d'audit et possède sa propre file d'attente d'audit et ses journaux d'audit. Les fichiers journaux de l'audit de zones doivent être gérés.

Améliorations apportées à l'audit dans la version Solaris10.

Les fonctionnalités d'audit suivantes ont été introduites dans la version Solaris 9 :

- L'audit peut utiliser l'utilitaire `syslog` pour stocker les enregistrements d'audit au format texte. Pour plus d'informations, reportez-vous à la section "Journaux d'audit" à la page 599. Pour configurer le fichier `audit_control` de sorte qu'il utilise l'utilitaire `syslog`, reportez-vous à la section "Configuration des journaux d'audit `syslog` " à la page 623.
- La commande `praudit` dispose d'un format de sortie supplémentaire, le XML. XML est un format standard, portable et exploitable. Ce format permet de lire la sortie dans un navigateur et fournit la source des scripts XML pour les rapports. L'option `-x` de la commande `praudit` est décrite dans la section "Commande `praudit`" à la page 675.
- L'ensemble des classes d'audit par défaut a été restructuré. Les métaclasses d'audit prennent en charge des classes d'audit plus spécifiques. Pour obtenir une liste de l'ensemble par défaut des classes, reportez-vous à la section "Définition de classes d'audit" à la page 685.
- La commande `bsmconv` ne permet plus de désactiver l'utilisation de la combinaison de touches Stop+A. L'événement Stop+A peut être audité.
- L'horodatage dans les enregistrements d'audit est indiqué au format ISO 8601. Pour plus d'informations concernant cette norme, reportez-vous à l'adresse `http://www.iso.org`.
- Trois options de stratégie d'audit ont été ajoutées :
  - **public** : les fichiers publics ne font plus l'objet d'audit pour des événements en lecture seule. La suppression de l'audit des fichiers publics réduit considérablement la taille de la piste d'audit. Ainsi, il est plus facile de surveiller les tentatives de lecture des fichiers sensibles. Pour plus d'informations sur les objets publics, reportez-vous à la section "Terminologie et concept de l'audit" à la page 594.
  - **perzone** : les effets de la stratégie `perzone` sont très vastes. Un démon d'audit distinct s'exécute dans chaque zone en se servant des fichiers de configuration d'audit qui lui sont propres. De même, la file d'attente de l'audit est spécifique à la zone. Pour plus d'informations, reportez-vous aux pages de manuel `auditd(1M)` et `auditconfig(1M)` Pour plus d'informations sur les zones, reportez-vous à la section "Audit et zones Oracle Solaris" à la page 684. Pour plus d'information sur la stratégie, reportez-vous à la section "Procédure de planification de l'audit par zone " à la page 606.
  - **zonename** : nom de la zone Oracle Solaris dans laquelle un événement d'audit qui s'est produit peut être inclus dans des enregistrements d'audit. Pour plus d'informations sur les zones, reportez-vous à la section "Audit et zones Oracle Solaris" à la page 684. Pour plus d'informations sur l'utiliser de l'option, reportez-vous à la section "Détermination de la stratégie d'audit" à la page 611.
- Cinq jetons d'audit ont été ajoutés :
  - Le jeton `cmd` enregistre la liste d'arguments et la liste de variables d'environnement associées à une commande. Pour plus d'informations, reportez-vous à la section "Jeton `cmd`" à la page 696.

- Le jeton `path_attr` enregistre la séquence des objets fichier attribut situés en dessous de l'objet jeton `path`. Pour plus d'informations, reportez-vous à la section "Jeton `path_attr`" à la page 703.
- Le jeton d'audit `privilege` enregistre l'utilisation de privilège sur un processus. Pour plus d'informations, reportez-vous à la section "Jeton `privilege`" à la page 703.
- Le jeton `uauth` enregistre l'utilisation d'autorisation à l'aide d'une commande ou d'une action. Pour plus d'informations, reportez-vous à la section "Jeton `uauth`" à la page 710.
- Le jeton `zonename` enregistre le nom de la zone non globale dans laquelle un événement d'audit s'est produit. L'option de stratégie d'audit `zonename` détermine si le jeton `zonename` est inclus dans l'enregistrement d'audit. Pour plus d'informations, reportez-vous à la section "Jeton `zonename`" à la page 710.

  Pour des informations de référence, reportez-vous à la section "Audit et zones Oracle Solaris" à la page 684. Pour en savoir plus sur les zones, reportez-vous à la Partie II, "Zones" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

◆ ◆ ◆ CHAPITRE 29

Planification de l'audit Oracle Solaris

Ce chapitre décrit les procédures de configuration du service d'audit pour votre installation Oracle Solaris. En particulier, le chapitre traite des points à prendre en compte avant d'activer le service d'audit. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre :

Pour une présentation de l'audit, reportez-vous au Chapitre 28, "Audit Oracle Solaris (présentation) ". Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au Chapitre 30, "Gestion de l'audit Oracle Solaris (tâches) ". Pour obtenir des informations de référence, reportez-vous au Chapitre 31, "Audit Oracle Solaris (référence) ".

Planification de l'audit Oracle Solaris (liste des tâches)

La liste suivante présente les principales tâches à effectuer pour planifier l'espace disque et définir les événements à enregistrer.

Tâche	Voir
Détermination de la stratégie d'audit pour les zones non globales	"Procédure de planification de l'audit par zone " à la page 606
Planification de l'espace de stockage pour la piste d'audit	"Procédure de planification du stockage pour les enregistrements d'audit" à la page 607
Détermination des personnes et objets à auditer	"Procédure de planification des personnes et objets à auditer" à la page 608

Planification de l'audit Oracle Solaris (tâches)

Vous voulez sélectionner avec soin les types d'activités auditées. Dans le même temps, vous voulez collecter des informations d'audit utiles. Les fichiers d'audit peuvent rapidement augmenter de volume et remplir l'espace disponible, de sorte que vous devez leur allouer suffisamment d'espace disque. Vous devez également planifier soigneusement les utilisateurs et objets audités.

▼ Procédure de planification de l'audit par zone

Si votre système a mis en œuvre des zones, vous avez deux possibilités de configuration d'audit :

- Vous pouvez configurer un seul service d'audit dans la zone globale pour toutes les zones.
- Vous pouvez configurer un service d'audit par zone.

Pour une description des compromis, reportez-vous à la section "Audit sur un système à zones Oracle Solaris" à la page 602.

- **Sélectionnez l'une des méthodes suivantes :**

  - **OPTION 1 : configuration d'un service d'audit pour toutes les zones.**

    L'audit de toutes les zones de façon identique peut créer une piste d'audit à image unique. Une piste d'audit à image unique se produit lorsque toutes les zones sur un système font partie d'un même domaine d'administration. Les enregistrements d'audit peuvent ensuite être facilement comparés, car les enregistrements de chaque zone sont présélectionnés avec des paramètres identiques.

    Cette configuration traite toutes les zones comme faisant partie d'un système. La zone globale exécute le démon d'audit sur un système et collecte les journaux d'audit pour chaque zone. Vous personnalisez les fichiers de configuration d'audit uniquement dans la zone globale, puis copiez ces fichiers dans chaque zone non globale.

    a. **Copiez le fichier `audit_control` de la zone globale dans chaque zone non globale.**

    b. **Utilisez la même base de données `audit_user` pour chaque zone.**

       La base de données `audit_user` peut être un fichier local, ou vous pouvez l'obtenir à partir d'un service de nommage partagé.

    c. **Activez la sélection par zone des enregistrements d'audit.**

       Pour placer le nom de la zone dans le cadre de l'enregistrement d'audit, définissez la stratégie `zonename` dans la zone globale. La commande `auditreduce` peut alors sélectionner les événements d'audit par zone dans la piste d'audit. Pour un exemple, reportez-vous à la page de manuel `auditreduce(1M)`.

Pour planifier une piste d'audit à image unique, reportez-vous à la section "Procédure de planification des personnes et objets à auditer" à la page 608. Commencez à la première étape. L'administrateur de la zone globale doit également réserver du stockage, comme décrit dans la section "Procédure de planification du stockage pour les enregistrements d'audit" à la page 607.

- **OPTION 2 : configuration d'un service d'audit par zone**

  Sélectionnez l'option de configuration d'audit par zone si différentes zones disposent de différents fichiers de service de nommage, ou si les administrateurs de zone souhaitent contrôler l'audit dans leurs zones.

  - Lorsque vous configurez l'audit par zone, vous devez configurer la zone globale pour l'audit. Vous définissez la stratégie d'audit `perzone` dans la zone globale. Pour définir la stratégie d'audit, reportez-vous à la section "Configuration de l'audit par zone" à la page 645.

    Remarque – Si les fichiers du service de nommage sont personnalisés dans des zones non globales, et la stratégie `perzone` n'est pas définie, une utilisation soigneuse des outils d'audit est requise pour sélectionner des enregistrements utilisables. Un ID d'utilisateur dans une zone peut se rapporter à un autre utilisateur du même ID dans une autre zone.

  - Pour générer des enregistrements dont le suivi peut être effectué jusqu'à leur zone d'origine, définissez la stratégie d'audit `zonename` dans la zone globale. Dans la zone globale, exécutez la commande `auditreduce` avec l'option `zonename`. Ensuite, dans la zone `zonename`, exécutez la commande `praudit` sur la sortie `auditreduce`.
  - Chaque administrateur de zone configure les fichiers d'audit pour la zone.

    Un administrateur de zone non globale peut définir toutes les options de stratégie à l'exception de `perzone` et `ahlt`.
  - Chaque administrateur de zone peut activer ou désactiver l'audit dans la zone.

  Si vous personnalisez les fichiers de configuration d'audit dans chaque zone, reportez-vous à la section "Procédure de planification des personnes et objets à auditer" à la page 608 pour planifier chaque zone. Vous pouvez ignorer la première étape. Chaque administrateur de zone doit également réserver du stockage pour chaque zone, comme décrit dans la section "Procédure de planification du stockage pour les enregistrements d'audit" à la page 607.

▼ Procédure de planification du stockage pour les enregistrements d'audit

La piste d'audit requiert un espace de fichiers dédié. L'espace de fichiers dédié pour les fichiers d'audit doit être disponible et sécurisé. Chaque système doit disposer de plusieurs répertoires

d'audit configurés pour les fichiers d'audit. Avant d'activer l'audit sur un système, vous devez d'abord décider de la manière de configurer les répertoires d'audit. La procédure suivante décrit les problèmes à résoudre lorsque vous planifiez le stockage de la piste d'audit.

Avant de commencer Si vous mettez en œuvre des zones non globales, effectuez la "Procédure de planification de l'audit par zone " à la page 606 avant d'utiliser cette procédure.

1. **Déterminez le niveau d'audit requis par votre site.**

   Définissez les besoins de sécurité de votre disque en tenant compte de l'espace disque disponible pour la piste d'audit.

   Pour obtenir des instructions sur la manière de réduire l'espace requis tout en maintenant la sécurité du site, ainsi que sur la conception du stockage d'audit, reportez-vous aux sections "Contrôle des coûts d'audit" à la page 615 et "Gestion efficace de l'audit" à la page 617.

2. **Déterminez les systèmes à auditer.**

   Sur ces systèmes, allouez de l'espace pour au moins un répertoire d'audit local. Pour spécifier les répertoires d'audit, reportez-vous à l'Exemple 30–3.

3. **Déterminez les systèmes pour le stockage des fichiers d'audit.**

   Décidez quels serveurs devront contenir les répertoires d'audit principal et secondaire. Pour consulter des exemples de configuration des disques pour les répertoires d'audit, reportez-vous à la section "Création des partitions pour les fichiers d'audit" à la page 631.

4. **Nommez les répertoires d'audit.**

   Créez une liste de tous les répertoires d'audit que vous prévoyez d'utiliser. Pour obtenir des instructions sur la procédure de nommage, reportez-vous aux sections "Stockage de la piste d'audit" à la page 601 et "Commande `auditreduce`" à la page 673.

5. **Déterminez quels répertoires d'audit doivent être utilisés par les systèmes.**

   Créez un tableau indiquant quel système doit utiliser quel répertoire d'audit. Le tableau doit vous permettre d'équilibrer les activités d'audit. Pour obtenir un exemple, reportez-vous aux Figure 31–1 et Figure 31–2.

▼ Procédure de planification des personnes et objets à auditer

Avant de commencer Si vous mettez en œuvre des zones non globales, effectuez la "Procédure de planification de l'audit par zone " à la page 606 avant d'utiliser cette procédure.

1 **Déterminez si vous souhaitez une piste d'audit d'image système unique.**

Des systèmes au sein d'un même domaine administratif peuvent créer une piste d'audit d'image système unique. Si vos systèmes utilisent différents services de nommage, commencez avec l'étape suivante. Vous devez effectuer le reste des étapes de planification pour chaque système.

Une piste d'audit d'image système unique traite les systèmes en cours d'audit comme un seul ordinateur. Pour créer une piste d'audit d'image système unique pour un site, chaque système dans l'installation doit être configuré comme suit :

- Utilisation du même service de nommage.

  Pour interpréter les enregistrements d'audit, deux commandes sont utilisées : `auditreduce` et `praudit`. Pour l'interprétation correcte des enregistrements d'audit, les fichiers `passwd`, `hosts` et `audit_user` doivent être cohérents.
- Utilisation des mêmes fichiers `audit_warn`, `audit_event`, `audit_class` et `audit_startup` que tout autre système.
- Utilisation de la même base de données `audit_user`. La base de données peut se trouver dans un service de nommage, tel que NIS ou LDAP.
- Disposition d'entrées `flags`, `naflags` et `plugin` identiques dans le fichier `audit_control`.

2 **Déterminez la stratégie d'audit.**

Utilisez la commande `auditconfig -lspolicy` pour afficher une brève description des options de stratégie disponibles. Par défaut, seule la stratégie `cnt` est activée. Pour une description plus complète, reportez-vous à l'Étape 8.

Pour les effets des options de stratégie, reportez-vous à la section “Détermination de la stratégie d'audit” à la page 611. Pour définir la stratégie d'audit, reportez-vous à la section “Configuration de la stratégie d'audit” à la page 635.

3 **Déterminez si vous souhaitez modifier les mappages des événements aux classes.**

Dans de nombreux cas, le mappage par défaut est suffisant. Cependant, si vous ajoutez de nouvelles classes, modifiez des définitions de classe ou déterminez qu'un enregistrement d'un appel système spécifique n'est pas utile, vous devrez peut-être également déplacer un événement vers une autre classe.

La section “Modification de l'appartenance à une classe d'un événement d'audit” à la page 629 présente un exemple.

4 **Déterminez les classes d'audit à présélectionner.**

Le meilleur moment pour ajouter des classes d'audit ou modifier des classes par défaut est avant le démarrage du service d'audit.

Les valeurs de classe d'audit des entrées `flags`, `naflags` et `plugin` dans le fichier `audit_control` s'appliquent à tous les utilisateurs et processus. Les classes présélectionnées déterminent si une classe d'audit est auditée en cas de réussite, d'échec ou dans les deux cas.

Pour présélectionner des classes d'audit, reportez-vous à la section “Modification du fichier audit_control ” à la page 621.

5 Déterminez les exceptions d'utilisateurs aux classes d'audit présélectionnées à l'échelle du système.

Si vous souhaitez que certains utilisateurs soient audités différemment selon la classe d'audit présélectionnée à l'échelle du système, modifiez les entrées d'utilisateurs dans la base de données `audit_user`.

Pour un exemple, reportez-vous à la section “Modification des caractéristiques d'audit d'un utilisateur” à la page 626.

6 Déterminez l'espace disque minimal disponible.

Lorsque l'espace disque disponible sur un système de fichiers d'audit passe en dessous du pourcentage `minfree`, le démon `auditd` bascule vers le prochain répertoire d'audit disponible. Le démon envoie ensuite un message d'avertissement indiquant que la limite dépassable a été dépassée.

Pour définir l'espace disque disponible minimal, reportez-vous à l'Exemple 30–4.

7 Déterminez la façon de gérer les alias de messagerie `audit_warn`.

Le script `audit_warn` est exécuté chaque fois que le système d'audit doit vous avertir d'une situation qui requiert l'attention du service d'administration. Par défaut, le script `audit_warn` envoie un e-mail à un alias `audit_warn` et un message à la console.

Pour configurer l'alias, reportez-vous à la section “Configuration de l'alias de messagerie audit_warn ” à la page 635.

8 Déterminez la mesure à prendre lorsque tous les répertoires d'audit sont pleins.

Par défaut, lorsque la piste d'audit est trop longue, le système continue de fonctionner. Le système comptabilise les enregistrements d'audit qui sont supprimés, mais n'enregistre pas les événements. Pour plus de sécurité, vous pouvez désactiver la stratégie `cnt` et activer la stratégie `ahlt`. La stratégie `ahlt` arrête le système lorsqu'un événement asynchrone ne peut pas être placé dans la file d'attente de l'audit.

Pour une description de ces options de stratégie, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones ” à la page 614. Pour configurer ces options de stratégie, reportez-vous à l'Exemple 30–16.

9 Déterminez si les enregistrements d'audit sont collectés au format binaire, au format `syslog` ou dans les deux formats.

Pour des informations générales, reportez-vous à la section “Journaux d'audit” à la page 599.

La section “Configuration des journaux d'audit syslog ” à la page 623 présente un exemple.

Détermination de la stratégie d'audit

La stratégie d'audit détermine les caractéristiques des enregistrements d'audit pour le système local. Les options de stratégie sont définies par un script de démarrage. Le script `bsmconv`, qui active le service d'audit, crée le script `/etc/security/audit_startup`. Le script `audit_startup` exécute la commande `auditconfig` pour établir la stratégie d'audit. Pour plus de détails sur le script, reportez-vous à la page de manuel `audit_startup(1M)`.

La plupart des options de la stratégie d'audit sont désactivées par défaut afin de réduire les exigences en matière de stockage et les demandes de traitement du système. Vous pouvez activer et désactiver dynamiquement les options de la stratégie d'audit à l'aide de la commande `auditconfig` . Vous pouvez activer et désactiver de manière permanente les options de stratégie à l'aide du script `audit_startup`.

Utilisez le tableau suivant pour déterminer si les besoins de votre site justifient le temps système supplémentaire résultant de l'activation d'une ou plusieurs options de stratégie d'audit.

TABLEAU 29–1 Effets des options de stratégie d'audit

Nom de la stratégie	Description	Pourquoi modifier l'option de stratégie
`ahlt`	Cette stratégie s'applique aux événements asynchrones uniquement. Lorsqu'elle est désactivée, cette stratégie permet à l'événement de se terminer sans générer d'enregistrement d'audit. Lorsqu'elle est activée, cette stratégie arrête le système lorsque les systèmes de fichiers d'audit sont pleins. L'intervention de l'administrateur est nécessaire pour nettoyer la file d'attente de l'audit, libérer de l'espace disponible pour les enregistrements d'audit, puis redémarrer l'ordinateur. Cette stratégie ne peut être activée que dans la zone globale. La stratégie affecte toutes les zones.	L'option désactivée est judicieuse lorsque la disponibilité du système est plus importante que la sécurité. L'option activée est opportune dans un environnement où la sécurité est primordiale.
`arge`	Lorsqu'elle est désactivée, cette stratégie omet les variables d'environnement d'un programme exécuté dans l'enregistrement d'audit `exec`. Lorsqu'elle est désactivée, cette stratégie ajoute les variables d'environnement d'un programme exécuté à l'enregistrement d'audit `exec`. Les enregistrements d'audit qui en résultent contiennent beaucoup plus de détails que lorsque cette stratégie est désactivée.	L'option désactivée collecte beaucoup moins d'informations que l'option activée. L'option activée est pratique lorsque vous auditez un petit nombre d'utilisateurs. L'option est également utile lorsque vous avez des doutes concernant les variables d'environnement utilisées dans les programmes `exec`.

TABLEAU 29–1 Effets des options de stratégie d'audit *(Suite)*

Nom de la stratégie	Description	Pourquoi modifier l'option de stratégie
`argv`	Lorsqu'elle est désactivée, cette stratégie omet les arguments d'un programme exécuté dans l'enregistrement d'audit `exec`. Lorsqu'elle est activée, cette stratégie ajoute les arguments d'un programme exécuté pour l'enregistrement d'audit `exec`. Les enregistrements d'audit qui en résultent contiennent beaucoup plus de détails que lorsque cette stratégie est désactivée.	L'option désactivée collecte beaucoup moins d'informations que l'option activée. L'option activée est pratique lorsque vous auditez un petit nombre d'utilisateurs. L'option est également utile lorsque vous avez des raisons de penser que des programmes `exec` inhabituels sont exécutés.
`cnt`	Lorsqu'elle est désactivée, cette stratégie bloque un utilisateur ou l'exécution d'une application. Le blocage se produit lorsque des enregistrements d'audit ne peuvent pas être ajoutés à la piste d'audit car aucun espace disque n'est disponible. Lorsqu'elle est désactivée, cette stratégie permet à l'événement de se terminer sans générer d'enregistrement d'audit. Cette stratégie comptabilise les enregistrements d'audit qui sont supprimés.	L'option désactivée est opportune dans un environnement où la sécurité est primordiale. L'option activée est judicieuse lorsque la disponibilité du système est plus importante que la sécurité.
`group`	Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de liste de groupes aux enregistrements d'audit. Lorsqu'elle est activée, cette stratégie ajoute une liste de groupes à chaque enregistrement d'audit en tant que jeton spécial.	L'option désactivée répond généralement aux exigences de sécurité du site. L'option activée est utile lorsque vous avez besoin d'auditer les groupes générant des événements d'audit.
`path`	Lorsqu'elle est désactivée, cette stratégie consigne dans un enregistrement d'audit au maximum un chemin utilisé au cours d'un appel système. Lorsqu'elle est activée, cette stratégie enregistre chaque chemin d'accès utilisé en association avec un événement d'audit pour chaque enregistrement d'audit.	L'option désactivée place au maximum un chemin d'accès dans un enregistrement d'audit. L'option activée entre chaque nom de fichier ou chemin d'accès utilisé au cours d'un appel système dans l'enregistrement d'audit en tant que jeton `path`.
`perzone`	Lorsqu'elle est désactivée, cette stratégie conserve une seule configuration d'audit pour un système. Un démon d'audit s'exécute dans la zone globale. Les événements d'audit dans les zones non globales peuvent être situés dans l'enregistrement d'audit en présélectionnant le jeton d'audit `zonename`. Lorsqu'elle est activée, cette stratégie conserve une configuration d'audit, une file d'attente d'audit et des journaux d'audit distincts pour chaque zone. Un démon d'audit distinct s'exécute dans chaque zone. Cette stratégie ne peut être activée que dans la zone globale.	L'option désactivée est utile lorsque vous n'avez aucune raison particulière de conserver un journal d'audit, une file d'attente et un démon distincts pour chaque zone. L'option activée est opportune lorsque vous ne pouvez pas contrôler votre système efficacement en présélectionnant simplement le jeton d'audit `zonename`.

TABLEAU 29–1 Effets des options de stratégie d'audit *(Suite)*

Nom de la stratégie	Description	Pourquoi modifier l'option de stratégie
`public`	Lorsqu'elle est désactivée, cette stratégie n'ajoute pas d'événements en lecture seule d'objets publics à la piste d'audit lorsque la lecture de fichiers est présélectionnée. Les classes d'audit contenant des événements en lecture seule incluent les classes `fr`, `fa` et `cl`. Lorsqu'elle est activée, cette stratégie enregistre tous les événements d'audit en lecture seule d'objets publics si une classe d'audit appropriée est présélectionnée.	L'option désactivée répond généralement aux exigences de sécurité du site. L'option activée est rarement utilisée.
`seq`	Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de numéro de séquence à chaque enregistrement d'audit. Lorsqu'elle est activée, cette stratégie ajoute un numéro de séquence à chaque enregistrement d'audit. Le jeton `sequence` contient le numéro de séquence.	L'option désactivée est suffisante lorsque l'audit s'exécute correctement. L'option activée est utile lorsque la stratégie `cnt` est activée. La stratégie `seq` vous permet de déterminer si des données ont été supprimées.
`trail`	Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de jeton `trailer` aux enregistrements d'audit. Lorsqu'elle est activée, cette stratégie ajoute un jeton `trailer` à chaque enregistrement d'audit.	L'option désactivée crée un enregistrement d'audit de plus petite taille. L'option activée marque clairement la fin de chaque enregistrement d'audit avec un jeton `trailer`. Le jeton `trailer` est souvent utilisé conjointement au jeton `sequence`. Le jeton `trailer` assure une resynchronisation plus facile et plus précise des enregistrements d'audit.
`zonename`	Lorsqu'elle est désactivée, cette stratégie n'inclut pas de jeton `zonename` dans les enregistrements d'audit. Lorsqu'elle est activée, cette stratégie comprend un `zonename` jeton dans chaque enregistrement d'audit à partir d'une zone non globale.	L'option désactivée est utile lorsque vous n'avez pas besoin de comparer le comportement d'audit des différentes zones. L'option activé est utile lorsque vous souhaitez isoler et comparer le comportement d'audit des différentes zones.

Stratégies d'audit des événements asynchrones et synchrones

Les stratégies `ahlt` et `cnt` déterminent ce qui se passe lorsque la file d'attente de l'audit est pleine et ne peut plus accepter d'événements. Les stratégies sont indépendantes et associées. Les combinaisons de ces stratégies ont les effets suivants :

- `-ahlt +cnt` est la stratégie adoptée par défaut. Cette valeur par défaut permet à un événement audité d'être traité même s'il ne peut pas être consigné.

  La stratégie `-ahlt` indique que si un enregistrement d'audit d'un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise les événements et poursuit le traitement. Dans la zone globale, le compteur `as_dropped` enregistre le nombre correspondant.

  La stratégie `+cnt` indique que si un événement synchrone survient et ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise l'événement et poursuit le traitement. Le compteur `as_dropped` de la zone enregistre le nombre correspondant.

  La configuration `-ahlt +cnt` est généralement utilisée sur les sites où le traitement doit se poursuivre, même si celui-ci peut entraîner une perte d'enregistrements d'audit. Les champs `auditstatdrop` indiquent le nombre d'enregistrements d'audit supprimés dans une zone.

- La stratégie `+ahlt -cnt` indique que le traitement s'arrête lorsqu'un événement ne peut pas être ajouté à la file d'attente d'audit du noyau.

  La stratégie `+ahlt` indique que si un enregistrement d'audit d'un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, toutes les opérations de traitement sont arrêtées. Le système panique. L'événement asynchrone ne sera pas dans la file d'attente de l'audit et doit être récupéré à partir de pointeurs sur la pile des appels.

  La stratégie `-cnt` indique que, si un événement synchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le thread tentant de fournir l'événement sera bloqué. Le thread est placé dans une file d'attente de mise en veille jusqu'à ce que de l'espace d'audit devienne disponible. Aucun compte n'est conservé. Des programmes peuvent sembler bloqués jusqu'à ce que de l'espace d'audit devienne disponible.

  La configuration `+ahlt -cnt` est généralement utilisée dans les sites où un enregistrement de chaque événement d'audit est prioritaire sur la disponibilité du système. Des programmes semblent être bloqués jusqu'à ce que de l'espace d'audit devienne disponible. Le champ `auditstat wblk` indique à combien de reprises des threads ont été bloqués.

  Toutefois, si un événement asynchrone se produit, le système va paniquer, entraînant une interruption de service. La file d'attente du noyau des événements d'audit peut être restaurée manuellement partir d'un vidage mémoire enregistré. L'événement asynchrone ne sera pas dans la file d'attente de l'audit et doit être récupéré à partir de pointeurs sur la pile des appels.

- La stratégie `-ahlt -cnt` indique que si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, l'événement sera comptabilisé et le traitement poursuivi. Lorsqu'un événement synchrone ne peut pas être placé dans la file d'attente

d'audit du noyau, le thread tentant de fournir l'événement sera bloqué. Le thread est placé dans une file d'attente de mise en veille jusqu'à ce que de l'espace d'audit devienne disponible. Aucun compte n'est conservé. Des programmes peuvent sembler bloqués jusqu'à ce que de l'espace d'audit devienne disponible.

La configuration `-ahlt -cnt` est généralement utilisée dans les sites où l'enregistrement de tous les événements d'audit synchrones est prioritaire sur la perte potentielle d'enregistrements d'audit asynchrones. Le champ `auditstat wblk` indique à combien de reprises des threads ont été bloqués.

- La stratégie `+ahlt +cnt` indique que si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système panique. Si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise l'événement et poursuit le traitement.

Contrôle des coûts d'audit

Étant donné que la fonction d'audit consomme des ressources système, vous devez contrôler le degré de détail enregistré. Lorsque vous déterminez la portée de l'audit, vous devez prendre en compte les facteurs coûts suivants :

- Coût de l'augmentation du temps de traitement
- Coût de l'analyse des données d'audit
- Coût du stockage des données d'audit

Coût de l'augmentation du temps de traitement des données d'audit

Le coût de l'augmentation du temps de traitement est le moins significatif des coûts d'audit. L'audit n'a généralement pas lieu durant des opérations à forte intensité de calcul, telles que le traitement d'images, des calculs complexes, etc. Par ailleurs, le coût des systèmes monoutilisateur est généralement assez faible pour être ignorer.

Coût de l'analyse des données d'audit

Le coût de l'analyse est globalement proportionnel à la quantité de données d'audit collectées. Le coût d'analyse comprend le temps requis pour fusionner et passer en revue les enregistrements d'audit. Le coût inclut également le temps requis pour archiver les enregistrements et conserver les enregistrements dans un endroit sûr.

Le temps requis pour analyser la piste d'audit est d'autant plus court que le nombre d'enregistrements générés est faible. Les prochaines sections “Coût du stockage des données

d'audit " à la page 616 et "Gestion efficace de l'audit" à la page 617 décrivent les différentes manières d'effectuer un audit efficace. Un audit efficace permet de réduire la quantité de données d'audit, tout en fournissant une couverture suffisante pour atteindre vos objectifs en matière de sécurité du site.

Coût du stockage des données d'audit

Le coût du stockage est le coût le plus significatif de l'audit. La quantité des données d'audit dépend des facteurs suivants :

- Nombre d'utilisateurs
- Nombre de systèmes
- Niveau d'utilisation
- Degré de traçabilité et de responsabilité requis

Étant donné que ces facteurs varient d'un site à l'autre, aucune formule ne permet de prédéterminer la quantité d'espace disque à réserver pour le stockage des données d'audit. Inspirez-vous des informations suivantes, données à titre d'exemple :

- Présélectionnez des classes d'audit judicieusement afin de réduire le volume des enregistrements générés.

  L'audit complet, c'est-à-dire, avec la classe `all` remplit les disques rapidement. Même une tâche simple, telle que la compilation d'un programme, peut générer un fichier d'audit volumineux. Un programme de taille modeste peut générer des milliers d'enregistrements d'audit en moins d'une minute.

  Par exemple, en omettant la classe d'audit `file_read`, `fr`, vous pouvez réduire considérablement le volume d'audit. En choisissant d'auditer uniquement les opérations ayant échoué, vous pouvez parfois réduire le volume d'audit. Par exemple, en auditant les opérations `file_read` qui ont échoué, `-fr`, vous générez bien moins d'enregistrements qu'en auditant tous les événements `file_read`.
- La gestion efficace des fichiers d'audit joue également un rôle important. Une fois les enregistrements d'audit créés, la gestion des fichiers réduit la quantité de stockage requis.
- Assurez-vous de bien comprendre les classes d'audit.

  Avant de configurer l'audit, vous devez comprendre les types d'événements contenus dans les classes. Vous pouvez modifier les mappages des événements aux classes d'audit afin d'optimiser la collecte des enregistrements d'audit.
- Développez une philosophie d'audit pour votre site.

  Basez votre philosophie sur des mesures raisonnables. De telles mesures incluent le niveau de traçabilité requis par votre site et les types d'utilisateurs que vous administrez.

Gestion efficace de l'audit

Les techniques suivantes peuvent vous aider à atteindre les objectifs de sécurité de votre organisation tout en améliorant l'efficacité de l'audit.

- Auditez de manière aléatoire uniquement un certain pourcentage d'utilisateurs à un moment donné.
- Réduisez l'espace de stockage sur disque requis pour les fichiers d'audit en combinant, réduisant et compressant les fichiers. Développez des procédures pour l'archivage des fichiers, le transfert des fichiers vers des supports amovibles et le stockage des fichiers hors ligne.
- Surveillez les données d'audit en temps réel pour identifier des comportements inhabituels. Vous pouvez étendre les outils d'analyse et de gestion que vous avez déjà développés pour traiter les enregistrements d'audit dans des fichiers `syslog`.

  Vous pouvez également configurer des procédures pour surveiller certaines activités dans la piste d'audit. Vous pouvez écrire un script pour déclencher une augmentation automatique de l'audit de certains utilisateurs ou systèmes en réponse à la détection d'événements inhabituels.

  Par exemple, vous pouvez écrire un script effectuant les opérations suivantes :

  1. Surveillance de la création des fichiers d'audit sur tous les serveurs de fichiers d'audit.
  2. Traitement des fichiers d'audit avec la commande `tail`.

     Le traitement pipeline de la sortie de la commande `tail -0f` via la commande `praudit` peut produire un flux d'enregistrements d'audit lorsque les enregistrements sont générés. Pour plus d'informations, reportez-vous à la page de manuel `tail(1)`.
  3. Analyse des types de messages inhabituels ou d'autres indicateurs dans ce flux et fourniture de l'analyse à l'auditeur.

     Ou, le script peut être utilisé pour le déclenchement de réponses automatiques.
  4. Surveillance permanente des répertoires d'audit pour détecter l'apparition de nouveaux fichiers d'audit `not_terminated`.
  5. Arrêt de processus `tail` à traiter lorsque leurs fichiers ne sont plus en cours d'écriture.

◆ ◆ ◆ CHAPITRE 30

Gestion de l'audit Oracle Solaris (tâches)

Ce chapitre présente les procédures vous permettant de configurer et gérer un système Oracle Solaris qui fait l'objet d'un audit. Ce chapitre comprend également des instructions de l'administration de la piste d'audit. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

Pour obtenir une présentation générale du service d'audit, reportez-vous au Chapitre 28, "Audit Oracle Solaris (présentation) ". Pour obtenir des suggestions de planification, reportez-vous au Chapitre 29, "Planification de l'audit Oracle Solaris". Pour obtenir des informations de référence, reportez-vous au Chapitre 31, "Audit Oracle Solaris (référence) ".

Audit Oracle Solaris (liste des tâches)

La liste des tâches suivante présente les principales tâches nécessaires à la gestion de l'audit. Les tâches sont triées.

Tâche	Description	Voir
1. Planification de l'audit	Vous devez prendre un certain nombre de décisions avant de procéder à la configuration du service d'audit.	"Planification de l'audit Oracle Solaris (liste des tâches) " à la page 605
2. Configuration des fichiers d'audit	Définit les événements, classes et utilisateurs qui nécessitent un audit.	"Configuration des fichiers d'audit (liste des tâches) " à la page 620

Tâche	Description	Voir
3. Configuration et activation de l'audit	Configure chaque hôte par rapport à l'espace disque et à d'autres exigences du service d'audit. Démarre ensuite le service d'audit.	"Configuration et activation du service d'audit (liste des tâches) " à la page 630
	Sur un hôte qui possède des zones non globales, configurez un service d'audit pour le système ou un service d'audit par zone.	"Configuration du service d'audit dans les zones (tâches) " à la page 642
4. Gestion des enregistrements d'audit	Collecte et analyse les données d'audit.	"Gestion des enregistrements d'audit (liste des tâches) " à la page 646

Configuration des fichiers d'audit (liste des tâches)

La liste des tâches suivante présente les procédures de configuration de fichiers pour personnaliser l'audit sur votre site. La plupart de ces tâches sont facultatives.

Tâche	Description	Voir
Sélection de classes d'audit et personnalisation des paramètres `audit_control`	Comprend les opérations suivantes : ■ Présélection des classes d'audit à l'échelle du système ■ Spécification des répertoires d'audit pour chaque système ■ Définition des limites de l'espace disque sur les systèmes de fichiers d'audit	"Modification du fichier `audit_control` " à la page 621
(Facultatif) Consignation des événements d'audit de deux façons	Vous permet de surveiller les événements d'audit en temps réel, en plus de stockage des enregistrements d'audit dans un format binaire.	"Configuration des journaux d'audit `syslog` " à la page 623
(Facultatif) Modification des caractéristiques d'audit pour les utilisateurs	Définit des exceptions utilisateurs aux classes d'audit présélectionnées à l'échelle du système.	"Modification des caractéristiques d'audit d'un utilisateur" à la page 626
(Facultatif) Ajout de classes d'audit	Réduit le nombre d'enregistrements d'audit en créant une nouvelle classe d'audit pour contenir les événements.	"Ajout d'une classe d'audit " à la page 627
(Facultatif) Modification des mappages événements-classes	Réduit le nombre d'enregistrements d'audit en modifiant les mappages événements-classes.	"Modification de l'appartenance à une classe d'un événement d'audit" à la page 629

Configuration des fichiers d'audit (tâches)

Avant d'activer l'audit sur votre réseau, vous pouvez personnaliser les fichiers de configuration d'audit pour répondre aux conditions requises pour l'audit de votre site. Vous pouvez également redémarrer le service d'audit ou réinitialiser le système local pour lire les fichiers de configuration modifiés après l'activation du service d'audit. Il est toutefois recommandé de personnaliser votre configuration de l'audit autant que possible avant de démarrer le service d'audit.

Si vous avez mis en œuvre des zones, vous pouvez choisir d'auditer toutes les zones à partir de la zone globale. Pour faire la différence entre les zones dans la sortie d'audit, vous pouvez définir l'option de stratégie `zonename`. Si vous décidez d'auditer les zones non globales individuellement, vous pouvez également définir la stratégie `perzone` dans la zone globale et personnaliser les fichiers de configuration d'audit dans les zones non globales. Pour obtenir une présentation générale, reportez-vous à la section "Audit et zones Oracle Solaris" à la page 684. Pour la planification, reportez-vous à la section "Procédure de planification de l'audit par zone " à la page 606. Pour plus d'informations sur les procédures, reportez-vous à la section "Configuration du service d'audit dans les zones (tâches) " à la page 642.

▼ Modification du fichier `audit_control`

Le fichier `/etc/security/audit_control` configure l'audit à l'échelle du système. Le fichier détermine les événements qui sont audités, le moment où les avertissements d'audit sont émis et l'emplacement des fichiers d'audit.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 (Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.orig
```

3 Modifiez le fichier `audit_control` pour votre site.

Chaque entrée possède le format suivant :

keyword : *value*

mot-clé Définit le type de ligne. Les types sont `dir`, `flags`, `minfree`, `naflags` et `plugin`. Dans la version Solaris10, les lignes `dir` et `minfree` ont été abandonnées.

Pour obtenir des explications sur les mots-clés, reportez-vous aux exemples suivants.

valeur Spécifie les données associées au type de ligne.

Remarque – Pour indiquer les emplacements des répertoires d'audit, utilisez l'attribut `p_dir` au plug-in `audit_binfile.so`. Pour spécifier l'espace disponible minimum, utilisez l'attribut `p_minfree`.

4 (Facultatif) Vérifiez la syntaxe du fichier.

```
# audit -v /etc/security/audit_control
syntax ok
```

Exemple 30–1 Présélection des classes d'audit pour tous les utilisateurs

La ligne `flags` dans le fichier `audit_control` définit les classes des événements attribuables qui sont audités pour tous les utilisateurs sur le système. Les classes sont séparées par des virgules. Un espace est autorisé. Dans cet exemple, les événements des classes `lo` et `ap` sont audités pour tous les utilisateurs.

```
## audit_control file
flags:lo,ap
naflags:lo
plugin:name=...
```

Pour voir les événements qui sont affectés à une classe, lisez le fichier `audit_event`. Vous pouvez également utiliser la commande `bsmrecord`, tel qu'illustré dans l'Exemple 30–27.

Exemple 30–2 Présélection d'événements non attribuables

Dans cet exemple, tous les événements dans la classe `na` et tous les événements `login` qui ne sont pas imputables font l'objet d'un audit.

```
## audit_control file
flags:lo
naflags:lo,na
plugin:name=...
```

Exemple 30–3 Définition de l'emplacement des données d'audit binaires

L'indicateur `p_dir` du plug-in `audit_binfile.so` répertorie les systèmes de fichiers d'audit à utiliser pour les données d'audit binaires. Dans cet exemple, trois emplacements sont définis pour les données d'audit binaires. Les répertoires sont classés dans l'ordre, du répertoire principal au répertoire de dernier recours. La ligne `plugin` ne contient pas de retour à la ligne.

```
## audit_control file
##
flags:lo
naflags:lo,na
```

```
plugin:name=audit_binfile.so; p_dir=/var/audit/egret.1/files,
/var/audit/egret.2/files,/var/audit
```

Pour configurer des systèmes de fichiers binaires d'audit pour contenir les données d'audit, reportez-vous à la section "Création des partitions pour les fichiers d'audit" à la page 631.

Exemple 30–4 Modification de la limite dépassable d'avertissements

Dans cet exemple, l'espace disponible minimum pour tous les systèmes de fichiers d'audit est défini de façon à ce qu'un message d'avertissement est émis lorsque seuls 10 % du système de fichiers est disponible.

La ligne `plugin` ne contient pas de retour à la ligne.

```
## audit_control file
#
flags:lo
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit/examplehost.1/files,
/var/audit/examplehost.2/files,/var/audit/localhost/files; p_minfree=10
```

L'alias `audit_warn` reçoit l'avertissement. Pour configurer l'alias, reportez-vous à la section "Configuration de l'alias de messagerie `audit_warn` " à la page 635.

▼ Configuration des journaux d'audit `syslog`

Vous pouvez demander au service d'audit de copier tout ou partie des enregistrements d'audit collectés dans la file d'attente de l'audit pour `syslog`. Dans la procédure suivante, vous allez enregistrer les données d'audit textuelles et binaires. Les données d'audit textuelles sont un sous-ensemble de données binaires.

Avant de commencer Vous devez présélectionner les classes d'audit. Les classes d'audit présélectionnées sont spécifiées dans les lignes `flags` et `naflags` du fichier `audit_control`. Vous pouvez également présélectionner des classes pour les utilisateurs·individuels·dans·le·fichier·?`audit_user` et ajouter de façon dynamique les classes d'audit avec la commande `auditconfig`.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 (Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.save
```

3 Ajoutez une entrée de plug-in `audit_syslog.so`.

```
## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so;p_dir=/var/audit; p_minfree=20;
plugin:name=audit_syslog.so;p_flags=+lo,-ss
```

Une entrée `plugin` se présente sous la forme suivante :

`plugin:name=`*name*`; qsize=`*max-queued-records*`;p_*=*value*

- `name=`*name* : spécifie le nom du plug-in. Les valeurs valides sont `audit_binfile.so` et `audit_syslog.so`.
- `qsize=`*max-queued-records* : spécifie le nombre maximal d'enregistrements à mettre en file d'attente pour des données d'audit envoyées au plug-in. L'attribut est facultatif.
- `p_*=` *value* : spécifie les attributs du plug-in. Le plug-in `audit_syslog.so` accepte `p_flags`. Le plug-in `audit_binfile.so` accepte `p_dir`, `p_minfree` et `p_fsize`. L'attribut `p_fsize` a été introduit dans Solaris 10 10/08.

Pour plus d'informations sur les attributs de plug-in, reportez-vous à la section `OBJECT ATTRIBUTES` des pages de manuel `audit_binfile(5)` et `audit_syslog(5)`.

4 Ajoutez une entrée `audit.notice` au fichier `syslog.conf`.

L'entrée inclut l'emplacement du fichier journal.

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

Ne stockez pas les journaux texte dans lesquels les fichiers d'audit sont stockés. La commande `auditreduce`, qui lit les fichiers d'audit binaires, suppose que tous les fichiers d'une partition d'audit sont des fichiers d'audit binaires.

5 Créez le fichier journal.

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

6 Actualisez les informations de configuration du service `syslog`.

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

7 Archivez régulièrement les fichiers journaux `syslog`.

Le service d'audit peut générer une sortie volumineuse. Pour gérer les journaux, reportez-vous à la page de manuel `logadm(1M)`.

Exemple 30–5 Spécification des classes d'audit pour la sortie `syslog`

Dans l'exemple suivant, l'utilitaire `syslog` collecte un sous-ensemble de classes d'audit présélectionnées.

```
## audit_user file
jdoe:pf

## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit/host.1/files,
/var/audit/host.2/files,/var/audit/localhost/files; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,-na,-ss,+pf
```

Les entrées `flags` et `naflags` demandent au système de collecter tous les enregistrements d'audit de connexion/déconnexion, non allouables et de changement de l'état du système au format binaire. L'entrée de plug-in `audit_syslog.so` demande à l'utilitaire `syslog` de collecter uniquement les connexions et événements non attribuables ayant échoué ainsi que les échecs de modification de l'état du système. Pour l'utilisateur `jdoe`, l'enregistrement d'audit binaire inclut toutes les utilisations d'un shell basé sur les profils. L'utilitaire `syslog` collecte les commandes réussies basées sur les profils. La classe `pf` est créée dans l'Exemple 30–10.

Exemple 30–6 Stockage des enregistrements d'audit `syslog` sur un système distant

Vous pouvez changer l'entrée `audit.notice` du fichier `syslog.conf` afin qu'elle pointe vers un système distant. Dans cet exemple, le nom du système local est `example1`. Le système distant est `remote1`.

```
example1 # cat /etc/syslog.conf
...
audit.notice       @remote1
```

L'entrée `audit.notice` du fichier `syslog.conf` sur le système `remote1` pointe vers le fichier journal.

```
remote1 # cat /etc/syslog.conf
...
audit.notice       /var/adm/auditlog
```

Exemple 30–7 Utilisation des plug-ins dans le fichier `audit_control`

La méthode préférée pour spécifier des informations non liées aux indicateurs dans le fichier `audit_control` est d'utiliser l'entrée `plugin`. Dans cet exemple, les indicateurs d'audit sont sélectionnés, puis les informations de plug-in sont répertoriées.

```
## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so;p_minfree=10; p_dir=/var/audit
plugin:name=audit_syslog.so; p_flags=+lo
```

▼ Modification des caractéristiques d'audit d'un utilisateur

Les définitions de chaque utilisateur sont stockées dans la base de données `audit_user`. Ces définitions modifient, pour l'utilisateur spécifié, les classes présélectionnées dans le fichier `audit_control`. Le fichier `nsswitch.conf` détermine si un fichier local ou une base de données de service de nommage est utilisé(e). Pour calculer le masque de présélection d'audit final de l'utilisateur, reportez-vous à la section "Caractéristiques de l'audit des processus" à la page 689.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 (Facultatif) Enregistrez une copie de sauvegarde de la base de données `audit_user`.

```
# cp /etc/security/audit_user /etc/security/audit_user.orig
```

3 Ajoutez de nouvelles entrées à la base de données `audit_user`.

Dans la base de données locale, chaque entrée a le format suivant :

username:*always-audit*:*never-audit*

username	Permet de sélectionner le nom de l'utilisateur audité.
always-audit	Sélectionne la liste des classes d'audit qui doivent toujours être auditées pour l'utilisateur spécifié.
never-audit	Sélectionne la liste des classes d'audit qui ne doivent jamais être auditées pour l'utilisateur spécifié.

Vous pouvez spécifier plusieurs classes en séparant les classes d'audit par une virgule.

Les entrées `audit_user` seront effectives à la prochaine connexion de l'utilisateur.

Exemple 30–8 Modification des événements à auditer pour un utilisateur

Dans cet exemple, le fichier `audit_control` contient les classes d'audit présélectionnées pour le système :

```
## audit_control file
...
flags:lo,ss
naflags:lo,na
```

Le fichier `audit_user` affiche une exception. Lorsque l'utilisateur `jdoe` utilise un shell de profil cette utilisation est auditée :

```
## audit_user file
jdoe:pf
```

Le masque de présélection d'audit pour `jdoe` est une combinaison des paramètres `audit_user` et `audit_control`. La commande `auditconfig -getaudit` affiche le masque de présélection pour `jdoe` :

```
# auditconfig -getaudit
audit id = jdoe(1234567)
process preselection mask = ss,pf,lo(0x13000,0x13000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 2138517656
```

Exemple 30–9 Audit des utilisateurs uniquement, et non du système

Dans cet exemple, les activités de connexion et de rôle de quatre utilisateurs uniquement sont auditées sur ce système. Le fichier `audit_control` n'a pas présélectionné les classes d'audit pour le système.

```
## audit_control file
...
flags:
naflags:
```

Le fichier `audit_user` présélectionne deux classes d'audit pour quatre utilisateurs, comme suit :

```
## audit_user file
jdoe:lo,pf
kdoe:lo,pf
pdoe:lo,pf
sdoe:lo,pf
```

Le fichier `audit_control` suivant enregistre l'intrusion injustifiée. Utilisé en combinaison avec le fichier `audit_user`, ce fichier protège plus le système que le premier fichier `audit_control` dans cet exemple.

```
## audit_control file
...
flags:
naflags:lo
plugin:name=...
```

▼ Ajout d'une classe d'audit

Lorsque vous créez votre propre classe d'audit, vous pouvez y placer uniquement les événements que vous souhaitez auditer pour votre site. Lorsque vous ajoutez la classe sur un seul système, vous devez copier la modification sur tous les systèmes audités.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **(Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_class`.**

```
# cp /etc/security/audit_class /etc/security/audit_class.orig
```

3 **Ajoutez de nouvelles entrées au fichier `audit_class`.**

Chaque entrée possède le format suivant :

`0x`*number*`:`*name*`:`*description*

0x	Identifie *number* en tant que valeur hexadécimale.
number	Définit le masque de classe d'audit unique.
name	Définit le nom en lettres de la classe d'audit.
description	Définit le nom descriptif de la classe d'audit.

L'entrée doit être unique dans le fichier. N'utilisez pas les masques de classe d'audit existants.

Exemple 30–10 Création d'une nouvelle classe d'audit

Cet exemple crée une classe qui contient un petit ensemble d'événements d'audit. L'entrée ajoutée au fichier `audit_class` se présente comme suit :

```
0x10000000:pf:profile command
```

L'entrée crée une nouvelle classe d'audit appelée `pf`. L'Exemple 30–11 remplit la nouvelle classe d'audit.

Erreurs fréquentes Si vous avez personnalisé le fichier `audit_class`, assurez-vous que les modifications éventuelles du fichier `audit_user` sont cohérentes avec les nouvelles classes d'audit. Des erreurs se produisent lorsque les classes d'audit dans `audit_user` ne sont pas un sous-ensemble de la base de données `audit_class`.

▼ Modification de l'appartenance à une classe d'un événement d'audit

Vous pouvez être amené à modifier l'appartenance à une classe d'un événement d'audit pour réduire la taille d'une classe d'audit ou pour placer l'événement dans une classe à part. Lorsque vous reconfigurez les mappages événements-classes d'audit d'un système, vous devez copier la modification sur tous les systèmes audités.

1 **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **(Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_event`.**

```
# cp /etc/security/audit_event /etc/security/audit_event.orig
```

3 **Modifiez la classe à laquelle appartiennent des événements particuliers en modifiant la valeur *class-list* de ces événements.**

Chaque entrée possède le format suivant :

number:*name*:*description*:*class-list*

number	ID de l'événement d'audit.
name	Nom de l'événement d'audit.
description	En règle générale, l'appel système ou l'exécutable qui déclenche la création d'un enregistrement d'audit.
class-list	Liste de classes d'audit séparées par des virgules.

Exemple 30–11 Mappage d'événements d'audit existants sur une nouvelle classe

Cet exemple permet de mapper un événement d'audit existant sur la nouvelle classe créée dans l'Exemple 30–10. Dans le fichier `audit_control`, l'enregistrement d'audit binaire capture les réussites et échecs des événements de la classe `pf`. Le journal d'audit `syslog` contient uniquement les échecs des événements de la classe `pf`.

```
# grep pf | /etc/security/audit_class
0x10000000:pf:profile command
# vi /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
# vi audit_control
...
flags:lo,pf
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
```

```
plugin:name=audit_syslog.so; p_flags=-lo,-pf
```

Exemple 30–12 Audit de l'utilisation des programmes `setuid`

Cet exemple crée une classe qui contiendra les événements surveillant les appels des programmes `setuid` et `setgid`. L'enregistrement d'audit binaire capture les réussites et échecs des événements des classes `lo` et `na`, et les réussites des événements de la classe `st`. Le journal d'audit `syslog` contient uniquement les réussites des événements de la classe `st`.

```
# vi /etc/security/audit_class
0x00000800:st:setuid class
# vi /etc/security/audit_event
26:AUE_SETGROUPS:setgroups(2):st
27:AUE_SETPGRP:setpgrp(2):st
40:AUE_SETREUID:setreuid(2):st
41:AUE_SETREGID:setregid(2):st
214:AUE_SETEGID:setegid(2):st
215:AUE_SETEUID:seteuid(2):st

# vi audit_control
## audit_control file
flags:lo,+st
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,+st
```

Configuration et activation du service d'audit (liste des tâches)

La liste des tâches suivante présente les procédures de configuration et d'activation du service d'audit. Les tâches sont triées.

Tâche	Description	Voir
1. (Facultatif) Modification des fichiers de configuration d'audit	Sélectionne les événements, les classes et les utilisateurs qui nécessitent un audit.	“Configuration des fichiers d'audit (liste des tâches) ” à la page 620
2. Création des partitions d'audit	Crée de l'espace disque pour les fichiers d'audit, et les protège à l'aide d'autorisations de fichiers.	“Création des partitions pour les fichiers d'audit” à la page 631
3. Création de l'alias `audit_warn`	Définit le destinataire des e-mails d'avertissement lorsque le service d'audit requiert l'attention d'un utilisateur.	“Configuration de l'alias de messagerie `audit_warn` ” à la page 635
4. (Facultatif) Modification de la stratégie d'audit	Définit d'autres données d'audit dont votre site a besoin.	“Configuration de la stratégie d'audit” à la page 635

Tâche	Description	Voir
6. Configuration de l'audit dans les zones non globales	Active les zones non globales pour collecter les enregistrements d'audit.	"Configuration du service d'audit dans les zones (tâches) " à la page 642
7. Activation de l'audit	Active le service d'audit.	"Activation du service d'audit " à la page 638
	Quand l'audit `perzone` est activé, autorise l'audit dans une zone non globale.	Exemple 30–20
8. (Facultatif) Désactivation de l'audit	Désactive le service d'audit.	"Désactivation du service d'audit " à la page 640
	Quand l'audit `perzone` est activé, empêche l'audit dans une zone non globale.	Exemple 30–25
9. (Facultatif) Relecture des modifications de configuration de l'audit	Lisez les modifications de configuration de l'audit dans le noyau pendant que le démon `auditd` est en cours d'exécution.	"Mise à jour du service d'audit " à la page 641

Configuration et activation du service d'audit (tâches)

Une fois que les fichiers de configuration ont été configurés pour votre site, vous devez définir une partie de l'espace disque pour vos fichiers d'audit. Vous avez également besoin de configurer d'autres attributs du service d'audit, puis d'activer le service. Cette section contient également des procédures d'actualisation du service d'audit lorsque vous modifiez les paramètres de configuration.

Lorsqu'une zone non globale est installée, vous pouvez choisir d'auditer cette zone exactement comme la zone globale qui est en cours d'audit. Si vous décidez d'auditer la zone non globale séparément, vous pouvez également modifier les fichiers de configuration d'audit dans la zone non globale. Pour personnaliser les fichiers de configuration d'audit, reportez-vous à la section "Configuration des fichiers d'audit (liste des tâches) " à la page 620.

▼ Création des partitions pour les fichiers d'audit

La procédure suivante décrit la création de partitions pour les fichiers d'audit, ainsi que les systèmes de fichiers et répertoires correspondants. Passez les étapes qui vous semblent inutiles si vous avez déjà une partition vide ou si vous avez déjà monté un fichier de fichiers vide.

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Déterminez la quantité d'espace disque requis.

Attribuez au moins 200 Mo d'espace disque par hôte. Toutefois, le type d'audit dont vous avez besoin dicte l'espace disque requis. Par conséquent, elles peuvent être beaucoup plus élevées que cette figure. N'oubliez pas d'inclure une partition locale pour un répertoire de dernier recours.

3 Créez des partitions d'audit dédiées, si nécessaire.

Cette étape est plus facile à réaliser au cours de l'installation du serveur. Vous pouvez également créer les partitions sur les disques qui n'ont pas encore été montés sur le serveur. Pour obtenir des instructions complètes sur la façon de créer les partitions, reportez-vous au Chapitre 11, “Administering Disks (Tasks)” du *System Administration Guide: Devices and File Systems*.

```
# newfs /dev/rdsk/cwtxdysz
```

où `/dev/rdsk/c`*w*`t` *x*`d`*y*`s` *z* est le nom du périphérique brut pour la partition.

Si l'hôte local est audité, créez également un répertoire d'audit de dernier recours pour cet hôte.

4 Créez des points de montage pour chaque nouvelle partition.

```
# mkdir /var/audit/server-name.n
```

où *server-name.n* est le nom de serveur, plus un nombre qui identifie chaque partition. Le nombre est facultatif, mais il s'avère utile lorsqu'il y a plusieurs répertoires d'audit.

5 Ajoutez des entrées pour monter automatiquement les nouvelles partitions.

Ajoutez une ligne au fichier `/etc/vfstab` comme suit :

```
/dev/dsk/cwtxdysz /dev/rdsk/cwtxdysz /var/audit/server-name.n   ufs  2  yes
```

6 (Facultatif) Supprimez le seuil d'espace disponible minimum sur chaque partition.

Si vous utilisez la configuration par défaut, un avertissement est généré lorsque le répertoire est plein à 80 %. Cet avertissement supprime la raison de réserver de l'espace disponible sur la partition.

```
# tunefs -m 0 /var/audit/server-name.n
```

7 Montez les nouvelles partitions d'audit.

```
# mount /var/audit/server-name.n
```

8 Créez les répertoires d'audit sur les nouvelles partitions.

```
# mkdir /var/audit/server-name.n/files
```

9 Corrigez les autorisations des points de montage et nouveaux répertoires.

```
# chmod -R 750 /var/audit/server-name.n/files
```

10 Sur un serveur de fichiers, définissez les systèmes de fichiers qui doivent être mis à la disposition d'autres hôtes.

Souvent, des parcs de disques sont installés pour stocker les enregistrements d'audit. Si un répertoire d'audit doit être utilisé par plusieurs systèmes, alors le répertoire doit être partagé par l'intermédiaire du service NFS. Pour chaque répertoire, ajoutez une entrée semblable à ce qui suit dans le fichier `/etc/dfs/dfstab` :

```
share -F nfs /var/audit/server-name.n/files
```

11 Sur un serveur de fichiers, redémarrez le service NFS.

Si cette commande est la première commande `share` ou le premier ensemble de commandes `share` que vous lancez, les démons NFS peuvent ne pas être en cours d'exécution.

- **Si le service NFS est hors ligne, activez le service.**

```
% svcs \*nfs\*
disabled       Nov_02   svc:/network/nfs/rquota:default
offline        Nov_02   svc:/network/nfs/server:default
# svcadm enable network/nfs/server
```

- **Si le service NFS est en cours d'exécution, redémarrez le service.**

```
% svcs \*nfs\*
online         Nov_02   svc:/network/nfs/client:default
online         Nov_02   svc:/network/nfs/server:default
# svcadm restart network/nfs/server
```

Pour plus d'informations sur le service NFS, reportez-vous à la section "Configuration des services NFS" du *Guide d'administration système : Services réseau*. Pour plus d'informations sur la gestion des services persistants, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base* et à la page de manuel `smf(5)`.

Exemple 30–13 Création d'un répertoire d'audit de dernier recours

Tous les systèmes qui exécutent le service d'audit doivent avoir un système de fichiers local qui peut être utilisé si aucun autre système de fichiers n'est disponible. Dans cet exemple, un système de fichiers est ajouté à un système appelé `egret`. Étant donné que ce système de fichiers est uniquement utilisé en local, les étapes liées au serveur de fichiers ne sont pas nécessaires.

```
# newfs /dev/rdsk/c0t2d0
# mkdir /var/audit/egret
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1  /dev/rdsk/c0t2d0s1  /var/audit/egret ufs  2  yes  -
# tunefs -m 0 /var/audit/egret
# mount /var/audit/egret
# mkdir /var/audit/egret/files
# chmod -R 750 /var/audit/egret/files
```

Exemple 30–14 Création de partitions d'audit

Dans cet exemple, un nouveau système de fichiers est créé sur deux nouveaux disques qui doivent être utilisés par d'autres systèmes du réseau.

```
# newfs /dev/rdsk/c0t2d0
# newfs /dev/rdsk/c0t2d1
# mkdir /var/audit/egret.1
# mkdir /var/audit/egret.2
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1  /dev/rdsk/c0t2d0s1  /var/audit/egret.1 ufs  2  yes  -
/dev/dsk/c0t2d1s1  /dev/rdsk/c0t2d1s1  /var/audit/egret.2 ufs  2  yes  -
# tunefs -m 0 /var/audit/egret.1
# tunefs -m 0 /var/audit/egret.2
# mount /var/audit/egret.1
# mount /var/audit/egret.2
# mkdir /var/audit/egret.1/files
# mkdir /var/audit/egret.2/files
# chmod -R 750 /var/audit/egret.1/files /var/audit/egret.2/files
# grep egret /etc/dfs/dfstab
 share -F nfs /var/audit/egret.1/files
 share -F nfs /var/audit/egret.2/files
# svcadm enable network/nfs/server
```

Exemple 30–15 Création de partitions d'audit ZFS

Dans cet exemple, l'administrateur exécute la commande `script` après la création des partitions d'audit ZFS. Le tableau ci-dessous présente la sortie de la commande :

```
# zpool create auditf mirror c0t4d0 c0t5d0
# zfs create -o mountpoint=/audit auditf/audit
# zfs create auditf/audit/noddy
# zfs create auditf/audit/noddy/files
# zfs create auditf/audit/blinken
# zfs create auditf/audit/blinken/files
# zfs set devices=off auditf/audit
# zfs set exec=off auditf/audit
# zfs set setuid=off auditf/audit
# zfs set sharenfs=on auditf/audit
# share
-               /audit/blinken/files   rw   ""
-               /audit/noddy   rw   ""
-               /audit/blinken   rw   ""
-               /audit/noddy/files   rw   ""
-               /audit   rw   ""
# ^D
script done on Fri Apr 10 10:10:20 2009
```

L'administrateur affiche ensuite les montages à partir d'un système distant, `remotesys`.

```
# dfshares remotesys
RESOURCE                                SERVER ACCESS    TRANSPORT
remotesys:/audit/blinken/files       remotesys  -         -
remotesys:/audit/noddy               remotesys  -         -
remotesys:/audit/blinken             remotesys  -         -
```

```
remotesys:/audit/noddy/files         remotesys  -         -
remotesys:/audit                     remotesys  -         -
```

Enfin, l'administrateur monte le système de fichiers `/audit` sur `/var/audit`.

```
# mount remotesys:/audit /var/audit
# ls /var/audit
blinken  noddy
```

Configuration de l'alias de messagerie `audit_warn`

Le script `audit_warn` génère un e-mail à un alias de messagerie appelé `audit_warn`. Pour envoyer ce message à une adresse e-mail valide, vous pouvez suivre l'une des options décrites dans l'Étape 2:

1 Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Configurez l'alias de messagerie `audit_warn`.

Procédez de l'une des manières suivantes :

- **OPTION 1** : remplacez l'alias de messagerie `audit_warn` par un autre compte de messagerie dans le script `audit_warn`.

  Modifiez l'alias de messagerie dans la ligne suivante du script :

  ```
  ADDRESS=audit_warn            # standard alias for audit alerts
  ```

- **OPTION 2** : redirigez l'e-mail `audit_warn` vers un autre compte de messagerie.

  Dans ce cas, vous devez ajouter l'alias de messagerie `audit_warn` au fichier d'alias de messagerie approprié. Vous pouvez ajouter l'alias au fichier local `/etc/mail/aliases` ou à la base de données `mail_aliases` de l'espace de noms. La nouvelle entrée doit ressembler à ce qui suit si le compte de messagerie `root` a été défini comme membre de l'alias de messagerie `audit_warn` :

  ```
  audit_warn: root
  ```

Configuration de la stratégie d'audit

La stratégie d'audit détermine les caractéristiques des enregistrements d'audit pour l'hôte local. Lorsque l'audit est activé, le contenu du fichier `/etc/security/audit_startup` détermine la stratégie d'audit.

Vous pouvez vérifier et modifier les options de la stratégie d'audit en cours avec la commande `auditconfig`. Vous pouvez également modifier les options de stratégie de la commande `auditconfig` dans le script `audit_startup` pour que les modifications apportées à la stratégie d'audit deviennent permanentes.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil Audit Control.

Pour créer un rôle incluant le profil Audit Control et l'affecter à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 Vérifiez la stratégie d'audit.

Avant l'activation de l'audit, le contenu du fichier `audit_startup` détermine la stratégie d'audit :

```
#! /bin/sh
...
/usr/bin/echo "Starting BSM services."
/usr/sbin/auditconfig -setpolicy +cnt       Counts rather than drops records
/usr/sbin/auditconfig -conf       Configures event-class mappings
/usr/sbin/auditconfig -aconf      Configures nonattributable events
```

3 Affichez les options de stratégie disponibles.

```
$ auditconfig -lspolicy
```

Remarque – Les options de stratégie et `ahlt` peuvent être définies uniquement dans la zone globale.

---

4 Activez ou désactivez les options de stratégie d'audit sélectionnées.

```
# auditconfig -setpolicy prefixpolicy
```

prefix Si *prefix* possède la valeur +, l'option de stratégie est activée. Si *prefix* possède la valeur -, l'option de stratégie est désactivée.

policy Sélectionne la stratégie à activer ou désactiver.

La stratégie est en vigueur jusqu'à la prochaine initialisation ou jusqu'à ce que la stratégie soit modifiée par la commande `auditconfig -setpolicy`.

Pour obtenir une description de chaque option de stratégie, reportez-vous à la section "Détermination de la stratégie d'audit" à la page 611.

Exemple 30–16 Définition des options de stratégie d'audit `cnt` et `ahlt`

Dans cet exemple, la stratégie `cnt` est désactivée et la stratégie `ahlt` est activée. À l'aide de ces paramètres, l'utilisation du système est interrompue lorsque les partitions d'audit sont complètes et qu'un événement asynchrone se produit. Lorsqu'un événement synchrone se

produit, le processus qui a créé le thread se bloque. Ces paramètres sont appropriés lorsque la sécurité est plus importante que la disponibilité.

Les entrées `audit_startup` suivantes désactivent l'option de stratégie `cnt` et activent l'option de stratégie `ahlt` d'un redémarrage à l'autre :

```
# cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy -cnt
/usr/sbin/auditconfig -setpolicy +ahlt
```

Exemple 30–17 Définition temporaire de la stratégie d'audit `seq`

Dans cet exemple, le démon `auditd` est en cours d'exécution et la stratégie d'audit `ahlt` a été définie. La stratégie d'audit `seq` est ajoutée à la stratégie actuelle. La stratégie d'audit `seq` ajoute un jeton `sequence` à chaque enregistrement d'audit. Cette option est utile pour le débogage du service d'audit lorsque les enregistrements d'audit sont corrompus, ou lorsque les enregistrements sont ignorés.

Le préfixe + ajoute l'option `seq` à la stratégie d'audit, plutôt que de remplacer la stratégie d'audit en cours par `seq`. La commande `auditconfig` rend la stratégie effective jusqu'au prochain appel de la commande, ou jusqu'à la prochaine initialisation.

```
$ auditconfig -setpolicy +seq
$ auditconfig -getpolicy
audit policies = ahlt,seq
```

Exemple 30–18 Définition de la stratégie d'audit `perzone`

Dans cet exemple, la stratégie d'audit `perzone` est définie dans le script `audit_startup` de la zone globale. Lors de l'initialisation d'une zone, la zone non globale recueille les enregistrements d'audit en fonction de la configuration de l'audit définie dans sa zone.

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +perzone
/usr/sbin/auditconfig -setpolicy +cnt
```

Exemple 30–19 Modification d'une stratégie d'audit

Dans cet exemple, le démon d'audit est en cours d'exécution et la stratégie d'audit a été définie. La commande `auditconfig` modifie les stratégies `ahlt` et `cnt` pour la durée de la session. À l'aide de ces paramètres, les enregistrements d'audit sont supprimés, mais comptabilisés, lorsque le système de fichiers d'audit est plein. Pour connaître les restrictions qui s'appliquent à la définition de la stratégie `ahlt`, reportez-vous à l'Étape 3.

```
$ auditconfig -setpolicy +cnt
$ auditconfig -setpolicy -ahlt
$ auditconfig -getpolicy
audit policies = cnt,seq
```

Une fois les modifications insérées dans le fichier `audit_startup`, les stratégies entrent définitivement en vigueur :

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +cnt
```

L'option `-ahlt` n'a pas à être spécifiée dans le fichier, car l'option de stratégie `ahlt` est désactivée par défaut. Ce paramètre est approprié lorsque la disponibilité est plus importante que la sécurité fournie par les enregistrements d'audit.

▼ Activation du service d'audit

Cette procédure permet d'activer le service d'audit pour toutes les zones. Pour démarrer le démon d'audit dans une zone non globale, reportez-vous à l'Exemple 30–20.

Lorsque l'audit est configuré de manière sécurisée, le système est en mode monoutilisateur jusqu'à ce que l'audit soit activé. Vous pouvez également activer l'audit en mode multiutilisateur.

Avant de commencer

Vous devez effectuer cette procédure en tant que superutilisateur après avoir terminé les tâches suivantes :

- Planification : “Planification de l'audit Oracle Solaris (liste des tâches) ” à la page 605
- Personnalisation des fichiers d'audit : “Configuration des fichiers d'audit (liste des tâches) ” à la page 620
- Configuration des partitions d'audit : “Création des partitions pour les fichiers d'audit” à la page 631

- Configuration des messages d'avertissement d'audit : "Configuration de l'alias de messagerie audit_warn " à la page 635
- Définition de la stratégie d'audit : "Configuration de la stratégie d'audit" à la page 635

Remarque – Pour que l'audit fonctionne, le nom d'hôte doit être correctement traduit. La base de données `hosts` dans les services de nommage doit être correctement configurée et en état de fonctionner.

Pour connaître la procédure de configuration de la base de données hosts, reportez-vous aux pages de manuel `nsswitch.conf`(4) et `netconfig`(4). Pour plus d'informations, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* ou au *System Administration Guide: Naming and Directory Services (NIS+)* .

---

1 Exécutez le script qui active le service d'audit.

Accédez au répertoire `/etc/security` et exécutez le script `bsmconv`.

```
# cd /etc/security
# ./bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation.

The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

Pour connaître les effets de ce script, reportez-vous à la page de manuel `bsmconv`(1M).

2 Redémarrez le système.

```
# reboot
```

Le fichier de démarrage `/etc/security/audit_startup` entraîne l'exécution automatique du démon `auditd` lorsque le système entre en mode multiutilisateur.

Un autre effet de ce script est d'activer l'allocation de périphériques. Pour configurer l'allocation de périphériques, reportez-vous à la section "Gestion de l'allocation des périphériques (liste des tâches) " à la page 87.

Exemple 30–20 Activation de l'audit dans une zone non globale

Dans l'exemple ci-après, l'administrateur de la zone globale activé dans la stratégie `perzone` une fois l'audit terminé l'a également été dans la zone globale et après le démarrage de la zone non globale. L'administrateur de zone de la zone non globale a configuré les fichiers d'audit de la zone, puis démarré le démon d'audit dans la zone.

```
zone1# svcadm enable svc:/system/auditd
```

▼ Désactivation du service d'audit

Si le service d'audit n'est plus nécessaire à un moment donné, cette procédure renvoie le système à l'état du système avant l'activation de l'audit. Si les zones non globales sont en cours d'audit, leur service d'audit est également désactivé.

Attention – Cette commande désactive également l'allocation de périphériques. N'exécutez pas cette commande si vous souhaitez pouvoir allouer des périphériques. Pour désactiver l'audit et conserver l'allocation de périphériques, reportez-vous à l'Exemple 30–21.

1 Connectez-vous en tant que superutilisateur et placez le système en mode monoutilisateur.

```
% su
Password:       <Type root password>
# init S
```

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

2 Exécutez le script pour désactiver l'audit.

Accédez au répertoire `/etc/security` et exécutez le script `bsmunconv`.

```
# cd /etc/security
# ./bsmunconv
```

Un autre effet de ce script est de désactiver l'allocation de périphériques.

Pour plus d'informations sur l'effet du script `bsmunconv`, reportez-vous à la page de manuel `bsmconv(1M)`.

3 Placez le système en mode multiutilisateur.

```
# init 6
```

Exemple 30–21 Désactivation de l'audit et maintien de l'allocation de périphériques

Dans cet exemple, le service d'audit ne cesse de collecter les enregistrements, mais l'allocation de périphériques continue à fonctionner. Toutes les valeurs des entrées `flags`, `naflags` et `plugin` dans le fichier `audit_control` sont supprimées, tout comme les entrées d'utilisateur dans le fichier `audit_user`.

```
## audit_control file
flags:
naflags:

## audit_user file
```

Le démon `auditd` s'exécute, mais aucun enregistrement d'audit n'est conservé.

Exemple 30–22 Désactivation de l'audit zone par zone

Dans cet exemple, le service d'audit arrête son exécution dans `zone1` où le service d'audit est désactivé. L'allocation de périphériques continue à fonctionner. Si cette commande est exécutée dans la zone globale, et si la stratégie d'audit `perzone` n'est pas définie, l'audit est désactivé pour toutes les zones, pas seulement dans la zone globale.

```
zone1 # audit -t
```

▼ Mise à jour du service d'audit

Cette procédure redémarre le démon `auditd` si, après son exécution, vous avez apporté des modifications aux fichiers de configuration d'audit.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits Audit Control.**

Pour créer un rôle incluant le profil de droits Audit Control et l'affecter à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 **Choisissez la commande appropriée.**

- **Si vous modifiez la ligne `naflags` dans le fichier `audit_control`, modifiez le masque de noyau pour les événements non allouables.**

  ```
  $ /usr/sbin/auditconfig -aconf
  ```

  Vous pouvez également réinitialiser.

- **Si vous modifiez d'autres lignes dans le fichier `audit_control`, relisez le fichier `audit_control`.**

  Le démon d'audit stocke des informations à partir du fichier `audit_control` en interne. Pour utiliser les nouvelles informations, redémarrez le système ou demandez au démon d'audit de lire le fichier modifié.

  ```
  $ /usr/sbin/audit -s
  ```

  Remarque – Les enregistrements d'audit sont générés en fonction du masque de présélection d'audit associé à chaque processus. L'exécution de la commande `audit -s` *ne modifie pas* les masques dans les processus existants. Pour changer le masque de présélection pour un processus existant, vous devez redémarrer le processus. Vous pouvez également réinitialiser.

Avec la commande `audit -s`, le démon d'audit relit le répertoire et les valeurs minfree du fichier `audit_control`. La commande modifie la génération du masque de présélection pour les processus générés par les connexions suivantes.

- **Si vous modifiez le fichier `audit_event` ou `audit_class` pendant que le démon d'audit est en cours d'exécution, actualisez le service d'audit.**

  Lisez les mappages événements-classes modifiés dans le système et assurez-vous que chaque utilisateur qui utilise l'ordinateur est correctement audité.

  ```
  $ auditconfig -conf
  $ auditconfig -setumask auid classes
  ```

  auid ID utilisateur.

  classes Classes d'audit présélectionnées.

  Pour obtenir un exemple, reportez-vous à la section "Modification d'un masque de présélection utilisateur" à la page 664.

- **Pour modifier une stratégie d'audit sur un système en cours d'exécution, reportez-vous à l'Exemple 30–17.**

Exemple 30–23 Redémarrage du démon d'audit

Dans cet exemple, le système est arrêté en mode monoutilisateur, puis sauvegardé en mode multiutilisateur. Lorsque le système est en mode multiutilisateur, les fichiers de configuration d'audit modifiés sont lus dans le système.

```
# init S
# init 6
```

Configuration du service d'audit dans les zones (tâches)

Le service d'audit effectue des audits sur la totalité du système, y compris les événements d'audit dans les zones. Un système doté de zones non globales peut auditer toutes les zones de manière identique, ou contrôler l'audit par zone. Pour de plus amples détails, reportez-vous à la section "Audit sur un système à zones Oracle Solaris" à la page 602. Pour la planification, reportez-vous à la section "Procédure de planification de l'audit par zone " à la page 606.

▼ Configuration identique de toutes les zones pour l'audit

Cette procédure permet d'auditer chaque zone de manière identique. Cette méthode est celle qui requiert le temps système le moins important de ressources en administration.

1 Configurez la zone globale pour l'audit.

a. Effectuez les tâches de la section "Configuration des fichiers d'audit (liste des tâches) " à la page 620.

b. Effectuez les tâches de la section "Configuration et activation du service d'audit (liste des tâches) " à la page 630, à l'exception des points suivants.

- N'activez pas la stratégie d'audit `perzone`.
- N'activez pas le service d'audit. Vous pouvez activer le service d'audit après avoir configuré les zones non globales pour l'audit.

2 Copiez les fichiers de configuration d'audit de la zone globale vers chaque zone non globale.

Copiez l'un des fichiers suivants modifiés : `audit_class`, `audit_control`, `audit_event`, `audit_user`. Ne copiez pas `audit_startup` ou `audit_warn`. Vous n'avez pas à copier des fichiers que vous n'avez pas modifiés.

Deux options s'offrent à vous : En tant que superutilisateur, vous pouvez copier les fichiers, ou monter les fichiers en loopback. La zone non globale doit être en cours d'exécution.

- **Copiez les fichiers.**

  a. À partir de la zone globale, répertoriez le répertoire `/etc/security` dans la zone non globale.

  ```
  # ls /zone/zonename/etc/security/
  ```

  b. Copiez les fichiers de configuration d'audit dans le répertoire `/etc/security` de la zone.

  ```
  # cp /etc/security/audit-file /zone/zonename/etc/security/audit-file
  ```

  Par la suite, si vous modifiez un fichier de configuration d'audit dans la zone globale, vous devez copier à nouveau le fichier dans les zones non globales.

- **Montez en loopback les fichiers de configuration.**

  a. À partir de la zone globale, arrêtez la zone non globale.

  ```
  # zoneadm -z non-global-zone halt
  ```

b. Créez un montage loopback en lecture seule pour chaque fichier de configuration d'audit que vous avez modifié dans la zone globale.

```
# zonecfg -z non-global-zone
 add fs
    set special=/etc/security/audit-file
    set dir=/etc/security/audit-file
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 exit
```

c. Pour valider les changements, initialisez la zone non globale.

```
# zoneadm -z non-global-zone boot
```

Vous pouvez également redémarrer le système.

Par la suite, si vous modifiez un fichier de configuration d'audit dans la zone globale, redémarrez le système pour actualiser les fichiers montés en loopback dans les zones non globales.

Exemple 30–24 Montage en loopback des fichiers de configuration d'audit

Dans cet exemple, l'administrateur système a modifié les fichiers `audit_class`, `audit_event`, `audit_control`, `audit_user`, `audit_startup` et `audit_warn`.

Les fichiers `audit_startup` et `audit_warn` sont lus dans la zone globale uniquement, de sorte qu'ils n'ont pas à être montés en loopback dans les zones non globales.

Sur ce système, `machine1`, l'administrateur a créé deux zones non globales, `machine1–webserver` et `machine1–appserver`. L'administrateur a terminé la personnalisation des fichiers de configuration d'audit. Si l'administrateur modifie ultérieurement les fichiers, le système sera redémarré pour valider les changements.

```
# zoneadm -z machine1-webserver halt
# zoneadm -z machine1-appserver halt
# zonecfg -z machine1-webserver
 add fs
    set special=/etc/security/audit_class
    set dir=/etc/security/audit_class
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 add fs
    set special=/etc/security/audit_event
    set dir=/etc/security/audit_event
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 add fs
    set special=/etc/security/audit_control
    set dir=/etc/security/audit_control
```

```
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
add fs
    set special=/etc/security/audit_user
    set dir=/etc/security/audit_user
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
 exit
# zonecfg -z machine1-appserver
 add fs
    set special=/etc/security/audit_class
    set dir=/etc/security/audit_class
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
...
 exit
```

Lorsque les zones sont redémarrées, les fichiers de configuration d'audit sont en lecture seule dans les zones.

▼ Configuration de l'audit par zone

Cette procédure permet aux administrateurs de zones distinctes de contrôler le service d'audit dans leur zone. Pour obtenir la liste complète des options de stratégie, reportez-vous à la page de manuel `auditconfig(1M)`.

1 Dans la zone globale, configurez l'audit mais n'activez pas le service d'audit.

a. Effectuez les tâches de la section "Configuration des fichiers d'audit (liste des tâches) " à la page 620.

b. Effectuez les tâches de la section "Configuration et activation du service d'audit (liste des tâches) " à la page 630, à l'exception des points suivants.

- Ajoutez la stratégie d'audit `perzone`. Pour consultez un exemple, reportez-vous à l'Exemple 30–18.
- N'activez pas le service d'audit. Vous pouvez activer le service d'audit après la configuration des zones non globales pour l'audit.

2 Dans chaque zone non globale, configurez les fichiers d'audit.

Remarque – Si vous effectuez une planification pour désactiver l'audit dans la zone non globale, vous pouvez ignorer cette étape. Pour désactiver l'audit, reportez-vous à l'Exemple 30–25.

---

a. **Effectuez les tâches de la section "Configuration des fichiers d'audit (liste des tâches) " à la page 620.**

b. **Suivez les procédures décrites à la section "Configuration et activation du service d'audit (liste des tâches) " à la page 630.**

c. **Ne configurez pas les paramètres d'audit système.**

   En particulier, n'ajoutez pas la stratégie `perzone` ou `ahlt` du fichier `audit_startup` de la zone non globale. N'exécutez pas la commande `bsmconv` à partir de la zone non globale.

d. **Activez l'audit dans votre zone.**

   Lorsqu'une zone globale redémarre après la configuration de l'audit, celui-ci est automatiquement activé dans votre zone.

   Si l'administrateur de la zone globale active la stratégie d'audit `perzone` après l'initialisation du système, les administrateurs de zones individuelles doivent activer l'audit. Pour plus d'informations, reportez-vous à l'Exemple 30–20.

3 **Dans la zone globale, activez le service d'audit.**

Pour connaître la procédure, reportez-vous à la section "Activation du service d'audit " à la page 638.

Exemple 30–25 Désactivation de l'audit dans une zone non globale

Cet exemple fonctionne si la zone globale a défini la stratégie d'audit `perzone`. L'administrateur de zone de la zone `noaudit` désactive l'audit pour cette zone. Étant donné que l'administrateur a prévu de désactiver l'audit, il n'a pas modifié les fichiers de configuration d'audit.

```
noauditzone # svcadm disable svc:/system/auditd
```

Gestion des enregistrements d'audit (liste des tâches)

La liste des tâches suivante présente les procédures de sélection, d'analyse et de gestion des enregistrements d'audit.

Tâche	Description	Voir
Affichage des formats des enregistrements d'audit	Affiche le type d'informations collectées pour un événement d'audit et l'ordre dans lequel les informations sont présentées.	"Affichage des formats d'enregistrement d'audit " à la page 647

Tâche	Description	Voir
Fusion des enregistrements d'audit	Combine des fichiers d'audit provenant de plusieurs machines dans une seule piste d'audit.	"Fusion des fichiers d'audit de la piste d'audit " à la page 649
Sélection des enregistrements à examiner	Sélectionne des événements particuliers à examiner.	"Sélection des événements d'audit de la piste d'audit " à la page 650
Affichage des enregistrements d'audit	Vous permet d'afficher des enregistrements d'audit binaires.	"Affichage du contenu des fichiers d'audit binaires" à la page 653
Nettoyage de fichiers d'audit portant un nom incorrect	Fournit un horodatage de fin pour les fichiers d'audit qui ont été accidentellement laissés ouverts par le service d'audit.	"Nettoyage d'un fichier d'audit `not_terminated` " à la page 654
Contrôle du dépassement de la piste d'audit	Empêche l'accumulation d'un nombre trop important de fichiers d'audit dans le système de fichiers d'audit.	"Contrôle du dépassement de la piste d'audit" à la page 655

Gestion des enregistrements d'audit

En gérant la piste d'audit, vous pouvez surveiller les actions des utilisateurs de votre réseau. L'audit peut générer de grandes quantités de données. Les tâches suivantes vous indiquent comment travailler avec toutes ces données.

▼ Affichage des formats d'enregistrement d'audit

Pour écrire des scripts qui peuvent trouver les données d'audit que vous voulez, vous avez besoin de connaître l'ordre des jetons dans un événement d'audit. La commande `bsmrecord` affiche le nombre d'événements d'audit, la classe d'audit, le masque de sélection et le format d'enregistrement d'un événement d'audit.

- **Placez le format de tous les enregistrements d'événements d'audit dans un fichier HTML.**

  L'option `-a` répertorie tous les formats d'enregistrement d'événements d'audit. L'option `-h` place la liste au format HTML qui peut être affiché dans un navigateur.

  ```
  % bsmrecord -a -h > audit.events.html
  ```

  Lorsque vous affichez le fichier `*html` dans un navigateur, utilisez l'outil de recherche du navigateur pour rechercher des enregistrements spécifiques.

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

Exemple 30–26 Affichage des formats d'enregistrement d'audit d'un programme

Dans cet exemple, le format de tous les enregistrements d'audit sont générés par le programme `login` est affiché. Les programmes login incluent `rlogin`, `telnet`, `newgrp`, ainsi que la connexion de rôle de la console de gestion Solaris, et Oracle Solaris Secure Shell.

```
% bsmrecord -p login
login: logout
  program     various              See login(1)
  event ID    6153                 AUE_logout
...

newgrp
  program     newgrp               See newgrp login
  event ID    6212                 AUE_newgrp_login
...

rlogin
  program     /usr/sbin/login      See login(1) - rlogin
  event ID    6155                 AUE_rlogin
...

SMC: role login
  program     SMC server           See role login
  event ID    6173                 AUE_role_login
...

/usr/lib/ssh/sshd
  program     /usr/lib/ssh/sshd    See login - ssh
  event ID    6172                 AUE_ssh
...

telnet login
  program     /usr/sbin/login      See login(1) - telnet
  event ID    6154                 AUE_telnet
  ...
```

Exemple 30–27 Affichage des formats d'enregistrement d'audit d'une classe d'audit

Dans cet exemple, le format de tous les enregistrements d'audit dans la classe `fd` est affiché.

```
% bsmrecord -c fd

rmdir
  system call rmdir                See rmdir(2)
  event ID    48                   AUE_RMDIR
  class       fd                   (0x00000020)
      header
      path
      [attribute]
      subject
      [use_of_privilege]
      return

unlink
  system call unlink               See unlink(2)
  event ID    6                    AUE_UNLINK
  ...

unlinkat
  system call unlinkat             See openat(2)
  event ID    286                  AUE_UNLINKAT
  ...
```

▼ Fusion des fichiers d'audit de la piste d'audit

En fusionnant tous les fichiers d'audit de tous les répertoires d'audit, vous pouvez analyser le contenu de la piste d'audit entière. La commande `auditreduce` fusionne tous les enregistrements à partir de ses fichiers d'entrée dans un seul fichier de sortie. Les fichiers d'entrée peuvent ensuite être supprimés. Lorsque le fichier de sortie est placé dans un répertoire nommé `/etc/security/audit/`*server-name* `/files`, la commande `auditreduce` peut trouver le fichier de sortie sans spécifiant le chemin d'accès complet.

Remarque – Cette procédure s'applique uniquement aux enregistrements d'audit binaires.

---

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil Audit Review.

Ce profil fait partie des prérogatives de l'administrateur système. Vous pouvez également créer un autre rôle, qui inclut le profil Audit Review. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 Créez un répertoire pour stocker les fichiers d'audit fusionnés.

```
# mkdir audit-trail-directory
```

3 Limitez l'accès au répertoire.

```
# chmod 700 audit-trail-directory
# ls -la audit-trail-directory
drwx------   3 root     sys          512 May 12 11:47 .
drwxr-xr-x   4 root     sys         1024 May 12 12:47 ..
```

4 Fusionnez les enregistrements d'audit de la piste d'audit.

Modifiez les répertoires vers *audit-trail-directory* et fusionnez les enregistrements d'audit dans un fichier avec un suffixe nommé. Tous les répertoires de la liste `dir`, dans le fichier `audit_control` du système local, sont fusionnés.

```
# cd audit-trail-directory
# auditreduce -Uppercase-option -O suffix
```

Les options majuscules de la commande `auditreduce` permettent de manipuler les fichiers dans la piste d'audit. Les options majuscules sont les suivantes :

`-A` Sélectionne tous les fichiers de la piste d'audit.

`-C` Sélectionne les fichiers complets uniquement. Cette option ignore les fichiers avec le suffixe `not_terminated`.

`-M` Sélectionne les fichiers avec un suffixe donné. Le suffixe peut être un nom de machine ou un suffixe que vous avez spécifié pour un fichier résumé.

`-O` Crée un fichier d'audit avec des horodatages de 14 caractères pour l'heure de début et l'heure de fin, avec le suffixe *suffix* dans le répertoire en cours.

Exemple 30–28 Copie des fichiers d'audit pour un fichier résumé

Dans l'exemple suivant, le rôle d'administrateur système, `sysadmin`, copie tous les fichiers de la piste d'audit dans un fichier fusionné.

```
$ whoami
sysadmin
$ mkdir /var/audit/audit_summary.dir
$ chmod 700 /var/audit/audit_summary.dir
$ cd /var/audit/audit_summary.dir
$ auditreduce -A -O All
$ ls *All
20100827183214.20100827215318.All
```

Dans l'exemple suivant, seuls les fichiers sont copiés à partir de la piste d'audit dans un fichier fusionné.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O Complete
$ ls *Complete
20100827183214.20100827214217.Complete
```

Dans l'exemple suivant, seuls les fichiers complets sont copiés à partir de la machine `example1` dans un fichier fusionné.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -M example1 -O example1summ
$ ls *summ
20100827183214.20100827214217.example1summ
```

Exemple 30–29 Déplacement de fichiers d'audit dans un fichier résumé

L'option `-D` de la commande `auditreduce` supprime un fichier d'audit lorsque vous la copiez dans un autre emplacement. Dans l'exemple suivant, les fichiers d'audit complets d'un système sont copiés dans le répertoire résumé pour être examinés à une date ultérieure.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O daily_example1 -D example1
$ ls *example1
20100827183214.20100827214217.daily_example1
```

Les fichiers d'audit du système `example1`, entrées du fichier `*daily_example1`, sont supprimés lorsque cette commande se termine.

▼ Sélection des événements d'audit de la piste d'audit

Vous pouvez filtrer les enregistrements d'audit pour les examiner. Pour obtenir la liste complète des options de filtrage, reportez-vous à la page de manuel `auditreduce(1M)`.

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil Audit Review.**

   Ce profil fait partie des prérogatives de l'administrateur système. Vous pouvez également créer un autre rôle, qui inclut le profil Audit Review. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2. **Sélectionnez les types d'enregistrements que vous souhaitez dans la piste d'audit, ou à partir d'un fichier d'audit spécifié.**

   `auditreduce` *-lowercase-option argument* [*optional-file*]

argument	Argument spécifique qui nécessite une option minuscule. Par exemple, l'option `-c` exige un *argument* d'une classe d'audit, tel que `ua`.
`-d`	Sélectionne tous les événements à une date donnée. Le format de date pour *argument* est *aaaammjj*. D'autres options de date, `-b` et `-a`, sélectionnent les événements avant et après une date particulière.
`-u`	Sélectionne tous les événements attribuables à un utilisateur particulier. L'*argument* est un nom d'utilisateur. Une autre option utilisateur, `-e`, sélectionne tous les événements attribuables à un ID d'utilisateur effectif.
`-c`	Sélectionne tous les événements d'une classe d'audit présélectionnée. L'*argument* est un nom de classe d'audit.
`-m`	Sélectionne toutes les instances d'un événement d'audit. L'*argument* est un événement d'audit.
optional-file	Nom d'un fichier d'audit.

Exemple 30–30 Association et réduction des fichiers d'audit

La commande `auditreduce` peut éliminer les enregistrements moins intéressants car elle combine les fichiers d'entrée. Par exemple, vous pouvez utiliser la commande `auditreduce` pour conserver uniquement les enregistrements de connexion et déconnexion dans les fichiers d'audit qui ont plus d'un mois. Si vous avez besoin de récupérer la piste d'audit complète, vous pouvez le faire à partir d'un support de sauvegarde.

```
# cd /var/audit/audit_summary.dir
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

Exemple 30–31 Copie des enregistrements d'audit na dans un fichier résumé

Dans cet exemple, tous les enregistrements d'événements d'audit non attribuables dans la piste d'audit sont regroupés dans un seul fichier.

```
$ whoami
sysadmin
```

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -c na -O nasumm
$ ls *nasumm
20100827183214.20100827215318.nasumm
```

Le fichier d'audit fusionné `nasumm` est horodaté avec la date de début et la date de fin des enregistrements `na`.

Exemple 30–32 Recherche d'événements d'audit dans un fichier d'audit spécifié

Vous pouvez sélectionner les fichiers d'audit manuellement pour rechercher uniquement l'ensemble de fichiers nommé. Par exemple, vous pouvez poursuivre le traitement du fichier `*nasumm` de l'exemple précédent pour trouver les événements de démarrage système. Pour ce faire, vous devez spécifier le nom du fichier comme argument final pour la commande `auditreduce`.

```
$ auditreduce -m 113 -O systemboot 20100827183214.20100827215318.nasumm
20100827183214.20100827183214.systemboot
```

Le fichier `20100827183214.20100827183214.systemboot` ne contient que les événements d'audit du démarrage système.

Exemple 30–33 Copie des enregistrements d'audit d'un utilisateur dans un fichier résumé

Dans cet exemple, les enregistrements de la piste d'audit qui contiennent le nom d'un utilisateur particulier sont fusionnés. L'option `-e` trouve l'utilisateur effectif. L'option `-u` trouve l'utilisateur d'audit.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -e tamiko -O tamiko
```

Vous pouvez rechercher des événements spécifiques dans ce fichier. L'exemple suivant permet de vérifier le moment où l'utilisateur s'est connecté et déconnecté le 7 septembre 2010, votre heure. Seuls les fichiers avec le nom d'utilisateur en tant que suffixe de fichier sont vérifiés. La forme abrégée de la date est *aaaammjj*.

```
# auditreduce -M tamiko -O tamikolo -d 20100907 -u tamiko -c lo
```

Exemple 30–34 Copie des enregistrements sélectionnés dans un seul fichier

Dans cet exemple, les messages de connexion et déconnexion pour un jour particulier sont sélectionnés dans la piste d'audit. Les messages sont fusionnés dans un fichier cible. Le fichier cible est écrit dans un répertoire autre que le répertoire root d'audit.

```
# auditreduce -c lo -d 20100827 -O /var/audit/audit_summary.dir/logins
# ls /var/audit/audit_summary.dir/*logins
/var/audit/audit_summary.dir/20100827183936.20100827232326.logins
```

▼ Affichage du contenu des fichiers d'audit binaires

La commande `praudit` vous permet de visualiser le contenu de fichiers d'audit binaires. Vous pouvez envoyez la sortie de la commande `auditreduce` ou vous pouvez lire un fichier d'audit particulier. L'option `-x` est utile pour un traitement supplémentaire.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil Audit Review.

Ce profil fait partie des prérogatives de l'administrateur système. Vous pouvez également créer un autre rôle, qui inclut le profil Audit Review. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

2 Utilisez l'une des commandes `praudit` suivantes afin de produire la sortie la mieux adaptée à vos besoins.

Les exemples suivants représentent la sortie `praudit` depuis le même événement d'audit. La stratégie d'audit a été définie de façon à inclure les jetons `sequence` et `trailer`.

- La commande `praudit -s` affiche les enregistrements d'audit dans un format court, un jeton par ligne. Utilisez l'option `-l` pour placer chaque enregistrement sur une seule ligne.

```
$ auditreduce -c lo | praudit -s
header,101,2,AUE_rlogin,,example1,2010-10-13 11:23:31.050 -07:00
subject,jdoe,jdoe,staff,jdoe,staff,749,749,195 1234 server1
text,successful login
return,success,0
sequence,1298
```

- La commande `praudit -r` affiche les enregistrements d'audit au format brut, un jeton par ligne. Utilisez l'option `-l` pour placer chaque enregistrement sur une seule ligne.

```
$ auditreduce -c lo | praudit -r
21,101,2,6155,0x0000,192.168.60.83,1062021202,64408258
36,2026700,2026700,10,2026700,10,749,749,195 1234 192.168.60.17
40,successful login
39,0,0
47,1298
```

- La commande `praudit -x` affiche les enregistrements d'audit au format XML, un jeton par ligne. Utilisez l'option `-l` pour placer la sortie XML pour un seul enregistrement sur une seule ligne.

```
$ auditreduce -c lo | praudit -x
<record version="2" event="login - rlogin" host="example1"
time="Wed Aug 27 14:53:22 PDT 2010" msec="64">
<subject audit-uid="jdoe" uid="jdoe" gid="staff" ruid="jdoe"
rgid="staff" pid="749" sid="749" tid="195 1234 server1"/>
<text>successful login</text>
<return errval="success" retval="0"/>
<sequence seq-num="1298"/>

</record>
```

Exemple 30–35 Impression de la piste d'audit complète

À l'aide d'un tube sur la commande `lp`, la sortie de la piste d'audit complète est dirigée vers l'imprimante. L'imprimante doit avoir un accès limité.

```
# auditreduce | praudit | lp -d example.protected.printer
```

Exemple 30–36 Affichage d'un fichier d'audit spécifique

Dans cet exemple, un fichier de connexion résumé est examiné dans une fenêtre de terminal.

```
# cd /var/audit/audit_summary.dir/logins
# praudit 20100827183936.20100827232326.logins | more
```

Exemple 30–37 Création d'enregistrements d'audit au format XML

Dans cet exemple, les enregistrements d'audit sont convertis au format XML.

```
# praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

Le fichier `*xml` peut être affiché dans un navigateur. Le contenu du fichier peut être exécuté par un script pour extraire les informations pertinentes.

Erreurs fréquentes Un message semblable à celui-ci indique que vous ne disposez pas de tous les privilèges nécessaires pour utiliser la commande `praudit` :

```
praudit: Can’t assign 20090408164827.20090408171614.example1 to stdin.
```

▼ Nettoyage d'un fichier d'audit `not_terminated`

Il peut arriver qu'un démon d'audit s'arrête alors que son fichier d'audit est toujours ouvert. Ou, un serveur devient inaccessible et force la machine à passer à un nouveau serveur. Dans de tels cas, un fichier d'audit conserve la chaîne `not_terminated` comme horodatage de fin, même si le fichier n'est plus utilisé pour les enregistrements d'audit. Utilisez la commande `auditreduce -O` pour donner au fichier le bon horodatage.

1 Affichez la liste des fichiers avec la chaîne `not_terminated` sur votre système de fichiers d'audit dans l'ordre de leur création.

```
# ls -R1t audit-directory*/files/* | grep not_terminated
```

`-R` Répertorie les fichiers dans des sous-répertoires.

`-t` Répertorie les fichiers du plus récent au plus ancien.

`-1` Affiche la liste des fichiers dans une seule colonne.

2. **Nettoyez l'ancien fichier `not_terminated`.**

   Spécifiez le nom de l'ancien fichier de la commande `auditreduce -O`.

   ```
   # auditreduce -O system-name old-not-terminated-file
   ```

3. **Supprimez l'ancien fichier `not_terminated`.**

   ```
   # rm system-name old-not-terminated-file
   ```

Exemple 30–38 Nettoyage de fichiers d'audit `not_terminated` fermés

Dans l'exemple suivant, les fichiers `not_terminated` sont trouvés, renommés, puis les originaux sont supprimés.

```
ls -R1t */files/* | grep not_terminated
.../egret.1/20100908162220.not_terminated.egret
.../egret.1/20100827215359.not_terminated.egret
# cd */files/egret.1
# auditreduce -O egret 20100908162220.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file
20100827230920.20100830000909.egret      Input (old) audit file
20100827215359.not_terminated.egret
# rm 20100827215359.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file
20100827230920.20100830000909.egret      Cleaned up audit file
```

L'horodatage de début sur le nouveau fichier reflète l'heure du premier événement d'audit dans le fichier `not_terminated`. L'horodatage de fin reflète l'heure du dernier événement d'audit dans le fichier.

▼ Contrôle du dépassement de la piste d'audit

Si votre stratégie de sécurité exige que toutes les données d'audit soient enregistrées, procédez comme suit :

1. **Planifiez l'archivage régulier des fichiers d'audit.**

   Archivez les fichiers d'audit en sauvegardant les fichiers sur un support hors ligne. Vous pouvez également déplacer les fichiers vers un système de fichiers d'archive.

   Si vous collectez des journaux d'audit au format texte avec l'utilitaire `syslog`, archivez les journaux texte. Pour plus d'informations, reportez-vous à la page de manuel `logadm(1M)`.

2. **Planifiez la suppression des fichiers d'audit archivés dans le système de fichiers d'audit.**

3 **Enregistrez et stockez les informations auxiliaires.**

Archivez les informations nécessaires pour interpréter les enregistrements d'audit ainsi que de la piste d'audit.

4 **Consignez les fichiers d'audit qui ont été archivés.**

5 **Stockez le support d'archivage correctement.**

6 **Réduisez le volume des données d'audit que vous pouvez stocker en créant des fichiers résumé.**

Vous pouvez extraire des fichiers résumés de la piste d'audit à l'aide d'options de la commande `auditreduce`. Les fichiers résumés contiennent uniquement les enregistrements de types spécifiés d'événements d'audit. Pour extraire les fichiers résumés, reportez-vous à l'Exemple 30–30 et l'Exemple 30–34.

Dépannage de l'audit Oracle Solaris (tâches)

Cette section couvre différents messages d'erreur et préférences de l'audit Oracle Solaris, et décrit l'audit proposé par d'autres outils. Ces procédures peuvent vous aider à enregistrer des événements d'audit dont vous avez besoin sur votre site.

Dépannage de l'audit Oracle Solaris (liste des tâches)

La liste des tâches suivante présente les procédures de dépannage de l'audit Oracle Solaris.

Problème	Solution	Voir
Pourquoi les fichiers d'audit ne se sont-ils pas créés alors que j'ai configuré l'audit ?	Résolvez les problèmes du démon d'audit et des fichiers de configuration d'audit.	“Vérification de l'exécution de l'audit Oracle Solaris” à la page 657
Comment puis-je réduire la quantité d'informations d'audit collectées ?	Auditez uniquement les événements que vous voulez contrôler.	“Atténuation du volume des enregistrements d'audit produits ” à la page 660
Comment puis-je auditer tout ce qu'un utilisateur fait sur le système ?	Auditez un ou plusieurs utilisateurs pour chaque commande.	“Audit de toutes les commandes par les utilisateurs ” à la page 661

Problème	Solution	Voir
Comment faire pour affecter aux sessions existantes les modifications que j'apporte actuellement aux événements d'audit en cours d'enregistrement ?	Mettez à jour un masque de présélection utilisateur.	"Modification d'un masque de présélection utilisateur" à la page 664
Comment accéder aux modifications apportées à un fichier particulier ?	Auditez les modifications du fichier, puis utilisez la commande `auditreduce` pour rechercher un fichier donné.	"Recherche des enregistrements d'audit concernant des modifications de fichiers spécifiques " à la page 664
Comment puis-je réduire la taille de mes fichiers d'audit ?	Limitez la taille du fichier d'audit binaire.	"Limitation de la taille des fichiers d'audit binaires " à la page 667
Comment puis-je supprimer les événements d'audit du fichier `audit_event` ?	Mettez à jour le fichier `audit_event`.	"Suppression de certains événements de la liste d'audit " à la page 666
Comment puis-je auditer tous les noms d'utilisateur d'un système Oracle Solaris ?	Auditez les connexions à partir de n'importe quel système.	"Audit des connexions à partir d'autres systèmes d'exploitation " à la page 667
Pourquoi les enregistrements d'audit ne sont-ils pas conservés pour mes transferts FTP ?	Utilisez l'outil d'audit qui permet aux utilitaires de gérer leurs propres journaux.	"Audit des transferts de fichiers FTP et SFTP " à la page 668

▼ Vérification de l'exécution de l'audit Oracle Solaris

Si vous pensez que l'audit a été activé, mais constatez qu'aucun enregistrement d'audit n'apparaît dans votre répertoire d'audit principal, essayez d'effectuer l'une des opérations suivantes.

Avant de commencer Vous avez correctement configuré la base de données `hosts` dans votre service de nommage et elle fonctionne. Pour déboguer des problèmes de service de nommage, reportez-vous aux sections suivantes :

- Page de manuel `nsswitch.conf(4)`
- *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*

1 Vérifiez que l'audit est en cours d'exécution.

- **Vérifiez que le module de noyau `c2audit` est chargé.**

```
# modinfo | grep c2audit
```

Aucune liste n'indique que l'audit n'est pas en cours d'exécution. La liste suivante indique que l'audit est en cours d'exécution :

```
40  132ce90  14230 186   1  c2audit (C2 system call)
```

- **Vérifiez que le démon d'audit est en cours d'exécution.**

  Vérifiez l'état du service `auditd`. La liste suivante indique que l'audit n'est pas en cours d'exécution :

  ```
  # svcs -x auditd
  svc:/system/auditd:default (Solaris audit daemon)
   State: disabled since Fri Aug 14 19:02:35 2009
  Reason: Disabled by an administrator.
     See: http://sun.com/msg/SMF-8000-05
     See: auditd(1M)
     See: audit(1M)
  Impact: This service is not running.
  ```

  La liste suivante indique que le service d'audit est en cours d'exécution :

  ```
  # svcs auditd
  STATE          STIME    FMRI
  online         10:10:10 svc:/system/auditd:default
  ```

- **Vérifiez la condition d'audit en cours.**

  La liste suivante indique que l'audit n'est pas en cours d'exécution :

  ```
  # auditconfig -getcond
  auditconfig: auditon(2) failed.
  auditconfig: error = Operation not supported(48)
  ```

  La liste suivante indique que l'audit est en cours d'exécution :

  ```
  # auditconfig -getcond
  audit condition = auditing
  ```

Si le service d'audit n'est pas activé, activez-le. Pour connaître la procédure, reportez-vous à la section “Activation du service d'audit ” à la page 638.

2 Vérifiez la syntaxe du fichier `audit_control`.

```
# audit -v /etc/security/audit_control
audit: audit_control must have either a valid "dir:" entry
or a valid "plugin:" entry with "p_dir:" specified.
```

Corrigez les erreurs. Le message `syntaxe ok` indique que le fichier est syntaxiquement correct.

3 Vérifiez que le fichier `audit_control` a des valeurs valides pour les mots-clés `flags` et `naflags`.

```
# grep flags /etc/security/audit_control
flags:lo
naflags:na,lp
```

Fournissez des valeurs valides si le fichier `audit_control` possède des valeurs non valides. Dans l'exemple précédent, `lp` est une classe non valide.

4 **Vérifiez que le fichier `audit_user` a des valeurs valides pour chaque utilisateur.**

```
# tail audit_user
...
# User Level Audit User File
#
# File Format
#
#    username:always:never
#
root:lo:no
admin:lp:no
```

Fournissez des valeurs valides si le fichier `audit_user` possède des valeurs non valides. Dans l'exemple précédent, `lp` est une classe non valide.

5 **Si vous avez créé une classe d'audit personnalisée, vérifiez que vous avez affecté des événements à cette classe.**

Par exemple, le fichier `audit_control` suivant contient une classe non fournie par le logiciel Oracle Solaris :

```
# grep flags /etc/security/audit_control
flags:lo,pf
naflags:na,lo
```

Pour obtenir une description de la création de la classe `pf`, reportez-vous à la section “Ajout d'une classe d'audit ” à la page 627.

a. **Vérifiez que la classe est définie dans le fichier `audit_class`.**

Le masque de classe d'audit doit être unique.

```
# grep pf /etc/security/audit_class
0x10000000:pf:profile command
```

Si la classe n'est pas définie, définissez-la. Dans le cas contraire, supprimez la classe des fichiers `audit_control` et `audit_user`.

b. **Vérifiez que les événements ont été affectés à la classe.**

```
# grep pf /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
```

Si des événements ne sont pas affectés à la classe, affectez-y les événements appropriés.

6 **Si aucun problème n'a été indiqué au cours des étapes précédentes, reportez-vous aux fichiers journaux système, `/var/adm/messages` et `/var/log/syslog`.**

a. **Localisez et résolvez les problèmes.**

b. **Ensuite, si le service d'audit est en cours d'exécution, redémarrez-le.**

```
# audit -s
```

c. Si le service d'audit n'est pas activé, activez-le.

Pour connaître la procédure, reportez-vous à la section "Activation du service d'audit " à la page 638.

▼ Atténuation du volume des enregistrements d'audit produits

Une fois que vous avez déterminé les événements à auditer sur votre site, utilisez les suggestions suivantes pour créer des fichiers d'audit faciles à gérer.

1 Utilisez la stratégie d'audit par défaut.

Évitez en particulier d'ajouter des événements et des jetons d'audit à la piste d'audit. Les stratégies suivantes ont une incidence sur la taille de la piste d'audit.

- Stratégie `arge` : ajoute des variables d'environnement aux événements d'audit `exec`.
- Stratégie `argv` : ajoute des paramètres de commande aux événements d'audit `exec`.
- Stratégie `public` : si des événements de fichier sont en cours d'audit, ajoute un événement à la piste d'audit chaque fois qu'un événement auditable se produit dans un fichier public. Les classes de fichier comprennent `fa`, `fc`, `fd`, `fm`, `fr`, `fw` et `cl`. Pour la définition d'un fichier public, reportez-vous à la section "Terminologie et concept de l'audit" à la page 594.
- Stratégie `path` : ajoute un jeton `path` aux événements d'audit qui comprennent un jeton `path` facultatif.
- Stratégie `group` : ajoute un jeton group aux événements d'audit qui comprennent un jeton `newgroups` facultatif.
- Stratégie `seq` : ajoute un jeton sequence à chaque événement d'audit.
- Stratégie `trail` : ajoute un jeton trailer à chaque événement d'audit.
- Stratégie `windata_down` : sur un système configuré avec Trusted Extensions, ajoute les événements lorsque les informations dans une fenêtre étiquetée sont réduites.
- Stratégie `windata_up` : sur un système configuré avec Trusted Extensions, ajoute les événements lorsque les informations dans une fenêtre étiquetée sont détaillées.
- Stratégie `zonename` : ajoute le nom de zone à chaque événement d'audit. Si la zone globale est la seule zone configurée, ajoute `zone, global` à chaque événement d'audit.

L'enregistrement d'audit suivant montre l'utilisation de l'instruction de la commande `ls`. La classe `ex` est auditée et la stratégie par défaut est en cours d'utilisation :

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

Ci-dessous, le même enregistrement lorsque toutes les stratégies sont activées :

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,136,432,0
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,PATH=/u
sr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
path,/lib/ld.so.1
attribute,100755,root,bin,136,4289,0
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,313540
trailer,375
```

2 **Utilisez le plug-in `audit_syslog.so` pour envoyer des événements d'audit à `syslog`.**

Cette stratégie fonctionne uniquement si vous n'êtes pas obligé de conserver des enregistrements binaires des événements d'audit que vous envoyez aux journaux `syslog`. En utilisant la commande `auditreduce`, vous pouvez éliminer les fichiers binaires de ces enregistrements, et, par conséquent, réduire la taille des fichiers binaires.

3 **Utilisez le fichier `audit_user` pour les événements d'audit pour des utilisateurs et des rôles spécifiques.**

Diminuez l'audit pour l'ensemble des utilisateurs en réduisant le nombre de classes d'audit dans le fichier `audit_control`. Dans le fichier `audit_user`, ajoutez des classes d'audit pour des utilisateurs et des rôles spécifiques.

4 **Créez votre propre classe d'audit.**

Vous pouvez créer des classes d'audit sur votre site. Dans ces classes, placez tous les événements d'audit que vous avez besoin de surveiller. Pour connaître cette procédure, reportez-vous à la section “Ajout d'une classe d'audit ” à la page 627.

Remarque – Si vous modifiez des affectations de classes d'audit existantes, vos modifications risquent d'être perdues lors de la mise à niveau vers une version plus récente du SE Oracle Solaris. Lisez attentivement les journaux d'installation.

▼ Audit de toutes les commandes par les utilisateurs

Dans le cadre de leur stratégie de sécurité, certains sites nécessitent des enregistrements d'audit pour toutes les commandes en cours d'exécution par l'utilisateur `root` ou par des rôles d'administration. Certains sites nécessitent également des enregistrements d'audit pour toutes les commandes exécutées par les utilisateurs.

1 **Auditez les classes `lo` et `ex`.**

La classe `ex` audite tous les appels des fonctions `exec()` et `execve()`. La classe `lo` audite les connexions, déconnexions et blocages d'écran. La sortie suivante répertorie tous les événements des classes `ex` et `lo`.

```
7:AUE_EXEC:exec(2):ps,ex
23:AUE_EXECVE:execve(2):ps,ex
...
6152:AUE_login:login - local:lo
6153:AUE_logout:logout:lo
6154:AUE_telnet:login - telnet:lo
6155:AUE_rlogin:login - rlogin:lo
6158:AUE_rshd:rsh access:lo
6159:AUE_su:su:lo
6162:AUE_rexecd:rexecd:lo
6163:AUE_passwd:passwd:lo
6164:AUE_rexd:rexd:lo
6165:AUE_ftpd:ftp access:lo
6171:AUE_ftpd_logout:ftp logout:lo
6172:AUE_ssh:login - ssh:lo
6173:AUE_role_login:role login:lo
6212:AUE_newgrp_login:newgrp login:lo
6213:AUE_admin_authenticate:admin login:lo
6221:AUE_screenlock:screenlock - lock:lo
6222:AUE_screenunlock:screenlock - unlock:lo
6227:AUE_zlogin:login - zlogin:lo
```

- **Pour auditer ces classes pour les administrateurs, modifiez le fichier `audit_user`.**

  Dans l'exemple suivant, le site a créé trois rôles, `sysadmin`, `auditadm` et `netadm`. Ces rôles et le compte `root` sont audités pour les classes `exec` et `lo` :

  ```
  ## audit_user file
  root:lo,ex:no
  sysadm:lo,ex:no
  auditadm:lo,ex:no
  netadm:lo,ex:no
  ```

- **Pour auditer la classe `lo` au niveau des événements non attribuables, modifiez le fichier `audit_control`.**

  ```
  ## audit_control file
  ...
  naflags:lo
  ...
  ```

- **Pour auditer ces classes pour tous les utilisateurs, modifiez le fichier `audit_control`.**

  ```
  ## audit_control file
  flags:lo,ex
  naflags:lo
  ...
  ```

  La sortie se présente de la manière suivante :

  ```
  header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
  path,/usr/bin/ls
  ```

```
   subject,jdoe,root,root,root,root,1401,737,0 0 mach1
   return,success,0
```

2 Pour enregistrer les arguments de commande, définissez la stratégie `argv`.

```
## audit_startup script
...
auditconfig -setpolicy +argv
...
```

Le jeton `exec_args` enregistre les arguments de commande :

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

3 Pour enregistrer l'environnement dans lequel la commande est exécutée, définissez la stratégie `arge`.

```
## audit_startup script
...
auditconfig -setpolicy +arge
...
```

Le jeton `exec_env` enregistre l'environnement de commande :

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
  PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

4 Pour enregistrer les arguments et l'environnement de commande, définissez les deux stratégies.

```
## audit_startup script
...
auditconfig -setpolicy +argv
auditconfig -setpolicy +arge
...
```

La sortie se présente de la manière suivante :

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
  PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

▼ Recherche des enregistrements d'audit concernant des modifications de fichiers spécifiques

Si vous avez l'intention de consigner les écritures d'un nombre limité de fichiers, par exemple, `/etc/passwd` et les fichiers du répertoire `/etc/default`, utilisez la commande `auditreduce` pour localiser les fichiers.

1. **La classe d'audit `fw`.**

   L'ajout de la classe au fichier `audit_user` génère moins d'enregistrements que si vous ajoutez la classe au fichier `audit_control`.

   - **Ajoutez la classe `fw` au fichier `audit_user`.**

     ```
     ## audit_user file
     root:fw:no
     sysadm:fw:no
     auditadm:fw:no
     netadm:fw:no
     ```

   - **Ajoutez la classe `fw` au fichier `audit_control`.**

     ```
     ## audit_control file
     flags:lo,fw
     ...
     ```

2. **Pour trouver les enregistrements d'audit pour des fichiers spécifiques, utilisez la commande `auditreduce`.**

   ```
   # /usr/sbin/auditreduce -o file=/etc/passwd,/etc/default -O filechg
   ```

   La commande `auditreduce` effectue la recherche dans la piste d'audit pour toutes les instances de l'argument `file`. Cette commande crée un fichier binaire avec le suffixe `filechg` qui contient tous les enregistrements incluant le chemin d'accès aux fichiers concernés. Reportez-vous à la page de manuel `auditreduce(1M)` pour plus d'informations sur la syntaxe de l'option `-o file=`*chemin*.

3. **Pour lire le fichier `filechg`, utilisez la commande `praudit`.**

   ```
   # /usr/sbin/praudit *filechg
   ```

▼ Modification d'un masque de présélection utilisateur

Si vous modifiez le fichier `audit_control` ou `audit_user`, le masque de présélection des utilisateurs déjà connectés ne change pas. Vous devez forcer la modification du masque de présélection.

Avant de commencer Vous avez activé l'audit, les utilisateurs se sont connectés, puis vous avez modifié la valeur `flags` ou `naflags` du fichier `audit_control`. Vous voulez activer l'audit des classes d'audit que vous venez de sélectionner pour les utilisateurs déjà connectés.

1. **Mettez à jour le masque de présélection des utilisateurs déjà connectés.**

   Deux options s'offrent à vous : Vous pouvez terminer la session existante ou utiliser la commande `auditconfig` pour mettre à jour les masques de présélection de ces utilisateurs.

   - **Fermez les sessions existantes de ces utilisateurs.**

     Les utilisateurs peuvent se connecter et se reconnecter, ou l'administrateur peut mettre fin manuellement (kill) aux sessions actives. La nouvelle session va hériter du nouveau masque présélection. Toutefois, l'arrêt des sessions utilisateurs n'est pas très pratique.

   - **Modifiez le masque de présélection de chaque utilisateur dynamiquement.**

     Supposons que l'attribut `flags` du fichier `audit_control` a changé de `lo` en `lo,ex`.

     a. **Déterminez l'ID d'audit de l'utilisateur et l'ID de la session d'audit.**

        Tout d'abord, recherchez tous les utilisateurs normaux. Dans l'exemple suivant, l'administrateur détecte tous les processus qui n'appartiennent pas à `root`, `daemon` ou `lp`:

        ```
        # /usr/bin/pgrep -v -u root,daemon,lp | more
        ..
        3941
        3948
        3949
        10640 ...
        ```

        Ensuite, utilisez l'un des processus de l'utilisateur pour rechercher l'ID d'audit de l'utilisateur :

        ```
        # auditconfig -getpinfo 3941
        audit id = jdoe(1002)
        process preselection mask = lo(0x1000,0x1000)
        terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
        audit session id = 713
        ```

        Notez que le masque de présélection utilisateur inclut la classe `lo` et n'inclut pas la classe `ex` récemment ajoutées.

     L'ID d'audit de l'utilisateur est `1002`. L'ID de session de l'audit utilisateur est `713`.

2. **Modifiez le masque de présélection de l'utilisateur.**

   Utilisez l'une des méthodes suivantes :

   - **Utilisez l'ID de la session de l'audit utilisateur pour modifier le masque de présélection de l'utilisateur.**

     ```
     # /usr/sbin/auditconfig -setsmask lo,ex 713
     ```

   - **Utilisez l'ID d'audit utilisateur pour modifier le masque de présélection de l'utilisateur.**

     ```
     # /usr/sbin/auditconfig -setumask lo,ex 1002
     ```

3 Vérifiez que le masque de présélection a changé.

```
# auditconfig -getpinfo 3941
audit id = jdoe(1002)
process preselection mask = ex,lo(0x40001000,0x40001000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 713
```

▼ Suppression de certains événements de la liste d'audit

Pour des raisons de maintenance, il arrive parfois qu'un site veuille empêcher les événements d'audit d'être soumis à un audit.

1 Changez la classe de l'événement pour la classe no.

Par exemple, les événements 26 et 27 appartiennent à la classe `pm`.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):pm
27:AUE_SETPGRP:setpgrp(2):pm
28:AUE_SWAPON:swapon(2):no
...
```

Modifiez ces événements pour la classe `no`.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):no
27:AUE_SETPGRP:setpgrp(2):no
28:AUE_SWAPON:swapon(2):no
...
```

Si la classe `pm` est actuellement en cours d'audit, les sessions existantes sont toujours les événements d'audit 26 et 27. Pour arrêter ces événements en cours d'audit, vous devez mettre à jour les masques de présélection des utilisateurs.

Attention – Ne commentez jamais les événements dans le fichier `audit_event`. Ce fichier est utilisé par la commande `praudit` binaire pour lire les fichiers d'audit binaires. Les fichiers d'audit archivés peuvent contenir des événements répertoriés dans le fichier.

2 Pour mettre à jour les masques de présélection d'utilisateurs, suivez les instructions contenues dans la section "Modification d'un masque de présélection utilisateur" à la page 664.

▼ Limitation de la taille des fichiers d'audit binaires

Les fichiers d'audit binaires augmentent sans limite. Pour faciliter la tâche de l'archivage et de la recherche, vous pouvez être amené à limiter la taille. Vous pouvez également créer de plus petits fichiers binaires à partir du fichier d'origine.

1 **À partir de la version Solaris 10 10/08, utilisez l'attribut `p_fsize` pour limiter la taille de chaque fichier d'audit binaire.**

L'attribut `p_fsize` sur le plug-in `audit_binfile.so` vous permet de limiter la taille d'un fichier d'audit. La valeur par défaut est zéro (0), ce qui permet au fichier de croître sans limite. La valeur est spécifiée en octets, de 512 000 à 2 147 483 647. Lorsque la taille spécifiée est atteinte, le fichier d'audit en cours est fermé et un nouveau fichier est ouvert.

Dans l'exemple suivant, vous pouvez limiter la taille du fichier d'audit à 1 Mo :

```
plugin:name=audit_binfile.so; p_dir:/var/audit; p_fsize=1024000
```

2 **Utilisez la commande `auditreduce` pour sélectionner des enregistrements et écrire les enregistrements dans un fichier pour une analyse plus approfondie.**

Les options `auditreduce` *-minuscules* recherchent des enregistrements spécifiques.

Les options `auditreduce` *-majuscules* écrivent vos sélections vers un fichier. Pour plus d'informations, reportez-vous à la page de manuel `auditreduce`(1M).

▼ Audit des connexions à partir d'autres systèmes d'exploitation

Oracle Solaris peut auditer les connexions, quelle que soit la source.

- **La classe d'audit `lo` pour les événements attribuables et non attribuables.**

Cette classe audite les connexions, déconnexions, et blocages d'écran.

```
## audit_control file
flags:lo
naflags:lo
...
```

Remarque – Pour effectuer l'audit des connexions `ssh`, votre système Oracle Solaris doit exécuter le démon `ssh` Oracle Solaris. Ce démon est modifié pour l'audit Oracle Solaris. Pour plus d'informations, reportez-vous à la section "Oracle Solaris Secure Shell et le projet OpenSSH" à la page 360.

▼ Audit des transferts de fichiers FTP et SFTP

Le service FTP crée des journaux pour les transferts de fichiers. Le service SFTP, qui s'exécute sous le protocole SSH, peut être contrôlé par l'audit Oracle Solaris. Les informations de connexion pour ces deux services peuvent être contrôlées par l'audit Oracle Solaris.

1 Pour consigner des commandes et transferts de fichiers du service FTP, reportez-vous à la page de manuel `ftpaccess(4)`.

Pour connaître les options de journalisation disponibles, reportez-vous à la section concernant les fonctions de journalisation. Les options `log commands` et `log transfers` peuvent notamment fournir des journaux utiles.

2 Pour consigner des transferts de fichiers `sftp`, effectuez l'une et/ou l'autre des opérations suivantes :

- **Audit des écritures de fichiers.**

  Les transferts de fichiers par le biais d'une connexion SSH utilisent la commande `sftp`. Ces transferts peuvent être enregistrés en utilisant l'indicateur d'audit `+fr`. Pour auditer les transferts de fichiers `sftp` ayant échoué, auditez l'indicateur d'audit `-fr`.

  La sortie suivante provient d'une session `sftp` réussie :

  ```
  header,138,2,open(2) - read,,ma2,2009-08-25 14:48:58.770 -07:00
  path,/home/jdoe/vpn_connect
  attribute,100644,jdoe,staff,391,437,0
  subject,jdoe,jdoe,staff,jdoe,staff,4444,120289379,8457 65558 ma1
  return,success,6
  ```

- **Utilisez l'option verbose pour la commande `sftp`.**

  L'option `-v` peut être répétée jusqu'à trois reprises.

  ```
  # sftp -vvv [ other options ] hostname
  ```

3 Pour enregistrer l'accès aux services FTP et SFTP, auditez la classe `lo`.

Comme indiqué dans la sortie suivante, la connexion et la déconnexion du démon `ftpd` génèrent des enregistrements d'audit.

```
% bsmrecord -c lo | more
...
in.ftpd
  program     /usr/sbin/in.ftpd    See ftp access
  event ID    6165                 AUE_ftpd
  class       lo                   (0x00001000)
      header
      subject
      [text]                       error message
      return

in.ftpd
  program     /usr/sbin/in.ftpd    See ftp logout
  event ID    6171                 AUE_ftpd_logout
```

```
  class       lo                  (0x00001000)
      header
      subject
      return
...
```

La connexion SSH enregistre tous les accès à la commande `sftp`.

```
...
/usr/lib/ssh/sshd
  program     /usr/lib/ssh/sshd   See login - ssh
  event ID    6172                AUE_ssh
  class       lo                  (0x00001000)
      header
      subject
      [text]                      error message
      return
```

◆ ◆ ◆ CHAPITRE 31

Audit Oracle Solaris (référence)

Ce chapitre décrit les éléments importants de l'audit Oracle Solaris. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre.

Pour une présentation de l'audit Oracle Solaris, reportez-vous au Chapitre 28, "Audit Oracle Solaris (présentation) ". Pour obtenir des suggestions de planification, reportez-vous au Chapitre 29, "Planification de l'audit Oracle Solaris". Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au Chapitre 30, "Gestion de l'audit Oracle Solaris (tâches) ".

Commandes d'audit

Cette section fournit des informations sur les commandes suivantes :

- “Commande auditconfig” à la page 677

Démon auditd

La liste suivante récapitule les tâches du démon auditd :

- Ouvre et ferme les fichiers d'audit dans les répertoires qui sont spécifiés dans le fichier audit_control. Ces fichiers sont ouverts dans leur ordre d'apparition.
- Charge un ou plusieurs plug-ins. Sun fournit deux plug-ins. Le plug-in audit_binfile.so écrit des données d'audit binaire dans un fichier. Le plug-in audit_syslog.so fournit des extraits de texte sélectionné dans les enregistrements d'audit du journal syslog.
- Lit les données d'audit à partir du noyau et insère les données en utilisant un plug-in auditd.
- Exécute le script audit_warn pour avertir de diverses conditions. Le plug-in audit_binfile.so exécute le script audit_warn. Le script, par défaut, envoie des avertissements à l'alias de messagerie audit_warn et à la console. Le plug-in syslog.so n'exécute pas le script audit_warn.
- Par défaut, lorsque tous les répertoires d'audit sont pleins, les processus qui génèrent les enregistrements d'audit sont interrompus. En outre, le démon auditd écrit un message sur la console et dans l'alias de messagerie audit_warn. A ce stade, seul l'administrateur système peut résoudre le service d'audit. L'administrateur peut se connecter pour écrire les fichiers d'audit sur un support hors ligne, supprimer les fichiers d'audit du système et effectuer d'autres tâches de nettoyage.

  La stratégie d'audit peut être reconfigurée avec la commande auditconfig.

Le démon auditd peut être démarré automatiquement lorsque le système est initialisé en mode multiutilisateur. Vous pouvez également démarrer le démon à partir de la ligne de commande. Lorsque le démon auditd est démarré, il calcule la quantité d'espace disponible nécessaire pour les fichiers d'audit.

Le démon auditd utilise la liste des répertoires d'audit dans le fichier audit_control pour définir les emplacements possibles pour la création de fichiers d'audit. Le démon gère un pointeur dans cette liste de répertoires, en commençant par le premier répertoire. Chaque fois que le démon auditd a besoin de créer un fichier d'audit, il place le fichier dans le premier répertoire disponible dans la liste. La liste commence au pointeur du démon auditd actuel. Vous pouvez rétablir le curseur au début de la liste en exécutant la commande audit - s. La commande audit -n demande au démon de passer à un nouveau fichier d'audit. Le nouveau fichier est créé dans le même répertoire que le fichier en cours.

Commande audit

La commande audit contrôle les actions du démon auditd. La commande audit permet d'effectuer les tâches suivantes :

- Activer et désactiver l'audit
- Réinitialiser le démon `auditd`
- Ajuster le masque de présélection de l'audit sur le système local
- Écrire les enregistrements d'audit dans un autre fichier d'audit

Pour connaître les différentes options disponibles, reportez-vous à la page de manuel `audit`(1M).

Commande `bsmrecord`

La commande `bsmrecord` affiche le format des événements d'audit définis dans le `/etc/security/audit_event`. La sortie inclut l'ID d'audit, la classe d'audit et l'indicateur d'audit de l'événement, ainsi que les jetons d'audit de l'enregistrement dans l'ordre. Sans aucune option, la sortie de la commande `bsmrecord` s'affiche dans une fenêtre de terminal. Avec l'option `-h`, la sortie de la commande peut s'afficher dans un navigateur. Pour consulter des exemples d'utilisation de la commande `bsmrecord`, reportez-vous à la section "Affichage des formats d'enregistrement d'audit " à la page 647. Reportez-vous également à la page de manuel `bsmrecord`(1M).

Commande `auditreduce`

La commande `auditreduce` récapitule les enregistrements d'audit stockés au format binaire. Cette commande peut fusionner des enregistrements d'audit à partir d'un ou plusieurs fichiers d'audit d'entrée. Elle peut également servir à la post-sélection d'enregistrements d'audit. Les enregistrements sont conservés dans un format binaire. Pour fusionner la piste d'audit entière, exécutez cette commande sur le serveur d'audit. Le serveur d'audit est le système qui monte tous les systèmes de fichiers d'audit pour l'installation. Pour plus d'informations, reportez-vous à la page de manuel `auditreduce`(1M).

La commande `auditreduce` vous permet d'auditer les actions effectuées sur plusieurs systèmes à partir d'un seul emplacement. La commande peut lire la combinaison logique de tous les fichiers d'audit comme s'il s'agissait d'une seule piste d'audit. Vous devez configurer tous les systèmes de manière identique sur un site destiné à l'audit et créer des serveurs et des répertoires locaux pour les fichiers d'audit. La commande `auditreduce` ignore comment les enregistrements ont été générés ou l'endroit où ceux-ci sont stockés. Sans aucune option, la commande `auditreduce` fusionne les enregistrements d'audit à partir de tous les fichiers d'audit, dans tous les sous-répertoires du répertoire root d'audit. En règle générale, `/etc/security/audit` correspond au répertoire root d'audit. La commande `auditreduce` envoie les résultats fusionnés dans la sortie standard. Vous pouvez également placer les résultats dans un seul fichier de sortie, trié par ordre chronologique. Le fichier contient des données binaires.

La commande `auditreduce` peut également sélectionner certains types d'enregistrements pour l'analyse. Les fonctions de fusion et de sélection de la commande `auditreduce` sont logiquement indépendantes. La commande `auditreduce` capture les données à partir du fichier d'entrée pendant la lecture des enregistrements, avant que les fichiers soient fusionnés puis écrits sur le disque.

Si vous spécifiez des options pour la commande `auditreduce`, les actions suivantes sont possibles :

- Demander les enregistrements d'audit qui ont été générés par les classes d'audit
- Demander les enregistrements d'audit qui ont été générés par un utilisateur particulier
- Demander les enregistrements d'audit qui ont été générés à des dates spécifiques

Sans argument, la commande `auditreduce` vérifie les sous-répertoires du répertoire `/etc/security/audit`, défini par défaut en tant que répertoire root d'audit. La commande recherche un répertoire `files` dans lequel résident les fichiers *start-time.end-time.hostname*. La commande `auditreduce` est très utile lorsque les données d'audit se trouvent dans des répertoires différents. La Figure 31–1 illustre des données d'audit stockées dans des répertoires différents pour différents hôtes. La Figure 31–2 illustre des données d'audit stockées dans des répertoires différents pour différents serveurs d'audit.

FIGURE 31–1 Stockage des pistes d'audit par hôte

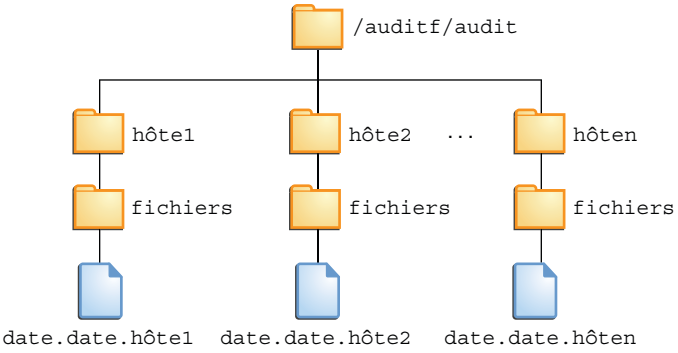
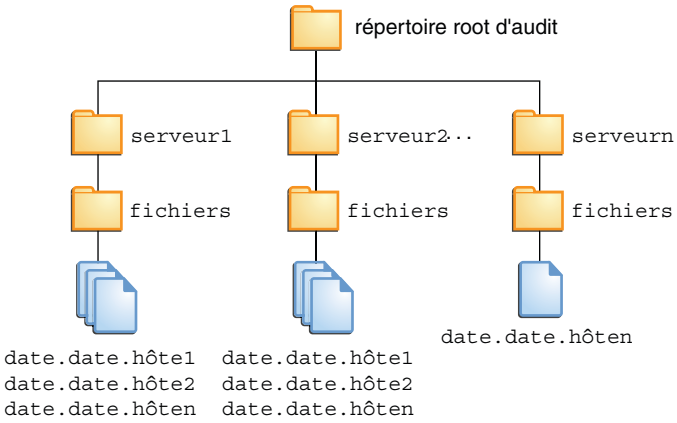


FIGURE 31–2 Stockage des pistes d'audit par serveur



Si la partition du répertoire `/etc/security/audit` est très petite, il vaut mieux de ne pas stocker les données d'audit dans le répertoire par défaut. Vous pouvez exécuter la commande `auditreduce` sur un autre répertoire en utilisant l'option `-R` :

```
# auditreduce -R /var/audit-alt
```

Vous pouvez également spécifier un sous-répertoire particulier en utilisant l'option `-S` :

```
# auditreduce -S /var/audit-alt/host1
```

Pour d'autres options et plus d'exemples, reportez vous à la page de manuel `auditreduce(1M)`.

Commande `praudit`

La commande `praudit` rend lisible la sortie binaire de la commande `auditreduce`. La commande `praudit` lit les enregistrements d'audit dans un format binaire à partir de l'entrée standard et affiche les enregistrements dans un format présentable. L'entrée peut être acheminée à partir de la commande `auditreduce` ou à partir d'un seul fichier d'audit. L'entrée peut aussi être produite avec la commande `cat` pour concaténer plusieurs fichiers, ou la commande `tail` pour un fichier d'audit actuel.

La commande `praudit` peut générer quatre formats de sortie. Une cinquième option, `-l` (long), imprime un enregistrement d'audit par ligne de sortie. L'option par défaut est de placer un jeton d'audit par ligne de sortie. L'option `-d` modifie le séparateur utilisé entre les champs de jeton et entre les jetons. Le séparateur par défaut est une virgule.

- **Par défaut :** La commande `praudit` sans aucune option affiche un jeton d'audit par ligne. La commande affiche l'événement d'audit en fonction de sa description, par exemple l'appel système `ioctl(2)`. N'importe quelle valeur qui peut être affichée sous forme de texte s'affiche sous forme de texte. Par exemple, c'est le nom de l'utilisateur qui s'affiche, et non son ID utilisateur.
- **Option –r :** Cette option de format brut affiche toute valeur qui peut être numérique sous la forme d'un chiffre. Par exemple, c'est l'ID de l'utilisateur qui s'affiche, les adresses Internet sont au format hexadécimal et les modes au format octal. L'événement d'audit s'affiche sous son numéro d'événement, par exemple `158`.
- **Option –s :** Cette option de format court affiche l'événement d'audit sous son nom de table, par exemple `AUE_IOCTL`. Elle affiche les autres jetons comme ils sont affichés par l'option par défaut.
- **Option –x :** Cette option XML affiche l'enregistrement d'audit au format XML. Elle est utile en tant qu'entrée pour les navigateurs, ou en tant qu'entrée pour les scripts qui manipulent le langage XML.

  Le fichier XML est décrit par une DTD fournie par le service d'audit. Le logiciel Oracle Solaris fournit également une feuille de style. La DTD et de la feuille de style se trouvent dans le répertoire `/usr/share/lib/xml`.

Dans le format de sortie par défaut de la commande `praudit`, chaque enregistrement est facilement identifié en tant que séquence de jetons d'audit. Chaque jeton s'affiche sur une ligne distincte. Chaque enregistrement commence par un jeton `header` (d'en-tête). Vous pourriez, par exemple, traiter la sortie plus en profondeur avec la commande `awk`.

Voici un exemple de sortie de la commande `praudit - l` pour un jeton `header` :

```
header,173,2,settppriv(2),,example1,2010-10-10 10:10:02.020 -07:00
```

Voici un exemple de sortie de la commande `praudit - r` pour le même jeton `header` :

```
121,173,2,289,0x0000,192.168.86.166,1066077962,174352445
```

EXEMPLE 31–1 Traitement de la sortie `praudit` à l'aide d'un script

Si vous le souhaitez, vous pouvez traiter la sortie de la commande `praudit` en tant que lignes de texte. Cela peut être utile pour sélectionner des enregistrements que la commande `auditreduce` ne peut pas sélectionner. Un simple script shell suffit pour traiter la sortie de la commande `praudit`. L'exemple de script suivant place un enregistrement d'audit sur une seule ligne, recherche une chaîne de caractères spécifiée par l'utilisateur, puis renvoie le fichier d'audit dans sa forme d'origine.

```
#!/bin/sh
#
## This script takes an argument of a user-specified string.
#  The sed command prefixes the header tokens with Control-A
#  The first tr command puts the audit tokens for one record
```

EXEMPLE 31–1 Traitement de la sortie `praudit` à l'aide d'un script *(Suite)*

```
#  onto one line while preserving the line breaks as Control-A
#
praudit | sed -e '1,2d' -e '$s/^file.*$//' -e 's/^header/^aheader/' \\
| tr '\\012\\001' '\\002\\012' \\
| grep "$1" \\      Finds the user-specified string
| tr '\\002' '\\012'       Restores the original newline breaks
```

Notez que les caractères `^a` dans le script signifie Ctrl+A, et non les deux caractères `^` et `a`. Le préfixe distingue le jeton `header` de la chaîne `header` qui pourrait s'afficher sous forme de texte.

Commande `auditconfig`

La commande `auditconfig` fournit une interface de ligne de commande pour récupérer et définir les paramètres de configuration d'audit. La commande `auditconfig` permet d'effectuer les tâches suivantes :

- Afficher, vérifier et configurer la stratégie d'audit
- Déterminer si l'audit est activé ou désactivé
- Gérer le répertoire d'audit et le fichier d'audit
- Gérer la file d'attente d'audit
- Obtenir et définir des masques de présélection
- Obtenir et définir des événements d'audit sur des mappages de classes d'audit
- Obtenir et définir des informations de configuration, telles que l'ID de session et l'ID d'audit
- Configurer les caractéristiques de l'audit d'un processus, d'un shell et d'une session
- Rétablir les statistiques d'audit

Pour connaître les différentes options de cette commande, reportez-vous à la page de manuel `auditconfig(1M)`.

Fichiers utilisés par le service d'audit

Le service d'audit utilise les fichiers suivants :

- "Script audit_warn" à la page 682
- "Script bsmconv" à la page 683

Fichier system

Le fichier /etc/system contient des commandes que le noyau lit lors de l'initialisation pour personnaliser les opérations du système. Les scripts shell bsmconv et bsmunconv utilisés pour activer et désactiver l'audit modifient le fichier /etc/system. Le script shell bsmconv ajoute la ligne suivante au fichier /etc/system :

```
set c2audit:audit_load=1
```

L'entrée set c2audit:audit_load=1 génère le chargement du module du noyau à auditer lorsque le système s'initialise. Le script shell bsmunconv désactive l'audit lors du redémarrage du système. Cette commande supprime la ligne c2audit du fichier /etc/system.

Fichier syslog.conf

Le fichier /etc/syslog.conf fonctionne avec le plug-in audit_syslog.so pour stocker les enregistrements d'audit au format texte. Le fichier syslog.conf peut être configuré de manière à activer l'utilitaire syslog pour stocker les enregistrements d'audit. La section "Configuration des journaux d'audit syslog " à la page 623 présente un exemple.

Fichier audit_class

Le fichier /etc/security/audit_class définit les classes d'audit. Les classes d'audit sont des groupes d'événements d'audit. Vous pouvez utiliser le nom de classe dans le fichier audit_control pour présélectionner les classes dont vous voulez auditer les événements. Les classes acceptent les préfixes pour sélectionner uniquement les événements ayant échoué ou uniquement ceux qui ont réussi. Pour plus d'informations, reportez-vous à la section "Syntaxe de classe d'audit" à la page 686.

Le superutilisateur, ou un administrateur dans un rôle équivalent, peut modifier les définitions des classes d'audit. Cet administrateur peut définir de nouvelles classes d'audit, renommer des classes existantes ou modifier des classes existantes en modifiant le fichier audit_class dans un éditeur de texte. Pour plus d'informations, reportez-vous à la page de manuel audit_class(4).

Fichier audit_control

Sur chaque système, le fichier /etc/security/audit_control contient des informations de configuration pour le démon auditd. Ce fichier permet à chaque système de monter un système de fichiers d'audit distant pour stocker les enregistrements d'audit.

Vous pouvez préciser cinq types d'informations dans le fichier `audit_control`. Chaque ligne d'informations commence par un mot-clé.

- Le **mot-clé** `flags` commence l'entrée qui présélectionne les classes d'événements qui seront auditées pour l'ensemble des utilisateurs du système. Les classes d'audit qui sont spécifiées ici déterminent le *masque de présélection d'audit à l'échelle du système*. Les classes d'audit sont séparées par des virgules.
- Le **mot-clé** `naflags` commence l'entrée qui présélectionne les classes d'événements qui seront auditées lorsqu'une action ne peut pas être attribuée à un utilisateur spécifique. Les classes d'audit sont séparées par des virgules. La classe d'événement `na` appartient à cette entrée. L'entrée `naflags` peut être utilisée pour la journalisation d'autres classes d'événement qui sont normalement attribuables mais ne peuvent pas être attribuées. Par exemple, si un programme qui se lance au démarrage lit un fichier, l'ajout de `fr` dans l'entrée `naflags` est susceptible de créer un enregistrement de l'événement.
- Le **mot-clé** `minfree` a été abandonné. Utilisez l'attribut `p_minfree` sur le plug-in `audit_binfile.so`.

  L'attribut `p_minfree` définit le niveau d'espace disponible minimum pour tous les systèmes de fichiers d'audit sous la forme d'un pourcentage. Ce pourcentage doit être égal ou supérieur à `0`. La valeur par défaut est 20 %. Lorsqu'un système de fichiers d'audit est rempli à 80 % de sa capacité, les données d'audit sont stockées dans le répertoire d'audit disponible suivant. Pour plus d'informations, reportez-vous à la page de manuel `audit_warn`(1M).
- Le **mot-clé** `dir` a été abandonné. Utilisez l'attribut `p_dir` sur le plug-in `audit_binfile.so`.

  L'attribut `p_dir` répertorie les emplacements de répertoire. Chaque valeur de ligne définit un système de fichiers d'audit et un répertoire utilisé par le système pour stocker ses fichiers d'audit. Vous pouvez spécifier un ou plusieurs emplacements de répertoire. L'ordre des valeurs est important. Le démon `auditd` crée des fichiers d'audit dans les répertoires en suivant l'ordre spécifié. Le premier répertoire représente le *répertoire d'audit principal* du système. Le second répertoire représente le *répertoire d'audit secondaire* dans lequel le démon `auditd` crée les fichiers d'audit lorsque le premier répertoire est plein, et ainsi de suite. Pour plus d'informations, reportez-vous à la page de manuel `audit`(1M).
- Le **mot-clé** `plugin` spécifie le *chemin d'accès au plug-in* pour les modules de plug-in `audit_binfile.so` et `audit_syslog.so`. Le module `audit_binfile.so` gère la création de fichiers d'audit binaires. Le module `audit_syslog.so` convertit en temps réel des enregistrements d'audit Oracle Solaris en texte. Les classes d'audit qui sont spécifiées dans l'attribut `p_flags` du plug-in `audit_syslog.so` doivent être un sous-ensemble des classes d'audit présélectionnées.

Pour plus d'informations sur le fichier `audit_control`, reportez-vous à la page de manuel `audit_control`(4). Pour plus d'informations sur les plug-ins, reportez-vous à la section “Plug-ins d'audit ” à la page 688 et aux pages de manuel `audit_binfile`(5) et `audit_syslog`(5).

EXEMPLE 31–2 Exemple de fichier `audit_control`

L'exemple ci-après représente un fichier `audit_control` pour le système de fichiers `noddy`. `noddy` utilise deux systèmes de fichiers d'audit sur le serveur d'audit `blinken`, et un troisième système de fichiers d'audit monté sur le deuxième serveur d'audit `winken`. Le troisième système de fichiers n'est utilisé que lorsque les systèmes de fichiers d'audit sur `clignote` sont pleins ou non disponibles. La valeur `minfree` de 20 % indique que le script d'avertissement est exécuté lorsque les systèmes de fichiers sont à 80 % de leur capacité. Les paramètres indiquent que les opérations de connexion et d'administration seront auditées. L'audit consistera à contrôler les réussites et les échecs de ces opérations. Les échecs de tous types, à l'exception des échecs de création d'un objet système de fichiers, doivent être vérifiés. Les événements non attribuables sont également audités. Le journal d'audit `syslog` enregistre moins d'événements d'audit. Ce journal récapitule les échecs de connexion et d'administration au format texte.

Dans la version Solaris10, les lignes `dir` et `minfree` ont été abandonnées. Dans l'exemple suivant, les lignes `plugin` ne contiennent pas de retour à la ligne.

```
flags:lo,am,-all,^-fc
naflags:lo,nt
plugin:name=audit_binfile.so; p_minfree=20; p_dir=/var/audit/blinken/files,
/var/audit/blinken.1/files,/var/audit/winken
plugin:name=audit_syslog.so; p_flags=-lo,-am
```

Fichier `audit_event`

Le fichier `/etc/security/audit_event` contient les mappages événements d'audit-classes par défaut. Vous pouvez modifier ce fichier pour modifier ces mappages. Pour lire un mappage de classes modifié dans le noyau, vous devez redémarrer le système ou exécuter la commande `auditconfig - conf`. Pour plus d'informations, reportez-vous à la page de manuel `audit_event(4)`.

Script `audit_startup`

Le script `/etc/security/audit_startup` configure automatiquement le service d'audit lorsque le système entre en mode multiutilisateur. Le démon `auditd` démarre lorsque le script a :

- configuré les mappages événements d'audit-classes ;
- défini les options de stratégie d'audit.

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

Base de données `audit_user`

La base de données `/etc/security/audit_user` modifie les classes présélectionnées à l'échelle du système pour un utilisateur individuel. Les classes que vous ajoutez à une entrée utilisateur dans la base de données `audit_user` modifient les paramètres dans le fichier `audit_control` de deux manières :

- Les classes d'audit spécifiées sont toujours à auditer pour cet utilisateur.
- Les classes d'audit spécifiées ne doivent jamais être auditées pour cet utilisateur.

Chaque entrée utilisateur dans la base de données `audit_user` contient trois champs :

username:*always-audit-classes*:*never-audit-classes*

Les champs d'audit sont traités dans l'ordre.

- Le champ *always-audit-classes* active l'audit des classes dans ce champ. Utilisez ce champ pour modifier des paramètres applicables à l'ensemble du système. Par exemple, si vous saisissez `all` dans le champ *always-audit-classes*, cela active l'audit intégral d'un utilisateur.
- Le champ *never-audit-classes* désactive l'audit des classes dans ce champ. Utilisez ce champ pour remplacer les paramètres système. Si vous saisissez `all` dans le champ *never-audit-classes*, cela désactive l'audit de cet utilisateur, y compris celui des classes d'audit spécifiées dans le fichier `audit_control`.

Supposons que vous souhaitez appliquer les paramètres d'audit du système à l'utilisateur `tamiko`, à l'exception des lectures réussies des objets système de fichiers. Remarquez la position du second deux-points (`:`) dans l'entrée `audit_user` :

```
tamiko:^+fr:no          modify system defaults for fr
```

L'entrée précédente signifie "toujours auditer tout, à l'exception des lectures de fichier réussies."

Si vous souhaitez auditer tout pour l'utilisateur `tamiko` à l'exception des lectures réussies, utilisez l'entrée suivante :

```
tamiko:all,^+fr:no          audit everything except fr
```

Supposons que vous voulez remplacer les valeurs par défaut du système pour les lectures de fichier réussies de l'utilisateur `tamiko`. L'entrée suivante signifie "toujours auditer tout, mais ne jamais auditer les lectures de fichier réussie."

```
tamiko:all:+fr          override system defaults for fr
```

Remarque – Les événements qui ont échoué sont traités séparément de ceux qui ont réussi. Un processus peut générer plus d'enregistrements d'audit pour les événements ayant échoué que pour ceux ayant réussi.

Script `audit_warn`

Le script `/etc/security/audit_warn` notifie un alias de messagerie lorsque le démon `auditd` rencontre une condition inhabituelle lors de l'écriture d'enregistrements d'audit. Vous pouvez personnaliser ce script pour votre site afin d'être prévenu des conditions qui pourraient nécessiter une intervention manuelle. Ou bien, vous pouvez indiquer comment gérer ces conditions automatiquement. Pour toutes les conditions d'erreur, le script `audit_warn` écrit un message dans `syslog` avec la gravité de `daemon.alert`. Vous pouvez utiliser `syslog.conf` pour configurer l'affichage console des messages `syslog`. Le script `audit_warn` envoie également un message à l'alias de messagerie `audit_warn`. Cet alias est configuré en même temps que les paramètres d'audit.

Lorsque le démon `auditd` détecte les conditions suivantes, il appelle le script`audit_warn`. Le script envoie un e-mail à l'alias `audit_warn`.

- Un répertoire d'audit contient plus de données que le volume autorisé par la valeur `minfree`. La valeur `minfree` ou une limite dépassable est un pourcentage de l'espace disponible sur un système de fichiers d'audit.

  Le script `audit_warn` est appelé avec la chaîne `soft` et le nom du répertoire dont l'espace disponible est inférieur à la valeur minimale. Le démon `auditd` passe automatiquement au répertoire approprié suivant. Le démon écrit les fichiers d'audit dans le nouveau répertoire jusqu'à ce que le répertoire atteigne sa limite `minfree`. Le démon `auditd` passe ensuite à chaque répertoire restant en suivant l'ordre indiqué dans le fichier `audit_control`. Le démon écrit les enregistrements d'audit jusqu'à ce que chaque répertoire atteigne sa limite `minfree`.
- Tous les répertoires d'audit ont atteint le seuil `minfree`.

  Le script `audit_warn` est appelé avec la chaîne `allsoft`. Un message est écrit sur la console. L'e-mail est également envoyé à l'alias `audit_warn`.

  Lorsque tous les répertoires d'audit mentionnés dans le fichier `audit_control` ont atteint leur seuil `minfree`, le démon `auditd` revient au premier répertoire. Le démon écrit des enregistrements d'audit jusqu'à ce que le répertoire soit complètement rempli.
- Un répertoire d'audit est complet et n'a plus d'espace disponible.

  Le script `audit_warn` est appelé avec la chaîne `hard` et le nom du répertoire. Un message est écrit sur la console. L'e-mail est également envoyé à l'alias `audit_warn`.

Le démon `auditd` passe automatiquement au répertoire suivant contenant suffisamment d'espace disponible. Le démon `auditd` passe ensuite à chaque répertoire restant en suivant l'ordre indiqué dans le fichier `audit_control`. Le démon écrit les enregistrements d'audit jusqu'à ce que chaque répertoire soit plein.

- Tous les répertoires d'audit sont pleins. Le script `audit_warn` est appelé avec la chaîne `allhard` comme un argument.

  Par défaut, un message est écrit sur la console. L'e-mail est également envoyé à l'alias `audit_warn`. Les processus qui généraient des enregistrements d'audit continuent de s'exécuter, mais ces enregistrements d'audit sont comptés et ne sont pas générés. Pour connaître un moyen de gérer cette situation, reportez-vous à l'Exemple 30–16 et à la section "Contrôle du dépassement de la piste d'audit" à la page 655.

- Une erreur interne se produit. Les erreurs internes possibles sont les suivantes :
  - `ebusy` : un autre démon `auditd` est déjà en cours d'exécution.
  - `tmpfile` : un fichier temporaire ne peut pas être utilisé.
  - `postsigterm` : un signal a été reçu pendant l'arrêt de l'audit.
  - `plugin` *name* : une erreur s'est produite au cours de l'exécution du plug-in.
- Un problème a été détecté au niveau de la syntaxe du fichier `audit_control`. Par défaut, un message est envoyé à la console. L'e-mail est également envoyé à l'alias `audit_warn`.

Si la stratégie d'audit `perzone` est définie, l'instance de zone non globale d'`auditd` appelle le script `audit_warn` de cette zone. Pour plus d'informations, reportez-vous à la page de manuel `audit_warn`(1M).

Script `bsmconv`

Le script `/etc/security/bsmconv` active le service d'audit. La commande `bsmunconv` désactive le service d'audit. Une fois le script `bsmconv` exécuté, vous devez configurer les répertoires et fichiers de configuration de l'audit. Lors du redémarrage, l'audit est activé.

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

Profils de droits d'accès pour l'administration de l'audit

Oracle Solaris fournit des profils de droits pour la configuration du service d'audit et pour l'analyse de la piste d'audit.

- **Audit Control (Contrôle d'audit)** : permet à un rôle de configurer l'audit Oracle Solaris. Ce profil de droits fournit des autorisations pour configurer des fichiers qui sont utilisés par le service d'audit. Il permet également à un rôle d'exécuter des commandes d'audit. Un rôle avec le profil Audit Control peut exécuter les commandes suivantes : `audit`, `auditd`, `auditconfig`, `bsmconv` et `bsmunconv`.

- **Audit Review (Vérification d'audit)** : permet à un rôle d'analyser les enregistrements d'audit Oracle Solaris. Ce profil de droits accorde l'autorisation de lire les enregistrements d'audit avec les commandes `praudit` et `auditreduce`. Un rôle avec ce profil de droits peut également exécuter la commande `auditstat`.
- **System Administrator (Administrateur système)** : inclut le profil de droits Audit Review. Un rôle avec le profil de droits System Administrator peut analyser les enregistrements d'audit.

Pour configurer des rôles permettant de gérer le service d'audit, reportez-vous à la section "Configuration de RBAC (liste des tâches)" à la page 208.

Audit et zones Oracle Solaris

Les zones non globales peuvent être auditées exactement comme la zone globale ou définir leurs propres indicateurs et stratégies de stockage et d'audit.

Lorsque toutes les zones sont auditées de la même façon, les fichiers de configuration dans la zone globale fournissent les paramètres d'audit pour chaque zone. L'option de stratégie `+zonename` est utile. Lorsque cette option est définie, les enregistrements d'audit de toutes les zones incluent le nom de la zone. Les enregistrements d'audit peuvent ensuite être sélectionnés par nom de zone. Pour comprendre la stratégie d'audit, reportez-vous à la section "Détermination de la stratégie d'audit" à la page 611. La section "Configuration de la stratégie d'audit" à la page 635 présente un exemple.

Les zones peuvent également être auditées individuellement. Lorsque l'option de stratégie `perzone` est définie dans la zone globale, chaque zone non globale exécute son propre démon d'audit, gère sa propre file d'attente d'audit et indique le contenu et l'emplacement de ses enregistrements d'audit. Une zone non globale peut également définir la plupart options de la stratégie d'audit. Elle ne peut pas définir une stratégie qui a une incidence sur l'ensemble du système, et ne peut donc pas définir la stratégie `ahlt` ou `perzone`. Pour plus d'informations, reportez-vous aux sections "Audit sur un système à zones Oracle Solaris" à la page 602 et "Procédure de planification de l'audit par zone " à la page 606.

Pour en savoir plus sur les zones, reportez-vous à la Partie II, "Zones" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Classes d'audit

Les valeurs par défaut du système pour l'audit Oracle Solaris sont présélectionnées en spécifiant une ou plusieurs classes d'événements. Les classes sont présélectionnées pour chaque système dans le fichier système `audit_control`. Toute personne qui utilise le système est auditée pour ces classes d'événements. Le fichier est décrit dans la section "Fichier `audit_control`" à la page 678.

Vous pouvez configurer les classes d'audit et effectuer de nouvelles classes d'audit. Les noms de classe d'audit peuvent contenir jusqu'à 8 caractères. La description de la classe est limitée à 72 caractères. Les caractères numériques et non alphanumériques sont autorisés.

Vous pouvez modifier les objets à auditer pour chaque utilisateur en ajoutant des classes d'audit à l'entrée utilisateur dans la base de données `audit_user`. Les classes d'audit sont également utilisées en tant qu'arguments de la commande `auditconfig`. Pour plus d'informations, reportez-vous à la page de manuel `auditconfig(1M)`.

Définition de classes d'audit

Le tableau suivant présente chaque classe d'audit prédéfinie, le nom descriptif pour chaque classe d'audit, ainsi qu'une brève description.

TABLEAU 31–1 Classes d'audit prédéfinies

Classe d'audit	Nom descriptif	Description
`all`	`all`	Toutes les classes (métaclasse)
`no`	`no_class`	Valeur Null pour désactiver la présélection d'événements.
`na`	`non_attrib`	Événements non allouables
`fr`	`file_read`	Lecture de données, ouverture pour la lecture
`fw`	`file_write`	Écriture de données, ouverture pour l'écriture
`fa`	`file_attr_acc`	Accès des attributs d'objet : `stat`, `pathconf`
`fm`	`file_attr_mod`	Modification des attributs d'objet : `chown`, `flock`
`fc`	`file_creation`	Création d'objet
`fd`	`file_deletion`	Suppression d'objet
`cl`	`file_close`	`close`, appel système
`ap`	`application`	Événement défini par l'application
`ad`	`administrative`	Actions d'administration (ancienne métaclasse administrative)
`am`	`administrative`	Actions d'administration (métaclasse)

TABLEAU 31–1 Classes d'audit prédéfinies *(Suite)*

Classe d'audit	Nom descriptif	Description
ss	État du système	Modification de l'état du système
as	system-wide administration	Administration du système entier
ua	user administration	Administration des utilisateurs
aa	audit administration	Utilisation d'audit
ps	process start	Début et arrêt de processus
pm	process modify	Modification de processus
pc	process	Processus (métaclasse)
ex	exec	Exécution de programme
io	ioctl	ioctl(), appel système
ip	ipc	Opérations IPC System V
lo	login_logout	Événements de connexion et de déconnexion
nt	network	Événements réseau : bind, connect, accept
ot	other	Divers, par exemple, l'allocation de périphériques et memcntl()

Vous pouvez définir de nouvelles classes en modifiant le fichier /etc/security/audit_class. Vous pouvez également renommer des classes existantes. Pour plus d'informations, reportez-vous à la page de manuel audit_class(4).

Syntaxe de classe d'audit

Les résultats des événements (échecs et réussites) peuvent être audités. Sans préfixe, l'audit d'une classe d'événements porte à la fois sur les réussites et les échecs. Avec un signe plus (+) en préfixe, l'audit d'une classe d'événements porte uniquement sur les réussites. Avec un signe moins (-) en préfixe, l'audit d'une classe d'événements porte uniquement sur les échecs. Le tableau suivant indique des représentations possibles des classes d'audit.

TABLEAU 31–2 Préfixes plus et moins pour les classes d'audit

[*préfixe*] *classe*	Explication
lo	Audit sur toutes les tentatives réussies de connexion et déconnexion, et sur tous les échecs de connexion. Un utilisateur ne peut pas échouer lors d'une tentative de connexion.
+lo	Audit sur toutes les tentatives réussies de connexion et déconnexion.

TABLEAU 31–2 Préfixes plus et moins pour les classes d'audit *(Suite)*

[*préfixe*] *classe*	Explication
`-all`	Audit sur tous les événements d'échec.
`+all`	Audit sur tous les événements de réussite.

Attention – La classe `all` peut générer de grandes quantités de données d'audit et remplir rapidement les systèmes de fichiers. Utilisez la classe `all` uniquement lorsque vous avez des raisons d'auditer toutes les activités.

Après avoir sélectionné des classes d'audit, vous pouvez les modifier en ajoutant un accent circonflexe ^ en préfixe. Le tableau suivant montre comment l'accent circonflexe en préfixe modifie une classe d'audit présélectionnée.

TABLEAU 31–3 Accent circonflexe en préfixe de classes d'audit déjà spécifiées

^[*préfixe*]*classe*	Explication
`-all,^-fc`	Audit de tous les événements d'échec, à l'exception des tentatives de création d'objet fichier ayant échoué.
`am,^+aa`	Audit de tous les événements d'administration, qu'il s'agisse d'échecs ou de réussites, à l'exception les tentatives réussies d'administration de l'audit.
`am,^ua`	Audit de tous les événements d'administration, qu'il s'agisse d'échecs ou de réussites, à l'exception des événements d'administration des utilisateurs.

Les classes d'audit et leurs préfixes peuvent être utilisés dans les fichiers et commandes ci-après :

- Dans la ligne `flags` du fichier `audit_control`
- Dans la ligne `plugin:name=audit_syslog.so; p_flags=` du fichier `audit_control`
- Dans l'entrée utilisateur de la base de données `audit_user`
- En tant qu'arguments des options de la commande `auditconfig`

La section "Fichier `audit_control`" à la page 678 présente un exemple d'utilisation des préfixes dans le fichier `audit_control`.

Plug-ins d'audit

Les plug-ins d'audit indiquent comment traiter les enregistrements d'audit dans la file d'attente d'audit. Ils sont spécifiés par leur nom dans le fichier `audit_control` : `audit_binfile.so` et `audit_syslog.so`. Les plug-ins et leurs paramètres permettent d'indiquer les éléments suivants :

- Où envoyer les données binaires, en utilisant le plug-in `audit_binfile.so` et le paramètre `p_dir`
- L'espace minimum restant sur un disque avant que l'administrateur ne reçoive un avertissement d'espace limite, en utilisant le plug-in `audit_binfile.so` et le paramètre `p_minfree`
- La taille maximale d'un fichier d'audit, en utilisant le plug-in `audit_binfile.so` et le paramètre `p_dirfsizefsize`

  Le paramètre `p_fsize` du plug-in est disponible à partir de la version Solaris 10 10/08.
- Une sélection d'enregistrements d'audit à envoyer à `syslog`, en utilisant le plug-in `audit_syslog.so` et le paramètre `p_flags`
- Le nombre maximum d'enregistrements d'audit mis en file d'attente pour le plug-in, en utilisant le paramètre de plug-in `qsize`

Reportez-vous aux pages de manuel `audit_binfile(5)`, `audit_syslog(5)` et `audit_control(4)`.

Stratégie d'audit

La stratégie d'audit détermine si des informations supplémentaires sont ajoutées à la piste d'audit.

Les stratégies suivantes ajoutent des jetons aux enregistrements d'audit : `arge`, `argv`, `group`, `path`, `seq`, `trail`, `windata_down`, `windata_up` et `zonename`.

Les autres stratégies n'ajoutent pas de jetons. Les stratégies `ahlt` et `cnt` déterminent ce qui se passe lorsque les enregistrements d'audit du noyau ne peuvent pas être transmis, la stratégie `public` limite l'audit aux fichiers publics et la stratégie `perzone` établit des files d'attente d'audit distinctes pour les zones non globales.

Les effets des différentes options de stratégie d'audit sont décrits dans la section "Détermination de la stratégie d'audit" à la page 611. Pour connaître les différentes options de stratégie d'audit, reportez-vous à la section sur l'option `-setpolicy` de la page de manuel `auditconfig(1M)`. Pour obtenir la liste des options disponibles, exécutez la commande `auditconfig -lspolicy`.

Caractéristiques de l'audit des processus

Lors de la connexion initiale, l'audit est défini selon les caractéristiques suivantes :

- **Masque de présélection du processus** : combinaison des classes d'audit issues du fichier `audit_control` et de la base de données `audit_user`. Lorsqu'un utilisateur se connecte, le processus de connexion combine les classes présélectionnées afin d'établir le *masque de présélection* des processus utilisateur. Ce masque de présélection de processus détermine la création ou non d'enregistrements d'audit selon les événements de chaque classe d'audit.

  L'algorithme suivant décrit la façon dont le système obtient le masque de présélection de processus utilisateur :

  `(flags` *line* `+` *always-audit-classes*`)` `-` *never-audit-classes*

  Ajoute les classes d'audit de la ligne `flags` du fichier `audit_control` dans les classes du champ *always-audit-classes* de l'entrée utilisateur de la base de données `audit_user`. Ensuite, effectue une soustraction à partir de la somme des classes indiquée dans le champ utilisateur *never-audit-classes*.
- **ID d'audit** : un processus acquiert un ID d'audit lorsque l'utilisateur se connecte. L'ID d'audit est hérité par tous les processus enfant qui ont été lancés par le processus utilisateur initial. L'ID d'audit permet d'appliquer la responsabilité. Même après qu'un utilisateur devient `root`, l'ID d'audit reste le même. L'ID d'audit enregistré dans chaque enregistrement d'audit vous permet toujours de retracer les actions jusqu'à l'utilisateur d'origine qui s'était connecté.
- ??**ID de session d'audit** : ID de session d'audit assigné lors de la connexion. Tous les processus enfants héritent de l'ID de session.
- **ID du terminal (ID de port, adresse de la machine)** : formé d'un nom d'hôte et de l'adresse Internet, l'ID du terminal est suivi d'un numéro unique qui identifie le périphérique physique sur lequel l'utilisateur est connecté. Le plus souvent, la connexion s'effectue par l'intermédiaire de la console. Le nombre qui correspond au périphérique de la console est `0`.

Piste d'audit

La *piste d'audit* contient des fichiers d'audit binaires. La piste est créée par le démon `auditd`. Une fois que le service d'audit a été activé avec la commande `bsmconv`, le démon `auditd` démon démarre lorsque le système est amorcé. Le démon `auditd` est responsable de la collecte de données de la piste d'audit et de l'écriture des enregistrements d'audit.

Les enregistrements d'audit sont stockés dans un format binaire sur les systèmes de fichiers qui sont dédiés aux fichiers d'audit. Même si vous pouvez physiquement placer des répertoires d'audit dans des systèmes de fichiers qui ne sont pas dédiés à l'audit, *ne le faites pas*, sauf en dernier recours. Les répertoires utilisés en dernier recours sont des répertoires dans lesquels les fichiers d'audit sont écrits uniquement lorsqu'aucun autre répertoire approprié n'est disponible.

Il existe un autre scénario qui autorise le placement de répertoires d'audit en dehors des systèmes de fichiers d'audit dédiés. Vous pouvez le faire dans un environnement de développement logiciel où l'audit est facultatif. Il est souvent plus important de garantir une utilisation optimale de l'espace disque que de conserver une piste d'audit. Cependant, dans un environnement sécurisé, le placement des répertoires d'audit au sein d'autres systèmes de fichiers n'est pas acceptable.

Vous devez également prendre en considération les facteurs suivants lors de l'administration des systèmes de fichiers d'audit :

- Un hôte doit avoir au moins un répertoire d'audit local. Le répertoire local peut être utilisé comme un répertoire de dernier recours si l'hôte n'est pas en mesure de communiquer avec le serveur d'audit.
- Les répertoires d'audit doivent être montés avec l'option read-write (`rw`). Lorsque vous montez des répertoires d'audit à distance, utilisez également les options `intr` et `noac`.
- Les systèmes de fichiers d'audit doivent être spécifiés sur le serveur d'audit dans lequel ils résident. La liste d'exportation doit inclure tous les systèmes qui sont en cours d'audit au niveau du site.

Conventions relatives aux noms de fichiers d'audit binaires

Chaque fichier d'audit binaire est un ensemble d'enregistrements autonome. Le nom du fichier identifie l'intervalle de temps pendant lequel les enregistrements ont été générés et le système qui les a générés.

Noms de fichiers d'audit binaires

Les fichiers d'audit terminés sont nommés de la manière suivante :

start-time.end-time.system

start-time Heure à laquelle le premier enregistrement d'audit a été généré dans le fichier d'audit.

end-time Heure à laquelle le dernier enregistrement a été écrit dans le fichier.

system Nom du système qui a généré le fichier.

Un fichier d'audit qui est toujours actif est nommé de la manière suivante :

start-time`.not_terminated.`*system*

Pour consulter des exemples de noms de fichiers d'audit `not_terminated` et fermés, reportez-vous à la section “Nettoyage d'un fichier d'audit `not_terminated` ” à la page 654.

Horodatages des fichiers d'audit binaires

Les horodatages dans les noms de fichiers sont utilisés par la commande `auditreduce` pour trouver les enregistrements au sein d'une plage de temps spécifique. Ces horodatages sont importants car il peut y avoir un mois ou plus d'accumulation de fichiers d'audit en ligne. Rechercher dans tous les fichiers pour les enregistrements qui ont été générés au cours des dernières 24 heures serait beaucoup trop cher.

Les valeurs *start-time* et *end-time* sont des horodatages à la seconde près. Elles sont spécifiées selon l'heure moyenne de Greenwich (GMT). Le format est composé de quatre chiffres pour l'année, suivi de deux chiffres pour chaque mois, le jour, l'heure, la minute et la seconde, comme suit :

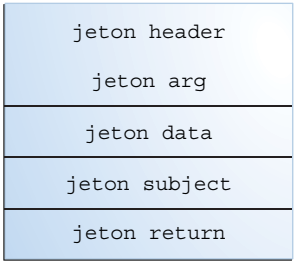
YYYYMMDDHHMMSS

Les horodatages sont à l'heure GMT pour s'assurer qu'ils trient dans le bon ordre, même sur plusieurs fuseaux horaires. En raison de ce rapport à l'heure GMT, la date et l'heure doivent être converties dans le fuseau horaire actuel pour être significatives. Faites-y attention chaque fois que vous manipulez ces fichiers avec des commandes de fichiers standard plutôt qu'avec la commande `auditreduce`.

Structure d'enregistrement d'audit

Un enregistrement d'audit est une séquence de jetons d'audit. Chaque jeton d'audit contient des informations sur les événements tels que l'ID utilisateur, la date et l'heure. Un jeton `header` commence un enregistrement d'audit et un jeton `trailer` peut éventuellement conclure l'enregistrement. D'autres jetons d'audit contiennent des informations relatives à l'événement d'audit. La figure suivante illustre un enregistrement d'audit standard.

FIGURE 31–3 Structure d'enregistrement d'audit standard



Analyse d'enregistrement d'audit

L'analyse d'enregistrement d'audit implique la sélection des enregistrements dans la piste d'audit. Vous pouvez utiliser l'un des deux approches pour l'analyse syntaxique des données binaires qui ont été collectées.

- Vous pouvez analyser le flux de données binaires. Pour analyser le flux de données, vous avez besoin de connaître l'ordre des champs dans chaque jeton, et l'ordre des jetons dans chaque enregistrement. Vous devez également connaître les variantes d'un enregistrement d'audit. Par exemple, l'appel système `ioctl()` crée un enregistrement d'audit pour "nom de fichier incorrect" qui contient différentes unités lexicales dans l'enregistrement de l'audit pour "descripteur de fichier incorrect".
  - Pour obtenir une description de l'ordre des données binaires dans chaque jeton d'audit, reportez-vous à la page de manuel `audit.log(4)`.
  - Pour obtenir une description de l'ordre des jetons dans un enregistrement d'audit, utilisez la commande `bsmrecord`. La sortie de la commande `bsmrecord` inclut les différents formats qui se produisent dans diverses conditions. Les crochets (`[]`) indiquent qu'un jeton d'audit est facultatif. Pour plus d'informations, reportez-vous à la page de manuel `bsmrecord(1M)`. Pour consulter des exemples, reportez-vous également à la section “Affichage des formats d'enregistrement d'audit ” à la page 647.
- Vous pouvez, pour ce faire, exécuter la commande `ping`. Les options de la commande fournissent des sorties de texte différentes. Par exemple, la commande `praudit -x` fournit du XML pour l'entrée dans les scripts et navigateurs. Les sorties `praudit` n'incluent pas les champs dont le seul but est d'aider à analyser les données binaires. Les sorties ne suivent pas nécessairement l'ordre des champs binaires. De plus, l'ordre et le format de la sortie `praudit` peuvent être différents selon la version Oracle Solaris.

  Pour consulter des exemples de sortie `praudit`, reportez-vous à la section “Affichage du contenu des fichiers d'audit binaires” à la page 653, et à la page de manuel `praudit(1M)`.

  Pour avoir une description de la sortie `praudit` pour chaque jeton d'audit, reportez-vous aux différents jetons répertoriés dans la section “Formats de jeton d'audit ” à la page 692.

Formats de jeton d'audit

Chaque jeton d'audit possède un identificateur de type de jeton, suivi par les données spécifiques au jeton. Chaque type de jeton possède son propre format. Le tableau ci-après indique les noms de jetons avec une brève description de chaque jeton. Les jetons obsolètes sont conservés pour des raisons de compatibilité avec les versions précédentes de Solaris.

TABLEAU 31–4 Jetons d'audit pour l'audit Oracle Solaris

Nom de variable	Description	Pour plus d'informations
`acl ;`	Liste de contrôle d'accès (ACL, Access Control List)	"Jeton `acl`" à la page 694
`arbitrary`	Données avec informations de format et de type	"Jeton `arbitrary` (obsolète)" à la page 694
`arg`	Valeur de l'argument d'appel système	"Jeton `arg`" à la page 695
`attribut`	Jetons vnode du fichier	"Jeton `attribute`" à la page 696
`cmd`	Arguments de commande et variables d'environnement	"Jeton `cmd`" à la page 696
`exec_args`	Arguments d'appel système Exec	"Jeton `exec_args`" à la page 697
`exec_env`	Variables d'environnement d'appel système Exec	"Jeton `exec_env`" à la page 697
`exit`	Informations sur la sortie du programme	"Jeton `exit` (obsolète) " à la page 698
`fichier`	Informations sur le fichier d'audit	"Jeton `file`" à la page 698
`group`	Informations sur les groupes de processus	"Jeton `group` (obsolète) " à la page 698
`groups`	Informations sur les groupes de processus	"Jeton `groups`" à la page 698
`header`	Indique le début de l'enregistrement d'audit	"Jeton `header` " à la page 699
`ip_addr`	Adresse Internet	"Jeton `ip_addr` " à la page 699
`ip`	Informations sur l'en-tête IP	"Jeton `ip` (obsolète) " à la page 700
`ipc`	Informations sur l'IPC System V	"Jeton `ipc`" à la page 700
`ipc_perm`	Jetons objet IPC System V	"Jeton `ipc_perm`" à la page 701
`iport`	Adresse du port Internet	"Jeton `iport`" à la page 702
`opaque`	Données non structurées (format non spécifié)	"Jeton `opaque` (obsolète) " à la page 702
`path`	Informations relatives aux chemins	"Jeton `path`" à la page 702
`path_attr`	Informations relatives aux chemins d'accès	"Jeton `path_attr`" à la page 703
`privilège`	Informations sur le jeu de privilèges	"Jeton `privilege`" à la page 703
`processus`	Informations sur le jeton de processus	"Jeton `process`" à la page 704
`return`	Statut des appels système	"Jeton `return`" à la page 705
`sequence`	Jeton de numéro de séquence	"Jeton `sequence`" à la page 706
`socket`	Types de socket et adresses	"Jeton `socket`" à la page 706
`sujet`	Jeton de sujet (même format que le jeton `process`)	"Jeton `subject`" à la page 707

TABLEAU 31–4 Jetons d'audit pour l'audit Oracle Solaris *(Suite)*

Nom de variable	Description	Pour plus d'informations
`text`	Chaîne de caractères ASCII	"Jeton `text`" à la page 709
`trailer`	Indique la fin de l'enregistrement d'audit	"Jeton `trailer`" à la page 709
`uauth`	Utilisation d'autorisation	"Jeton `uauth`" à la page 710
`upriv`	Utilisation de privilège	"Jeton `upriv`" à la page 710
`zonename`	Nom de la zone	"Jeton `zonename`" à la page 710

Un enregistrement d'audit commence toujours par un jeton `header`. Ce jeton `header` indique l'endroit où l'enregistrement d'audit commence dans la piste d'audit. Dans le cas d'événements attribuables, les jetons `subject` et `process` font référence aux valeurs du processus qui ont causé l'événement. Dans le cas d'événements non attribuables, le jeton `process` fait référence au système.

Jeton `acl`

Le jeton `acl` enregistre des informations sur la liste de contrôle d'accès (ACL).

Le jeton `acl` se compose de quatre champs fixes :

- Un ID de jeton qui identifie ce jeton comme un jeton `acl`
- Un champ qui spécifie le type d'ACL
- Un champ de valeur pour l'ACL
- Un champ qui répertorie les droits d'accès associés à cette liste de contrôle d'accès

La commande `praudit -x` affiche les champs du jeton `acl` :

```
<acl type="1" value="root" mode="6"/>
```

Jeton `arbitrary` (obsolète)

Le jeton `arbitrary` encapsule les données pour la piste d'audit. Ce jeton se compose de quatre champs fixes et d'une série de données. Les champs fixes sont comme suit :

- Un ID de jeton qui identifie ce jeton comme un jeton `arbitrary`
- Un champ de format d'impression suggéré, au format hexadécimal
- Champ de taille d'élément qui spécifie la taille des données encapsulées, par exemple "short" (court)
- Champ numérique qui fournit le nombre d'éléments suivants

Le reste du jeton est composé du *nombre* du type spécifié. La commande `praudit` affiche le jeton `arbitrary` de la manière suivante :

```
arbitrary,decimal,int,1
42
```

Le tableau suivant affiche les valeurs possibles du champ du format d'impression.

TABLEAU 31–5 Valeurs du champ du format d'impression du jeton `arbitrary`

Valeur	Action
`AUP_BINARY`	Imprime la date au format binaire
`AUP_OCTAL`	Imprime la date au format octal
`AUP_DECIMAL`	Imprime la date au format décimal
`AUP_HEX`	Imprime la date au format hexadécimal
`AUP_STRING`	Imprime la date sous forme de chaîne

Le tableau ci-dessous présente les valeurs possibles du champ de taille d'élément.

TABLEAU 31–6 Valeurs du champ de taille d'élément du jeton `arbitrary`

Valeur	Action
`AUR_BYTE`	Imprime les données en octets dans 1 octet
`AUR_SHORT`	Imprime les données en unités courtes dans 2 octets
`AUR_LONG`	Imprime les données en unités longues dans 4 octets

Jeton `arg`

Le jeton `arg` contient des informations sur les arguments d'un appel système : le numéro de l'argument de l'appel système, la valeur de l'argument et une description facultative. Ce jeton autorise un argument d'appel système de type entier 32 bits dans un enregistrement d'audit.

Le jeton `arg` a cinq champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `arg`
- Un ID d'argument qui détermine l'argument d'appel système auquel le jeton fait référence
- La valeur de l'argument
- La longueur de la chaîne de texte descriptif
- La chaîne de texte

La commande `praudit -x` affiche les champs du jeton `arg` :

```
<argument arg-num="2" value="0x0" desc="new file uid"/>
```

Jeton attribute

Le jeton attribute contient des informations issues du fichier vnode.

Le jeton attribute a sept champs :

- Un ID de jeton qui identifie ce jeton comme un jeton attribute
- Le mode et le type d'accès au fichier
- L'ID utilisateur du propriétaire
- L'ID de groupe du propriétaire
- L'ID du système de fichiers
- L'ID du nœud
- L'ID du périphérique que le fichier peut représenter

Pour plus d'informations sur l'ID du système de fichiers et l'ID du périphérique, reportez-vous à la page de manuel statvfs(2).

Le jeton attribute s'accompagne habituellement d'un jeton path. Le jeton attribute est produit pendant les recherches de chemins. Si une erreur de recherche de chemin se produit, aucun vnode ne permet d'obtenir les informations requises sur le fichier. Par conséquent, le jeton attribute n'est pas inclus dans l'enregistrement d'audit. La commande praudit -x affiche les champs du jeton attribute :

```
<attribute mode="100644" uid="adm" gid="adm" fsid="136" nodeid="2040" device="0"/>
```

Jeton cmd

Le jeton cmd enregistre la liste d'arguments et la liste de variables d'environnement associées à une commande.

Le jeton cmd contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton cmd
- Un nombre d'arguments de commande
- La liste d'arguments
- La longueur du champ suivant
- Le contenu des arguments
- Un nombre de variables d'environnement
- La liste des variables d'environnement
- La longueur du champ suivant
- Le contenu de ces variables d'environnement

La commande praudit -x affiche les champs du jeton cmd : L'exemple suivant est un jeton cmd tronqué. La ligne est renvoyée à des fins d'affichage.

```
<cmd><arge>WINDOWID=6823679</arge>
<arge>COLORTERM=gnome-terminal</arge>
<arge>...LANG=C</arge>...<arge>HOST=machine1</arge>
<arge>LPDEST=printer1</arge>...</cmd>
```

Jeton exec_args

Le jeton exec_args enregistre les arguments d'un appel système exec(). Le jeton exec_args a deux champs fixes :

- Un ID de jeton qui identifie ce jeton comme un jeton exec_args
- Un nombre représentant le nombre d'arguments transmis à l'appel système exec()

Le reste du jeton est composé de chaînes *numériques*. La commande praudit -x affiche les champs du jeton exec_args :

```
<exec_args><arg>/usr/bin/sh</arg><arg>/usr/bin/hostname</arg></exec_args>
```

Remarque – Le jeton exec_args s'affiche en sortie uniquement lorsque l'option de stratégie d'audit argv est active.

Jeton exec_env

Le jeton exec_env enregistre les variables d'environnement actuel transmises à un appel système exec(). Le jeton exec_env a deux champs fixes :

- Un ID de jeton qui identifie ce jeton comme un jeton exec_env
- Un nombre représentant le nombre d'arguments transmis à l'appel système exec()

Le reste du jeton est composé de chaînes *numériques*. La commande praudit -x affiche les champs du jeton exec_env : La ligne est renvoyée à des fins d'affichage.

```
<exec_env><env>_=/usr/bin/hostname</env>
<env>DTXSERVERLOCATION=local</env><env>SESSIONTYPE=altDt</env>
<env>LANG=C</env><env>SDT_NO_TOOLTALK=1</env><env>SDT_ALT_HELLO=/bin/true</env>
<env>PATH=/usr/bin:/usr/openwin/bin:/usr/ucb</env>
<env>OPENWINHOME=/usr/openwin</env><env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env><env>START_SPECKEYSD=no</env>
<env>SDT_ALT_SESSION=/usr/dt/config/Xsession2.jds</env><env>HOME=/home/jdoe</env>
<env>SDT_NO_DTDBCACHE=1</env><env>PWD=/home/jdoe</env><env>TZ=US/Pacific</env>
</exec_env>
```

Remarque – Le jeton exec_env s'affiche en sortie uniquement lorsque l'option de stratégie d'audit arge est active.

Jeton `exit` (obsolète)

Le jeton `exit` enregistre l'état de sortie d'un programme. Le jeton `exit` contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton `exit`
- L'état de sortie de programme transmis à l'appel système `exit()`
- Une valeur de retour qui décrit l'état de sortie ou qui fournit un numéro d'erreur système

La commande `praudit` affiche le jeton `exit` de la manière suivante :

```
exit,Error 0,0
```

Jeton `file`

Le jeton `file` est un jeton spécial généré par le démon `auditd`. Le jeton marque le début d'un nouveau fichier d'audit et la fin d'un ancien fichier d'audit lorsque l'ancien fichier est désactivé. Le premier jeton `file` identifie le fichier précédent dans la piste d'audit. Le dernier jeton `file` identifie le fichier suivant dans la piste d'audit. Le démon `auditd` crée un enregistrement d'audit spécial qui contient ce jeton pour lier les fichiers d'audit successifs dans une seule piste d'audit.

La commande `praudit -x` affiche les champs du jeton `file`. Ce jeton identifie le fichier suivant dans la piste d'audit. La ligne est renvoyée à des fins d'affichage.

```
<file iso8601="2009-04-08 14:18:26.200 -07:00">
/var/audit/machine1/files/20090408211826.not_terminated.machine1</file>
```

Jeton `group` (obsolète)

Ce jeton a été remplacé par le jeton `groups`. Voir "Jeton `groups`" à la page 698.

Jeton `groups`

Le jeton `groups` remplace le jeton `group`. Le jeton `groups` enregistre les entrées de groupe dans les données d'identification du processus.

Le jeton `groups` a deux champs fixes :

- Un ID de jeton qui identifie ce jeton comme un jeton `groups`
- Un nombre représentant le nombre de groupes contenus dans cet enregistrement d'audit

Le reste du jeton est composé d'entrées de groupe *numériques*.

La commande `praudit -x` affiche les champs du jeton `groups` :

```
<group><gid>staff</gid><gid>other</gid></group>
```

Remarque – Le jeton `groupes` s'affiche en sortie uniquement lorsque l'option de stratégie d'audit `group` est active.

Jeton `header`

Le jeton `header` est spécial car il marque le début d'un enregistrement d'audit. Le jeton `header` se combine avec le jeton `trailer` pour entourer tous les autres jetons de l'enregistrement.

Le jeton `header` a huit champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `header`
- Un nombre d'octets représentant la longueur totale de l'enregistrement d'audit, y compris les jetons `header` et `trailer`
- Un numéro de version, qui identifie la version de la structure de l'enregistrement d'audit
- L'ID permettant d'identifier l'événement d'audit représenté par l'enregistrement
- Le modificateur d'ID qui identifie des caractéristiques spécifiques de l'événement d'audit

  Le champ modificateur d'ID est associé aux indicateurs suivants :

  ```
  0x4000          PAD_NOTATTR                     nonattributable event
  0x8000          PAD_FAILURE                     failed audit event
  ```
- Le type d'adresse IPv4 ou IPv6
- L'adresse de l'ordinateur
- L'heure et la date à laquelle l'enregistrement a été créé

Sur les systèmes 64 bits, le jeton `header` s'affiche avec un horodatage 64 bits à la place de l'horodatage 32 bits.

La commande `praudit` affiche le jeton `header` de la manière suivante :

```
header,69,2,su,,machine1,2009-04-08 13:11:58.209 -07:00
```

La commande `praudit -x` affiche les champs du jeton `header` au début de l'enregistrement d'audit. La ligne est renvoyée à des fins d'affichage.

```
<record version="2" event="su" host="machine1"
iso8601="2009-04-08 13:11:58.209 -07:00">
```

Jeton `ip_addr`

Le jeton `ip_addr` contient une adresse de protocole Internet. Depuis la version Solaris 8, l'adresse Internet peut être affichée dans format IPv4 ou IPv6. L'adresse IPv4 utilise 4 octets. L'adresse IPv6 utilise 1 octet pour décrire le type d'adresse, et 16 octets pour décrire l'adresse.

Le jeton `in_addr` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `in_addr`
- Le type d'adresse IP au format IPv4 ou IPv6
- Une adresse IP

La commande `praudit -x` affiche le contenu du jeton `ip_addr` :

```
<ip_address>machine1</ip_address>
```

Jeton `ip` (obsolète)

Le jeton `ip` contient une copie d'un en-tête de protocole Internet. Le jeton `ip` a deux champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `ip`
- Une copie de l'en-tête IP, c'est-à-dire les 20 octets

La commande `praudit` affiche le jeton `ip` de la manière suivante :

```
ip address,0.0.0.0
```

La structure de l'en-tête IP est définie dans le fichier `/usr/include/netinet/ip.h`.

Jeton `ipc`

Le jeton `ipc` contient les identificateurs IPC System V de message, de sémaphore ou de mémoire partagée qui sont utilisés par le programme appelant pour identifier un objet IPC.

Le jeton `ipc` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `ipc`
- Un champ de type qui spécifie le type d'objet IPC
- L'identificateur de l'objet IPC

Remarque – Les identificateurs d'objet IPC ne respectent pas la nature sans contexte des jetons d'audit Oracle Solaris. Aucun "nom" global n'identifie de manière unique les objets IPC. Au lieu de cela, les objets IPC sont identifiés par leurs identificateurs. Ces identificateurs ne sont valides que pendant la période au cours de laquelle les objets IPC sont actifs. Toutefois, l'identification des objets IPC ne constitue pas un problème. Les mécanismes des IPC System V IPC sont rarement utilisés et partagent tous la même classe d'audit.

Le tableau ci-dessous présente les valeurs possibles du champ du type d'objet IPC. Ces valeurs sont définies dans le fichier `/usr/include/bsm/audit.h`.

TABLEAU 31–7 Valeurs du champ du type d'objet IPC

Nom	Valeur	Description
AU_IPC_MSG	1	Objet de message IPC
AU_IPC_SEM	2	Objet de sémaphore IPC
AU_IPC_SHM	3	Objet de mémoire partagée IPC

La commande `praudit -x` affiche les champs du jeton `ipc` :

```
<IPC ipc-type="shm" ipc-id="15"/>
```

Jeton `ipc_perm`

Le jeton `ipc_perm` contient une copie des autorisations d'accès de l'IPC System V. Ce jeton est ajouté aux enregistrements d'audit générés par les événements IPC de mémoire partagée, de sémaphore et de message.

Le jeton `ipc_perm` a huit champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `ipc_perm`
- L'ID utilisateur du propriétaire de l'IPC
- L'ID de groupe du propriétaire de l'IPC
- L'ID utilisateur du créateur de l'IPC
- L'ID du groupe du créateur de l'IPC
- Le mode d'accès de l'IPC
- Le numéro de séquence de l'IPC
- La valeur de clé IPC

La commande `praudit -x` affiche les champs du jeton `ipc_perm` : La ligne est renvoyée à des fins d'affichage.

```
<IPC_perm uid="jdoe" gid="staff" creator-uid="jdoe"
creator-gid="staff" mode="100600" seq="0" key="0x0"/>
```

Les valeurs sont récupérées à partir de la structure `ipc_perm` associée à l'objet IPC.

Jeton `iport`

Le jeton `iport` contient l'adresse de port TCP ou UDP.

Le jeton `iport` a deux champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `iport`
- L'adresse du port UDP ou TCP

La commande `praudit` affiche le jeton `iport` de la manière suivante :

```
ip port,0xf6d6
```

Jeton `opaque` (obsolète)

Le jeton `opaque` contient des données non formatées sous la forme d'une séquence d'octets. Le jeton `opaque` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `opaque`
- Un nombre d'octets pour les données
- Un tableau des données d'octet

La commande `praudit` affiche le jeton `opaque` de la manière suivante :

```
opaque,12,0x4f5041515545204441544100
```

Jeton `path`

Le jeton `path` contient les informations de chemin d'accès pour un objet.

Le jeton `path` contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton `path`
- La longueur du chemin
- Le chemin absolu de l'objet basé sur la racine réelle du système

La commande `praudit` affiche le jeton `path` sans le deuxième champ, de la manière suivante :

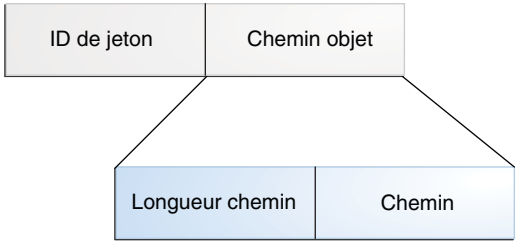
```
path,/etc/security/audit_user
```

La commande `praudit -x` affiche le contenu du jeton `path` :

```
<path>/etc/security/prof_attr</path>
```

La figure suivante illustre le format d'un jeton `path`.

FIGURE 31–4 Format du jeton `path`



Jeton `path_attr`

Le jeton `path_attr` contient les informations de chemin d'accès pour un objet. Le chemin d'accès spécifie la séquence d'objets de fichier d'attributs figurant sous l'objet de jeton `path`. Les appels système tels que `openat()` accèdent aux fichiers d'attributs. Pour plus d'informations sur les objets fichiers d'attributs, reportez-vous à la page de manuel `fsattr(5)`.

Le jeton `path_attr` contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton `path_attr`
- un nombre représentant le nombre de sections de chemins de fichiers d'attributs ;
- Chaînes *numériques* terminées par une valeur null

La commande `praudit` affiche le jeton `path_attr` de la manière suivante :

```
path_attr,1,attr_file_name
```

Jeton `privilege`

Le jeton `privilege` enregistre l'utilisation de privilèges sur un processus. Le jeton `privilege` n'est pas enregistrée pour les privilèges du jeu de base. Si un privilège a été supprimé du jeu de base par une action administrative, alors l'utilisation de ce privilège est enregistrée. Pour plus d'informations sur les privilèges, reportez-vous à la section “Privilèges (présentation)” à la page 197.

Le jeton `privilege` contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton `privilege`
- La longueur du champ suivant
- Le nom du jeu de privilèges
- La longueur du champ suivant
- La liste des privilèges

La commande `praudit -x` affiche les champs du jeton `privilege`. La ligne est renvoyée à des fins d'affichage.

```
<privilege set-type="Effective">file_chown,file_dac_read,
file_dac_write,net_privaddr,proc_exec,proc_fork,proc_setid</privilege>
```

Jeton `process`

Le jeton `process` contient des informations sur l'utilisateur associé à un processus, tels que le destinataire d'un signal.

Le jeton `process` a neuf champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `process`
- L'ID d'audit
- L'ID d'utilisateur effectif
- L'ID de groupe effectif
- L'ID utilisateur réel
- L'ID de groupe réel
- L'ID de processus
- L'ID de la session d'audit
- Un ID de terminal qui se compose d'un ID de périphérique et d'une adresse de la machine

L'ID d'audit, l'ID utilisateur, l'ID de groupe, l'ID de processus, et l'ID de session sont longs au lieu de courts.

Remarque – Les champs du jeton `process` correspondant à l'ID de session, l'ID utilisateur réel ou l'ID de groupe réel risquent de ne pas être disponibles. La valeur est alors définie sur `-1`.

Un jeton qui contient un ID de terminal a plusieurs variantes. La commande `praudit` masque ces variantes. Par conséquent, l'ID de terminal est géré de la même façon pour tous les jetons qui incluent un ID de terminal. L'ID de terminal est soit une adresse IP et un numéro de port, soit un ID de périphérique. Un ID de périphérique, tel que le port série connecté à un modem, peut être égal à zéro. L'ID de terminal est spécifié dans plusieurs formats.

L'ID de terminal pour les numéros de périphérique est spécifié comme suit :

- **Applications 32 bits** : numéro du périphérique à 4 octets, 4 octets inutilisés
- **Applications 64 bits** : numéro du périphérique à 8 octets, 4 octets inutilisés

Dans les versions antérieures à Solaris 8, l'ID de terminal pour les numéros de port est défini comme suit :

- **Applications 32 bits** : numéro de port à 4 octets, adresse IP à 4 octets
- **Applications 64 bits** : numéro de port à 8 octets, adresse IP à 4 octets

À partir de la version Solaris 8, l'ID de terminal pour les numéros de port est défini comme suit :

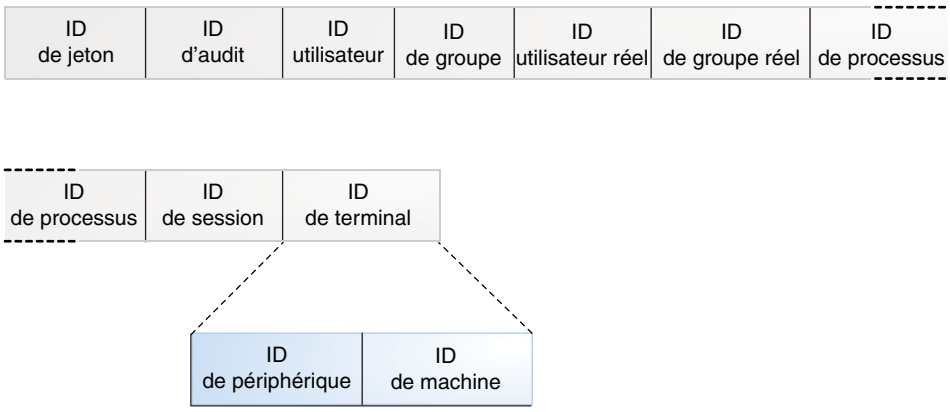
- **Applications 32 bits avec IPv4** : numéro de port à 4 octets, type IP à 4 octets, adresse IP à 4 octets
- **Applications 32 bits avec IPv6** : numéro de port à 4 octets, type IP à 4 octets, adresse IP à 16 octets
- **Applications 64 bits avec IPv4** : numéro de port à 8 octets, type IP à 4 octets, adresse IP à 4 octets
- **Applications 64 bits avec IPv6** : numéro de port à 8 octets, type IP à 4 octets, adresse IP à 16 octets

La commande `praudit -x` affiche les champs du jeton `process`. La ligne est renvoyée à des fins d'affichage.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="9" sid="0" tid="0 0 0.0.0.0"/>
```

La figure suivante illustre le format d'un jeton `process`.

FIGURE 31–5 Format du jeton `process`



Jeton `return`

Le jeton `return` contient l'état de retour de l'appel système (`u_error`) et la valeur de retour du processus (`u_rval1`).

Le jeton `return` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `return`
- L'état d'erreur de l'appel système
- La valeur de retour de l'appel système

Le jeton `return` est toujours retourné dans le cadre des enregistrements d'audit générés par le noyau pour les appels système. Dans l'audit de l'application, ce jeton indique l'état de sortie et d'autres valeurs de retour.

La commande `praudit` affiche le jeton `return` de la manière suivante :

```
return,failure: Operation now in progress,-1
```

La commande `praudit -x` affiche les champs du jeton `return` :

```
<return errval="failure: Operation now in progress" retval="-1/">
```

Jeton `sequence`

Le jeton `sequence` contient un numéro de séquence. Le numéro de séquence est incrémenté chaque fois qu'un enregistrement d'audit est ajouté à la piste d'audit. Ce jeton est utile pour le débogage.

Le jeton `sequence` a deux champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `sequence`
- Un champ long 32 bits non signé contenant le numéro de séquence

La commande `praudit` affiche les champs du jeton `sequence` :

```
sequence,1292
```

La commande `praudit -x` affiche le contenu du jeton `sequence` :

```
<sequence seq-num="1292"/>
```

Remarque – Le jeton `sequence` s'affiche en sortie uniquement lorsque l'option de stratégie d'audit `seq` est active.

Jeton `socket`

Le jeton `socket` contient des informations qui décrivent un socket Internet. Dans certaines instances, le jeton a quatre champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `socket`
- Un champ du type de socket qui indique le type de socket référencé, soit TCP, UDP ou UNIX
- Le port local
- L'adresse IP locale

La commande `praudit` affiche l'instance du jeton `socket` de la manière suivante :

```
socket,0x0002,0x83b1,localhost
```

Dans la plupart des instances, le jeton a huit champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `socket`
- Le domaine de socket
- Un champ du type de socket qui indique le type de socket référencé, soit TCP, UDP ou UNIX
- Le port local
- Le type d'adresse IPv4 ou IPv6
- L'adresse IP locale
- Le port distant
- L'adresse IP distante

Depuis la version Solaris 8, l'adresse Internet peut être affichée dans format IPv4 ou IPv6. L'adresse IPv4 utilise 4 octets. L'adresse IPv6 utilise 1 octet pour décrire le type d'adresse, et 16 octets pour décrire l'adresse.

La commande `praudit` affiche le jeton `socket` de la manière suivante :

```
socket,0x0002,0x0002,0x83cf,example1,0x2383,server1.Subdomain.Domain.COM
```

La commande `praudit -x` affiche les champs du jeton `socket`. La ligne est renvoyée à des fins d'affichage.

```
<socket sock_domain="0x0002" sock_type="0x0002" lport="0x83cf"
laddr="example1" fport="0x2383" faddr="server1.Subdomain.Domain.COM"/>
```

Jeton `subject`

Le jeton `subject` décrit un utilisateur qui exécute ou tente d'effectuer une opération. Le format est le même que le jeton `process`.

Le jeton `subject` a neuf champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `subject`
- L'ID d'audit
- L'ID d'utilisateur effectif
- L'ID de groupe effectif
- L'ID utilisateur réel
- L'ID de groupe réel

- L'ID de processus
- L'ID de la session d'audit
- Un ID de terminal qui se compose d'un ID de périphérique et d'une adresse IP de la machine

L'ID d'audit, l'ID utilisateur, l'ID de groupe, l'ID de processus, et l'ID de session sont longs au lieu de courts.

Remarque – Les champs du jeton `subject` correspondant à l'ID de session, l'ID utilisateur réel ou l'ID de groupe réel risquent de ne pas être disponibles. La valeur est alors définie sur `-1`.

Un jeton qui contient un ID de terminal a plusieurs variantes. La commande `praudit` masque ces variantes. Par conséquent, l'ID de terminal est géré de la même façon pour tous les jetons qui incluent un ID de terminal. L'ID de terminal est soit une adresse IP et un numéro de port, soit un ID de périphérique. Un ID de périphérique, tel que le port série connecté à un modem, peut être égal à zéro. L'ID de terminal est spécifié dans plusieurs formats.

L'ID de terminal pour les numéros de périphérique est spécifié comme suit :

- **Applications 32 bits** : numéro du périphérique à 4 octets, 4 octets inutilisés
- **Applications 64 bits** : numéro du périphérique à 8 octets, 4 octets inutilisés

Dans les versions antérieures à Solaris 8, l'ID de terminal pour les numéros de port est défini comme suit :

- **Applications 32 bits** : numéro de port à 4 octets, adresse IP à 4 octets
- **Applications 64 bits** : numéro de port à 8 octets, adresse IP à 4 octets

À partir de la version Solaris 8, l'ID de terminal pour les numéros de port est défini comme suit :

- **Applications 32 bits avec IPv4** : numéro de port à 4 octets, type IP à 4 octets, adresse IP à 4 octets
- **Applications 32 bits avec IPv6** : numéro de port à 4 octets, type IP à 4 octets, adresse IP à 16 octets
- **Applications 64 bits avec IPv4** : numéro de port à 8 octets, type IP à 4 octets, adresse IP à 4 octets
- **Applications 64 bits avec IPv6** : numéro de port à 8 octets, type IP à 4 octets, adresse IP à 16 octets

Le jeton `subject` est toujours retourné dans le cadre des enregistrements d'audit générés par le noyau pour les appels système. La commande `praudit` affiche le jeton `subject` de la manière suivante :

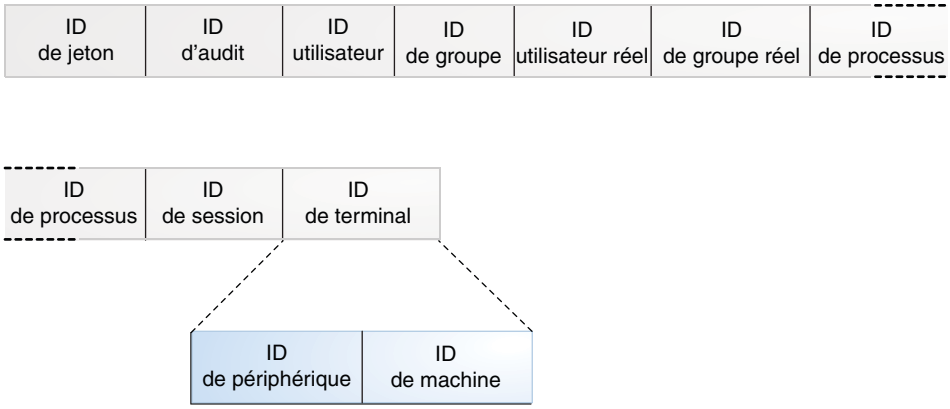
```
subject,jdoe,root,root,root,root,1631,1421584480,8243 65558 machine1
```

La commande `praudit -x` affiche les champs du jeton `subject`. La ligne est renvoyée à des fins d'affichage.

```
<subject audit-uid="jdoe" uid="root" gid="root" ruid="root"
rgid="root" pid="1631" sid="1421584480" tid="8243 65558 machine1"/>
```

La figure suivante illustre le format d'un jeton `subject`.

FIGURE 31–6 Format du jeton `subject`



Jeton `text`

Le jeton `text` contient une chaîne de texte.

Le jeton `text` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `text`
- La longueur de la chaîne de texte
- La chaîne de texte lui-même

La commande `praudit -x` affiche le contenu du jeton `text` :

```
<text>booting kernel</text>
```

Jeton `trailer`

Les deux jetons, `header` et `trailer`, sont spéciaux car ils distinguent les points de fin d'un enregistrement d'audit et entourent tous les autres jetons. Un jeton `header` commence par un enregistrement d'audit. Un jeton `trailer` se termine par un enregistrement d'audit. Le jeton `trailer` est facultatif. Le jeton `trailer` est ajouté en tant que dernier jeton de chaque enregistrement uniquement lorsque l'option de stratégie d'audit `trail` a été définie.

Lorsqu'un enregistrement d'audit est généré avec des blocs de fin activés, la commande `auditreduce` peut vérifier que le bloc de fin pointe correctement vers l'en-tête d'enregistrement. Le jeton `trailer` prend en charge les recherches en arrière dans la piste d'audit.

Le jeton `trailer` a trois champs :

- Un ID de jeton qui identifie ce jeton comme un jeton `trailer`
- Un numéro de pavé destiné à faciliter le marquage de la fin de l'enregistrement
- Le nombre total de caractères dans l'enregistrement d'audit, y compris les jetons `header` et `trailer`

La commande `praudit` affiche le jeton `trailer` comme suit :

```
trailer,136
```

Jeton `uauth`

Le jeton `uauth` enregistre l'utilisation d'autorisation à l'aide d'une commande ou d'une action.

Le jeton `uauth` contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton `uauth`
- La longueur du texte dans le champ suivant
- Une liste d'autorisations

La commande `praudit` affiche le jeton `uauth` de la manière suivante :

```
use of authorization,solaris.admin.printer.delete
```

Jeton `upriv`

Le jeton `upriv` enregistre l'utilisation de privilège à l'aide d'une commande ou d'une action.

La commande `praudit -x` affiche les champs du jeton `upriv` :

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

Jeton `zonename`

Le jeton `zonename` enregistre la zone dans laquelle l'événement d'audit s'est produit. La chaîne "global" indique les événements d'audit qui se produisent dans la zone globale.

Le jeton zonename contient les champs suivants :

- Un ID de jeton qui identifie ce jeton comme un jeton zonename
- La longueur du texte dans le champ suivant
- Le nom de la zone

La commande praudit -x affiche le contenu du jeton zonename :

```
<zone name="graphzone"/>
```

Glossaire

AES Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des États-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 œuvre 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 Dans RBAC, remplace la stratégie de sécurité qui permet à une commande d'administration de s'exécuter correctement lorsque celle-ci est exécutée par un utilisateur autre que le superutilisateur. Dans le modèle de superutilisateur, les programmes `setuid` 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 attributs de sécurité sont les privilèges. Quand un privilège est donné à une commande, celle-ci s'exécute correctement. 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 principal de l'utilisateur, l'adresse IP de l'hôte de l'utilisateur, ainsi qu'un horodatage. À 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 le contrôle d'accès basé sur les rôles (RBAC), 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'actions autrement interdites par la stratégie de sécurité.

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 individuel ou tous les hôtes desservis par un service de nommage, tel que NIS, NIS+ ou LDAP. Les champs d'application sont appliqués aux boîtes à outils de la console de gestion Solaris.

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 cryptographie par clé publique.

clé 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.

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 clé.

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 clé.

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 clé.

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.

code d'authentification des messages (MAC) MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.

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.

consommateur Dans la structure cryptographique 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.

cryptographie par clé publique Modèle de chiffrement où chaque utilisateur dispose de deux clés, l'une publique et l'autre privée. Dans le cas de la cryptographie 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.

DES Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique mise au point en 1975 et normalisée par l'ANSI en 1981 car ANSI X.3.92. DES utilise une clé 56 bits.

domaine 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@ENG.EXAMPLE.COM`, le domaine est `ENG.EXAMPLE.COM`. Voir également nom de principal.

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 Écart maximal toléré entre les horloges système interne 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`.

escalade des privilèges Accès aux ressources situées en dehors de la plage autorisée par les attributs de sécurité qui vous sont attribués, y compris les remplacements. Il en résulte qu'un processus peut effectuer des actions non autorisées.

événement 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. Le démarrage système initial et les événements d'entrée et de sortie PROM sont des exemples d'événements asynchrones.

événement d'audit asynchrone 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, tels que l'échec d'une connexion.

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

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 redémarré pour authentifier automatiquement le KDC avant qu'il ne démarre les processus `kadmind` et `krb5kdc`. Étant 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 une partition d'audit.

fournisseur Dans la structure cryptographique d'Oracle Solaris, service cryptographique 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 consommateur.

fournisseur de logiciel Dans la 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 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 l'unité centrale 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 nommage. 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.

informations d'identification 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.

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. Instance du 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 de 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 esclave.

KDC esclave Copie d'un KDC maître capable de réaliser la plupart des fonctions du maître. Chaque domaine dispose généralement de plusieurs KDC esclave 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 œuvre ce service.

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

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 code d'authentification des messages (MAC).

2. Également 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, l'acronyme de 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.

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

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 structure cryptographique d'OSOL;, mise en œuvre 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 stricte sur un système informatique que le modèle superutilisateur. 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 être en vigueur pour certaines commandes uniquement.

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 faire toutes les activités d'administration.

module de sécurité de base (BSM) Allocation de périphériques et service d'audit d'OSOL;. Ensemble, ces fonctionnalités remplissent les exigences du niveau de sécurité C2.

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

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

NTP Network Time Protocol. Logiciel de l'Université de l'État 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.

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

partition d'audit Partition de disque dur configurée pour stocker les fichiers d'audit.

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

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

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 (par exemple, pour modifier des stratégies) 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 (par exemple, `jdoe` ou `jdoe/admin`). Également 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.

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

profil de droits Également désigné comme un droit ou un profil. Ensemble de remplacements utilisés dans RBAC et pouvant être affectés à un rôle ou un utilisateur. Un profil de droits peut se composer d'autorisations, de privilèges, de commandes avec des attributs de sécurité et d'autres profils de droits.

protocole Diffie-Hellman Également appelé cryptographie par clé publique. Protocole d'accord de clés cryptographique asymétrique 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 (Role-Based Access Control) Alternative au modèle tout ou rien des superutilisateurs. Le RBAC permet à une organisation de diviser les capacités du superutilisateur et de les affecter à des comptes utilisateur spéciaux appelés rôles. Les rôles peuvent être attribués à des individus spécifiques en fonction de leurs responsabilités.

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

rôle Identité spécifique à l'exécution d'applications privilégiées ne pouvant être pris que par des utilisateurs assignés.

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

SEAM Mécanisme d'authentification Sun Enterprise (Sun Enterprise Authentication Mechanism) Nom de produit des versions initiales d'un système d'authentification des utilisateurs d'un réseau, conçu à partir de la technologie Kerberos V5 développée par le Massachusetts Institute of Technology. Le produit est maintenant appelé le service Kerberos. SEAM fait référence à des parties du service Kerberos qui n'ont pas été incluses dans différentes versions de Solaris.

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

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

serveur d'application Voir serveur d'application réseau.

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

service 1. Ressource fournie aux clients du réseau, souvent par plusieurs serveurs. Si, par exemple, vous vous connectez par `rlogin` à la machine `central.example.com`, 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 Algorithme de hachage sécurisé (Secure Hashing Algorithm) 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 RBAC, 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 shells de profil sont `pfsh`, `pfcsh` et `pfksh`. Ils correspondent au shell Bourne (`sh`), au shell C (`csh`) et au shell Korn (`ksh`), respectivement.

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

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 la mise en œuvre des stratégies dans des zones spécifiques du SE Oracle Solaris, voir stratégie d'audit, stratégie dans la structure cryptographique, stratégie de périphériques, stratégie Kerberos, stratégie de mot de passe et stratégie RBAC.

stratégie 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.

stratégie dans la structure cryptographique Dans la structure cryptographique d'Oracle Solaris, la stratégie correspond à la désactivation de mécanismes cryptographiques 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`, à partir d'un fournisseur, par exemple, DES.

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, combien d'entrées de mot de passe erroné sont autorisées 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 MD5, 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 limiter l'utilisation des clés et des certificats qui sont gérés par la bibliothèque KMF.

stratégie RBAC Stratégie de sécurité associé à une commande. Actuellement, `suser` et `solaris` sont des stratégies valides. La stratégie `solaris` reconnaît les privilèges, les autorisations et les attributs de sécurité `setuid`. La stratégie `suser` reconnaît uniquement les attributs de sécurité `setuid`. Les systèmes Trusted Solaris et Trusted Extensions, qui peuvent interagir avec un système Oracle Solaris, fournissent une stratégie `tsol` qui reconnaît les privilèges, les attributs de sécurité `setuid` et les étiquettes sur les processus.

synthèse Voir synthèse de message.

synthèse de message Valeur de hachage calculée à partir d'un message. La valeur de hachage identifie de manière 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, informations d'identification, 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 Étant 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'utilisateur `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 adopter 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.

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 cryptographiques et de mise en tunnel pour connecter les utilisateurs via un réseau public.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

W

X

Y

Z