Gestion de l'audit dans Oracle® Solaris 11.2

Référence: E53972
Juillet 2014

ORACLE®

Table des matières

Utilisation de la présente documentation

Gestion de l'audit dans Oracle® Solaris 11.2 documente la fonction d'audit de Oracle Solaris.

- **Présentation** : décrit l'administration de l'audit sur un système Oracle Solaris ou sur un réseau de systèmes.
- **Public visé** : administrateurs système qui doivent implémenter la sécurité dans l'entreprise.
- **Connaissances requises** : connaissance des concepts et de la terminologie de sécurité.

Bibliothèque de documentation des produits

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

Accès aux services de support Oracle

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

Commentaires

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

♦ ♦ ♦ CHAPITRE 1

A propos de l'audit dans Oracle Solaris

Le sous-système d'audit Oracle Solaris conserve 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:

Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous aux chapitres suivants :

- Chapitre 3, Gestion du service d'audit
- Chapitre 4, Surveillance de l'activité du système
- Chapitre 5, Utilisation des données d'audit
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Nouveautés du service d'audit dans Oracle Solaris

Cette section met en évidence des informations pour les clients existants sur des nouvelles fonctions importantes du service d'audit Oracle Solaris.

- Les enregistrements d'audit d'un système Oracle Solaris peuvent se connecter à Oracle Audit Vault and Database Firewall, qui peut ensuite être utilisé pour obtenir des informations sur les événements ayant fait l'objet d'un audit sur les systèmes Oracle Solaris.

- Deux attributs de package sont définis pour les fichiers de configuration d'audit `audit_class`, `audit_event` et `audit_warn`. L'attribut `preserve=renamenew` permet de modifier les fichiers, et les modifications sont conservées dans les mises à jour et correctifs de package. L'attribut `overlay=allow` permet de remplacer les fichiers par des fichiers de packages créés par un utilisateur.

Définition 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. A chaque connexion, une fois qu'un utilisateur fournit un nom d'utilisateur et que l'authentification PAM réussit, un *ID utilisateur d'audit* unique et immuable est généré et associé à l'utilisateur et 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. Lorsqu'un utilisateur change d'identité, toutes ses actions sont suivies avec le même ID utilisateur d'audit. Pour plus d'informations sur le changement d'identité, reportez-vous à la page de manuel `su`(1M). Par défaut, certaines actions, telles que l'initialisation et la fermeture du système, sont toujours soumises à un audit.

Le service d'audit active les opérations possibles 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

Remarque - Pour des raisons de sécurité, il n'est pas possible d'afficher tous les événements audités tels que les mots de passe modifiés. Pour plus d'informations, reportez-vous à la section “Enregistrements d'audit et jetons d'audit” à la page 15.

Terminologie et concepts de l'audit

Les termes suivants sont utilisés pour décrire le service d'audit. Certaines définitions incluent des pointeurs vers des descriptions plus complètes.

classe d'audit	Regroupement d'événements d'audit. Les classes d'audit permettent de sélectionner un groupe d'événements à auditer. Pour plus d'informations, reportez-vous aux pages de manuel "Classes d'audit et présélection" à la page 14, `audit_flags`(5), `audit_class`(4) et `audit_event`(4).
système de fichiers d'audit	Référentiel de fichiers d'audit au format binaire. Pour plus d'informations, reportez-vous à la section "Journaux d'audit" à la page 17 et à la page de manuel `audit.log`(4).
événement d'audit	Action du système ayant trait à la sécurité et pouvant faire l'objet d'un audit. Pour faciliter la sélection, les événements sont regroupés en classes d'audit. Pour plus d'informations, reportez-vous à la section "Evénements d'audit" à la page 13 et à la page de manuel `audit_event`(4).
indicateur d'audit	Classe d'audit fournie comme argument d'une commande ou d'un mot-clé. Un indicateur peut être précédé d'un signe plus ou moins pour indiquer que la classe fait l'objet d'un audit portant respectivement sur la réussite (+) ou l'échec (-). Un caret (^) précédant indique qu'une réussite ne doit pas faire l'objet d'un audit (^+) ou qu'un échec ne doit pas faire l'objet d'un audit (^-). Pour plus d'informations, reportez-vous à la page de manuel `audit_flags`(5) et à la section "Syntaxe de classe d'audit" à la page 122.
plug-in d'audit	Module transférant les enregistrements d'audit placés dans la file d'attente vers un emplacement spécifié. Le plug-in `audit_binfile` crée des fichiers d'audit binaires. Les fichiers binaires constituent la piste d'audit, qui est stockée sur les systèmes de fichiers d'audit. Le plug-in `audit_remote` envoie les enregistrements d'audit binaires à un référentiel distant. Le plug-in `audit_syslog` récapitule les enregistrements d'audit sélectionnés dans les journaux `syslog`. Pour plus d'informations, reportez-vous à la section "Modules de plug-in d'audit" à la page 16 et aux pages de manuel du module `audit_binfile`(5), `audit_remote`(5) et `audit_syslog`(5).
stratégie d'audit	Ensemble d'options d'audit que vous pouvez activer ou désactiver sur votre site. Vous avez la possibilité d'enregistrer certains types de données d'audit, et d'indiquer si les actions auditables doivent être suspendues ou pas lorsque la file d'attente d'audit est pleine.

Pour plus d'informations, reportez-vous à la section “Principes de la stratégie d'audit” à la page 35 et à la page de manuel `auditconfig`(1M).

enregistrement d'audit
: Données d'audit collectées dans la file d'attente 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, reportez-vous à la section “Enregistrements d'audit et jetons d'audit” à la page 15 et à la page de manuel `audit.log`(4).

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 plus d'informations, reportez-vous à la section “Formats de jeton d'audit” à la page 129 et à la page de manuel `audit.log`(4).

piste d'audit
: Ensemble composé d'un ou de plusieurs fichiers d'audit, stockant les données d'audit de tous les systèmes soumis à l'audit qui exécutent le plug-in par défaut `audit_binfile`.

  Pour plus d'informations, reportez-vous à la section “Piste d'audit” à la page 127.

audit local
: Collecte des enregistrements d'audit générés sur le système local. Les enregistrements peuvent être générés dans la zone globale ou dans des zones non globales, ou les deux.

  Pour plus d'informations, reportez-vous à la section “Modules de plug-in d'audit” à la page 16.

postsélection
: Sélection des événements d'audit à examiner dans la piste d'audit. Le plug-in actif par défaut `audit_binfile` crée 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 aux pages de manuel `auditreduce`(1M) et`praudit`(1M).

présélection
: Sélection des classes d'audit à surveiller. Les événements d'audit des classes d'audit présélectionnées sont recueillis dans la file d'attente d'audit. Les classes d'audit non présélectionnées ne sont pas soumises à l'audit. Les événements correspondants n'apparaissent donc pas dans la file d'attente.

Pour plus d'informations, reportez-vous à la section “Classes d'audit et présélection” à la page 14 et aux pages de manuel `audit_flags`(5) et `auditconfig`(1M).

objet public

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 pas l'objet d'un audit pour les 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 écraser la valeur par défaut en modifiant l'option de stratégie d'audit `public`.

audit à distance

Serveur d'audit à distance (ARS) qui reçoit et stocke les enregistrements d'audit d'un système dont l'audit est en cours et qui est configuré avec un plug-in `audit_remote` actif. Pour différencier un système audité d'un serveur ARS, le système audité peut être appelé le “système audité localement”.

Pour plus d'informations, reportez-vous aux options `-setremote` présentées dans la page de manuel `auditconfig`(1M) et dans la section “Serveur d'audit à distance” à la page 123.

Evénements d'audit

Les événements d'audit représentent les actions pouvant faire l'objet d'un audit sur un système. Les événements d'audit sont répertoriés dans le fichier `/etc/security/audit_event`. Chaque événement d'audit est connecté à un appel système ou une commande utilisateur et est affecté à une ou plusieurs classes d'audit. Pour obtenir une description du format du fichier `audit_event`, reportez-vous à la page de manuel `audit_event`(4).

Par exemple, l'événement d'audit `AUE_EXECVE` soumet à l'audit l'appel système `execve()`. La commande `auditrecord -e execve` affiche cette entrée :

```
# auditrecord -e execve
execve
system call execve              See execve(2)
event ID    23                  AUE_EXECVE
class       ps,ex               (0x0000000040100000)
header
path
[attribute]                 omitted on error
[exec_arguments]            output if argv policy is set
[exec_environment]          output if arge policy is set
subject
[use_of_privilege]
```

`return`

Lorsque vous présélectionnez la classe d'audit `ps` ou `ex`, chaque appel système `execve()` est enregistré dans la file d'attente de l'audit.

L'audit gère les événements *attribuables* et*non attribuables*. La stratégie d'audit répartit les événements en événements *synchrones* et *asynchrones*, comme suit :

- **Evénements attribuables** : événements pouvant être attribués à un utilisateur. L'appel système `execve()` peut être attribué à un utilisateur, de sorte qu'il est considéré comme un événement attribuable. Tous les événements attribuables sont des événements synchrones.
- **Evénements 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 auxquels sont associés des processus, tels qu'un échec de connexion, sont des événements synchrones.
- **Evénements synchrones** : événements associés à un processus dans le système. Les événements synchrones constituent la majorité des événements système.
- **Evénements asynchrones** : événements associés à aucun processus, de sorte qu'aucun processus ne peut être bloqué puis réactivé ultérieurement. L'initialisation système initiale et les événements d'entrée et de sortie PROM sont des exemples d'événements asynchrones.

Outre les événements d'audit définis par le service d'audit, 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. Les fournisseurs doivent contacter leur représentant Oracle Solaris pour réserver des numéros d'événements et obtenir l'accès aux interfaces d'audit.

Classes d'audit et présélection

Chaque événement d'audit appartient à une *classe d'audit*. Les classes d'audit sont des conteneurs pratiques pour les grands nombres d'événements d'audit. Lorsque vous *présélectionnez* une classe pour la soumettre à un audit, tous les événements de cette classe sont enregistrés dans la file d'attente de l'audit. Par exemple, lorsque vous présélectionnez la classe d'audit `ps`, les appels système `execve()`, `fork()` et autres sont enregistrés.

Vous pouvez effectuer une présélection pour des événements sur un système et pour des événements initiés par un utilisateur particulier.

- **Présélection à l'échelle du système :** spécifiez les paramètres d'audit par défaut du système à l'aide des options `-setflags` et `-setnaflags` de la commande `auditconfig`.

Remarque - Si la stratégie `perzone` est définie, les classes d'audit par défaut peuvent être spécifiées dans chaque zone. Pour l'audit `perzone`, les paramètres par défaut sont à l'échelle d'une zone, et non à l'échelle du système.

- **Présélection spécifique à l'utilisateur :** spécifiez les différences par rapport aux paramètres d'audit par défaut du système en configurant les indicateurs d'audit spécifiques à l'utilisateur concerné. Les commandes `useradd`, `roleadd`, `usermod` et `rolemod` placent l'attribut de sécurité `audit_flags` dans la base de données `user_attr`. La commande `profiles` place les indicateurs d'audit pour les profils de droits dans la base de données `prof_attr`.

  Le masque de présélection d'audit détermine les classes d'événements auditées pour un utilisateur. Pour obtenir une description du masque de présélection utilisateur, reportez-vous à la section “Caractéristiques de l'audit de processus” à la page 126. Pour les indicateurs d'audit configurés utilisés, reportez-vous à la section “ Ordre de recherche pour Assigned Rights ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

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 `lo` et `ps` s'affichent dans le fichier `audit_class` comme suit :

```
0x0000000000001000:lo:login or logout
0x0000000000100000:ps:process start/stop
```

Les classes d'audit comprennent les deux classes globales : `all` et `no`. Les classes d'audit sont décrites à la page de manuel `audit_class`(4). Pour obtenir la liste des classes, consultez le fichier `/etc/security/audit_class`.

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 connaître la procédure, reportez-vous à la section “Modification de l'appartenance à une classe d'un événement d'audit” à la page 58. Pour afficher les événements associés à une classe, utilisez la commande `auditrecord -c` *class*.

Enregistrements d'audit et jetons d'audit

Chaque*enregistrement d'audit* enregistre 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` avec trois jetons, `header`, `subject` et `return` :

```
header,69,2,login - local,,example_system,2010-10-10 10:10:10.020 -07:00
```

```
subject,jdoe,jdoe,staff,jdoe,staff,1210,4076076536,69 2 example_system
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 du jeton. Ensemble, les jetons d'audit `header`, `subject` et `return` constituent l'enregistrement d'audit `login - local`. Pour afficher les jetons qui constituent un enregistrement d'audit, utilisez la commande `auditrecord -e` *event*.

Remarque - Les fichiers comportant l'attribut système`sensitive` n'ont pas leur contenu ou modifications de contenu inclus dans l'enregistrement d'audit. L'attribut permet de s'assurer qu'aucune des informations sensibles dans des fichiers spécifiques, telles que les mots de passe, les codes PIN, les clés, etc., n'est accessible à qui que ce soit. Pour plus d'informations, reportez-vous à la page de manuel `pfedit`(1M).

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 129.
Pour une description du flux binaire des jetons d'audit, reportez-vous à la page de manuel `audit.log`(4).

Modules de plug-in d'audit

Les modules du plug-in d'audit dirigent les enregistrements d'audit de la file d'attente d'audit vers un fichier ou un référentiel. Au moins un plug-in doit être actif. Par défaut, le plug-in `audit_binfile` est actif. Vous pouvez configurer les plug-ins à l'aide de la commande `auditconfig -setplugin`*plug-in-name* .

Le service d'audit fournit les plug-ins suivants :

- Plug-in `audit_binfile` : gère la distribution de la file d'attente d'audit aux fichiers d'audit binaires. Pour plus d'informations, reportez-vous à la page de manuel `audit.log`(4).
- Plug-in `audit_remote` : gère la distribution des enregistrements d'audit binaires de la file d'attente d'audit au serveur distant configuré. Le plug-in `audit_remote` utilise la bibliothèque `libgss()` pour authentifier le serveur. La transmission est protégée en matière de confidentialité et d'intégrité.
- Plug-in `audit_syslog` : gère la distribution des enregistrements sélectionnés de la file d'attente d'audit aux journaux `syslog`.

Pour plus d'informations sur la configuration d'un plug-in , reportez-vous à la page de manuel `auditconfig`(1M). Pour consulter des exemples de configuration de plug-in, reportez-vous

aux tâches décrites dans la section “Configuration des journaux d'audit” à la page 77.
Pour plus d'informations sur les plug-ins, reportez aux pages de manuel `audit_binfile`(5), `audit_remote`(5) et`audit_syslog`(5).

Journaux d'audit

Les enregistrements d'audit sont collectés dans des journaux d'audit. Le service d'audit propose trois modes de sortie pour les enregistrements 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*. Ces journaux sont créés par le plug-in `audit_binfile` et peuvent être révisés par les commandes de postsélection `praudit` et `auditreduce`.
- Le plug-in `audit_remote` diffuse les enregistrements d'audit à un référentiel distant. Le référentiel est chargé de tenir à jour une piste d'audit et de fournir les outils de postsélection.
- L'utilitaire `syslog` collecte et stocke des résumés d'enregistrements d'audit au format texte. Un enregistrement `syslog` n'est pas complet. L'exemple suivant montre une entrée `syslog` pour un d'enregistrement d'audit `login` :

```
Oct 10  10:10:20 example_system auditd: [ID 6472 audit.notice] \
login - login ok session 4076172534 by root as root:other
```

Un site peut configurer l'audit de façon à collecter les enregistrements d'audit à tous les formats. Vous pouvez configurer les systèmes de votre site de manière à ce qu'ils utilisent le mode binaire localement, qu'ils envoient les fichiers binaires à un référentiel distant et qu'ils utilisent le mode `syslog`. Le tableau suivant compare les enregistrements d'audit binaires aux enregistrements d'audit `syslog`.

TABLEAU 1-1 Comparaison des enregistrements d'audit binaires, distants et `syslog`

Caractéristique	Enregistrements binaires et distants	Enregistrements `syslog`
Protocole	Binaire : écrit dans le système de fichiers Distant : diffuse vers un référentiel distant	Utilise UDP pour la connexion à distance
Type de données	Binaire	Texte
Longueur d'enregistrement	Aucune limite	Jusqu'à 1024 caractères par enregistrement d'audit
Emplacement	Binaire : stocké dans un `zpool` sur le système Distant : référentiel distant	Stockés dans un emplacement spécifié dans le fichier `syslog.conf`
Configuration	Binaire : définir l'attribut `p_dir` sur le plug-in `audit_binfile`. Distant : définir l'attribut `p_hosts` sur le plug-in `audit_remote` et activer le plug-in.	Activer le plug-in `audit_syslog` et configurer le fichier `syslog.conf`

Caractéristique	Enregistrements binaires et distants	Enregistrements `syslog`
Lecture	Binaire : en général, en mode batch, sortie navigateur au format XML	En temps réel ou recherché par des scripts que vous avez créés pour `syslog`
	Distant : le référentiel dicte la procédure	Sortie en texte brut
Exhaustivité	Exhaustivité garantie et affichage dans l'ordre approprié	Exhaustivité non garantie
Horodatage	Temps universel (UTC)	Heure du système audité

Pour plus d'informations sur les plug-ins et les journaux d'audit, reportez-vous à :

- Page de manuel `audit_binfile`(5)
- Page de manuel `audit_syslog`(5)
- Page de manuel `audit.log`(4)
- “Affectation de l'espace d'audit pour la piste d'audit” à la page 82
- “Configuration des journaux d'audit `syslog`” à la page 91

A propos des enregistrements binaires

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 exigences d'audit Critères communs (http://www.commoncriteriaportal.org/).

Le plug-in `audit_binfile` écrit les enregistrements 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 UTC dans les journaux binaires permet une comparaison exacte lorsque des systèmes d'une piste d'audit sont répartis sur 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.

Le plug-in `audit_remote` écrit les enregistrements d'audit dans un référentiel distant. Le référentiel gère le stockage et la postsélection.

A propos des enregistrements d'audit `syslog`

En revanche, les enregistrements `syslog` peuvent offrir 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. Pensez néanmoins à fournir les inconvénients suivants pour le mode `syslog`.

- 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, le protocole UDP peut déposer des paquets ou les distribuer dans le désordre.
- La limite de 1024 caractères autorisés pour les entrées `syslog` peut faire que des enregistrements d'audit soient tronqués dans le journal.
- Sur un système unique, tous les enregistrements d'audit ne sont pas collectés et peuvent ne pas être affichés dans l'ordre.
- Chaque enregistrement d'audit est indiqué avec la date et l'heure du système local. Par conséquent, vous ne pouvez pas vous fier à l'horodatage pour créer une piste d'audit pour plusieurs systèmes.

Stockage et gestion de la piste d'audit

Lorsque le plug-in `audit_binfile` est actif, un *système de fichiers d'audit* maintient les fichiers d'audit au format binaire. L'installation standard utilise le système de fichiers `/var/audit` et peut utiliser des systèmes de fichiers supplémentaires. Le contenu de tous les systèmes de fichiers d'audit constitue la *piste d'audit*. Les enregistrements d'audit sont stockés dans ces systèmes de fichiers d'audit selon l'ordre suivant :

- **Système de fichiers d'audit principal :** système de fichiers `/var/audit`, système de fichiers par défaut pour les fichiers d'audit d'un système
- **Systèmes de fichiers d'audit secondaires** : systèmes de fichiers dans lesquels les fichiers d'audit d'un système sont placés à la discrétion de l'administrateur

Les systèmes de fichiers sont spécifiés en tant qu'arguments de l'attribut `p_dir` du plug-in `audit_binfile`. Un système de fichiers n'est pas utilisé tant qu'un système de fichiers occupant une position supérieure dans la liste n'est pas saturé. Pour obtenir un exemple de liste d'entrées de système de fichiers, reportez-vous à la section “Création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 78.

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 `/var/audit`.

Vous pouvez utiliser les options suivantes à l'aide de la commande `auditreduce` :

- L'option-M de la commande auditreduce peut être utilisée pour spécifier des fichiers d'audit à partir d'un ordinateur spécifique.
- L'option-S peut être utilisée pour spécifier un autre système de fichiers d'audit.

Pour consulter des exemples d'utilisation de la commande auditreduce, reportez-vous à la section “Fusion des fichiers d'audit de la piste d'audit” à la page 104. Pour plus d'informations, reportez-vous à la page de manuel auditreduce(1M).

Le service d'audit fournit des commandes pour combiner et filtrer 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.

Garantie de la fiabilité de l'horodatage

Lorsque vous fusionnez les journaux d'audit de plusieurs systèmes, il est impératif que la date et l'heure sur ces systèmes soient exactes. De même, lorsque vous envoyez les journaux d'audit à un système distant, le système d'enregistrement et le système de référentiel doivent disposer d'horloges précises. Le protocole NTP (Network Time Protocol) assure la précision et la coordination des horloges système. Pour plus d'informations, reportez-vous au Chapitre 3, “ Services d’horodatage ” du manuel “ Introduction aux services réseau d’Oracle Solaris 11.2 ” et à la page de manuel xntpd (1M).

Gestion d'un référentiel distant

Une fois le plug-in audit_remote configuré, un référentiel distant reçoit les enregistrements d'audit. Le serveur ARS fournit un récepteur pour les enregistrements d'audit. Les enregistrements d'audit sont envoyés au serveur ARS par le biais d'une connexion protégée et peuvent être stockés de la même manière qu'ils sont stockés localement. Pour configurer un serveur ARS, reportez-vous à la section “Configuration d'un référentiel distant pour les fichiers d'audit” à la page 87. Pour une description du serveur ARS, reportez-vous à la section “Serveur d'audit à distance” à la page 123 et à la page de manuel ars(5).

Rapports entre l'audit et la sécurité

L'audit permet de détecter des violations de sécurité potentielles en révélant des modèles suspects ou anormaux d'utilisation du système. L'audit 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.

Il est conseillé de définir les paramètres d'audit S avant la connexion des utilisateurs ou le démarrage des processus système, car la plupart des activités d'audit impliquent la surveillance des événements en cours et la signalisation des événements qui répondent aux paramètres spécifiés. La manière dont l'audit surveille les événements et génère des rapports est traitée en détail dans les Chapitre 2, Planification de l'audit et Chapitre 3, Gestion du service d'audit.

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.

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 de droits
- 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

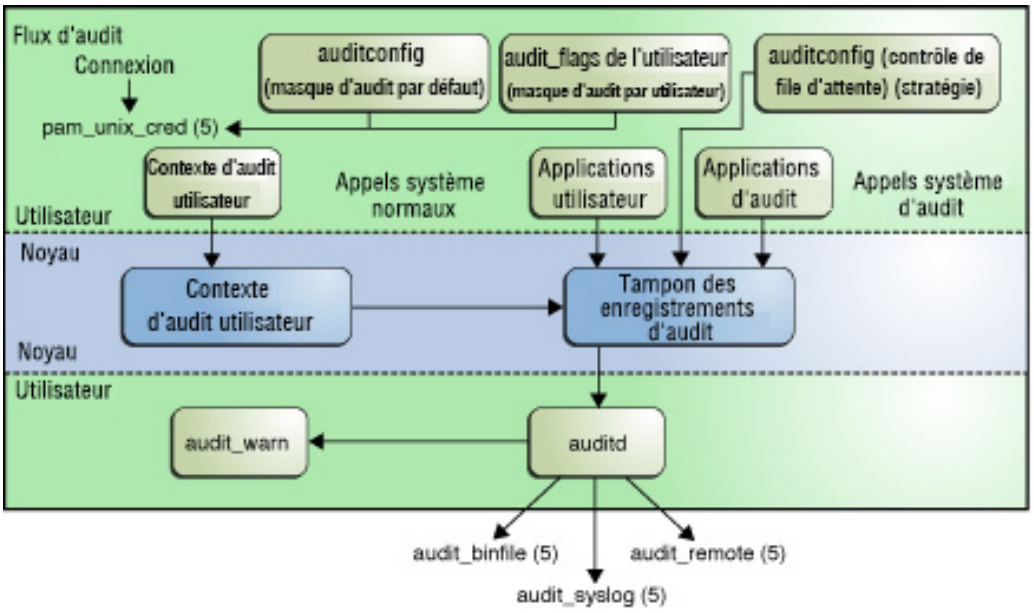
- A la suite d'un événement d'audit asynchrone
- A la suite d'un appel système de processus

Une fois recueillies, les informations pertinentes d'événement prennent la forme d'un enregistrement d'audit. Chaque enregistrement d'audit contient des informations qui identifient l'événement, la cause, l'heure et d'autres informations pertinentes. Cet enregistrement est ensuite placé dans une file d'attente d'audit et envoyé aux *plug-ins* actifs pour le stockage. Au moins un plug-in doit être actif, bien que tous puissent l'être. Les plug-ins sont décrits dans les sections “Configuration de l'audit” à la page 22 et “Modules de plug-in d'audit” à la page 16.

Configuration de l'audit

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 dans Oracle Solaris.

FIGURE 1-1 Flux d'audit



Une fois les données d'audit collectées dans le noyau, les plug-ins distribuent les données aux emplacements appropriés.

- Le plug-in `audit_binfile` place les enregistrements d'audit binaires dans le système de fichiers `/var/audit`. Par défaut, le plug-in `audit_binfile` est actif. Les outils de postsélection vous permettent d'examiner des parties intéressantes de la piste d'audit.

  Les fichiers d'audit peuvent être stockés dans un ou plusieurs pools ZFS. Ils peuvent résider sur différents systèmes et sur des réseaux différents mais liés. L'ensemble des fichiers d'audit liés est considéré comme une *piste d'audit*.
- Le plug-in `audit_remote` envoie les enregistrements d'audit binaires à un référentiel distant par le biais d'un lien protégé.
- Le plug-in `audit_syslog` envoie des résumés au format texte d'enregistrements d'audit à l'utilitaire `syslog`.

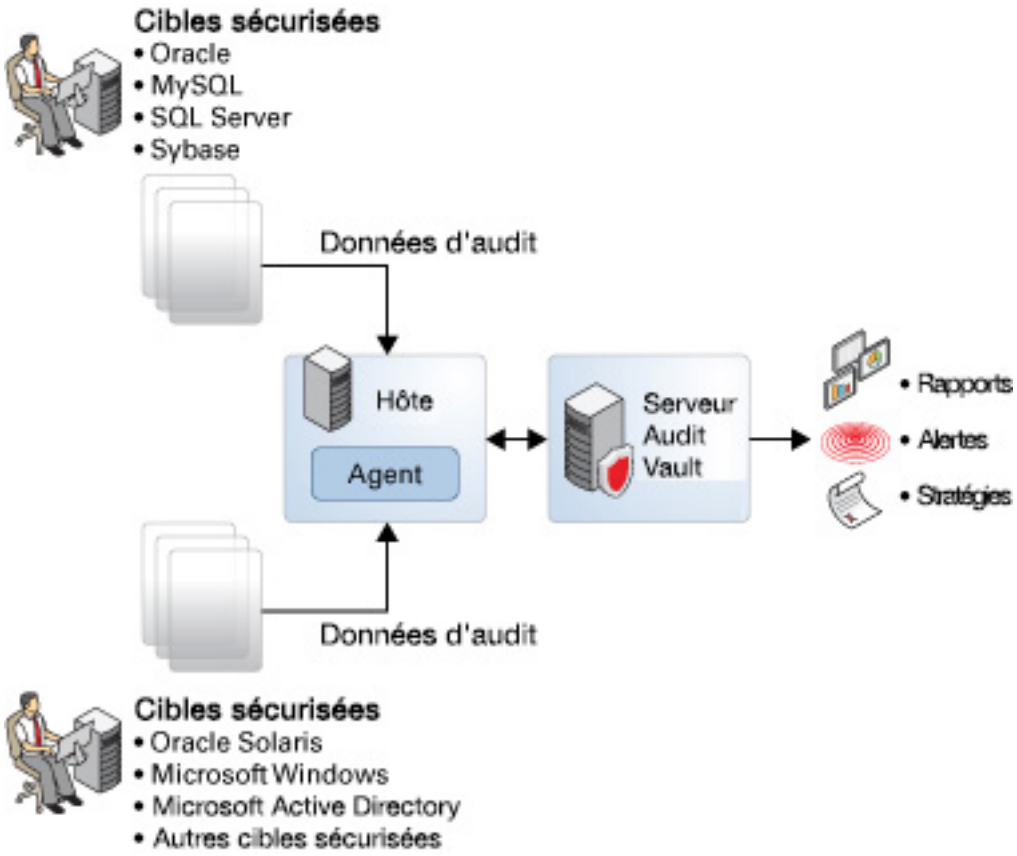
Les systèmes qui installent des zones non globales peuvent auditer toutes les zones de la même façon que la zone globale. Ces systèmes peuvent également être configurés pour collecter différents enregistrements dans les zones non globales. Pour plus d'informations, reportez-vous à la section “Audit et Oracle Solaris Zones” à la page 121.

Utilisation du coffre d'audit Oracle et du pare-feu de base de données pour le stockage et l'analyse des enregistrements d'audit

Les enregistrements d'audit d'un système Oracle Solaris peuvent se connecter à Oracle Audit Vault and Database Firewall, version 12.1.0.0. Oracle Audit Vault and Database Firewall automatise la consolidation et la surveillance des données d'audit à partir des bases de données Oracle et autres. Oracle Audit Vault and Database Firewall peut alors être utilisé pour l'analyse et des rapports d'événements d'audit sur les systèmes Oracle Solaris. Pour plus d'informations, reportez-vous à la section Oracle Audit Vault and Database Firewall (http://www.oracle.com/technetwork/products/audit-vault/overview/index.html).

L'image suivante illustre comment Oracle Audit Vault and Database Firewall collecte des enregistrements d'audit Oracle Solaris à partir de cibles sécurisées désignées. Une cible sécurisée est un système qui stocke les enregistrements d'audit ou les données.

FIGURE 1-2 Oracle Solaris and Audit Vault



Un hôte est désigné pour exécuter l'agent AV qui communique avec Oracle Audit Vault and Database Firewall. L'agent active Oracle Audit Vault and Database Firewall pour recevoir et traiter les données d'audit de cibles sécurisées. L'agent lit les enregistrements d'audit à partir d'une piste d'audit désignée sur la cible sécurisée. Ces enregistrements d'audit sont codés au format binaire d'origine. L'agent convertit les données à un format analysable par Oracle Audit Vault and Database Firewall. Oracle Audit Vault and Database Firewall reçoit les données et génère des rapports pour les administrateurs et les responsables de la sécurité si besoin.

L'agent peut être installé sur une cible sécurisée à la place d'un hôte ou système distinct. Plusieurs hôtes avec agents peuvent également être configurés pour se connecter au serveur Audit Vault. Indiquez toutefois, lors de l'enregistrement de cibles sécurisées, un hôte spécifique avec lequel le serveur AV communique pour obtenir les données d'audit.

Pour configurer Oracle Audit Vault and Database Firewall de façon à ce qu'il accepte les enregistrements d'audit des cibles sécurisées Oracle Solaris et autres, assurez-vous que l'agent est installé et activé sur le système hôte désigné. Pour plus d'informations à ce sujet, reportez-vous à la documentation Oracle Audit Vault and Database Firewall (http://www.oracle.com/technetwork/products/audit-vault/documentation/index.html).

Audit sur un système avec Oracle Solaris Zones

Une zone non globale représente un environnement virtualisé du système d'exploitation, créé dans une seule instance du Oracle Solaris (SE). 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 exécuter 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 noms personnalisé.

  Si toutes les zones d'un système se trouvent à l'intérieur d'un domaine d'administration, la stratégie d'audit `zonename` permet de distinguer les événements d'audit configurés 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 noms 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 per-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. Chaque administrateur de zone est tenu d'administrer l'audit. Chaque zone exécute son propre démon d'audit et possède sa propre file d'attente d'audit et ses journaux d'audit. Ces journaux d'audit doivent être gérés.

♦ ♦ ♦ CHAPITRE 2

Planification de l'audit

Ce chapitre décrit la procédure de planification de la personnalisation du service d'audit pour votre installation Oracle Solaris :

Pour une présentation de l'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous aux chapitres suivants :

- Chapitre 3, Gestion du service d'audit
- Chapitre 4, Surveillance de l'activité du système
- Chapitre 5, Utilisation des données d'audit
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Concepts de planification de l'audit

Vous voulez sélectionner avec soin les types d'activités auditées. Dans le même temps, vous voulez collecter des informations d'audit utiles. Vous devez également planifier soigneusement les utilisateurs et objets audités. Si vous utilisez le plug-in `audit_binfile` par défaut, 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.

Planification d'une piste d'audit de système unique

Remarque - L'implémentation d'une piste d'audit de système unique s'applique uniquement au plug-in `audit_binfile`.

Des systèmes au sein d'un même domaine administratif peuvent créer une piste d'audit d'image système unique.

Pour créer une piste d'audit d'image système unique pour un site, procédez comme suit :

- Utilisez le même service de noms pour tous les systèmes.

  Pour une interprétation correcte des enregistrements d'audit, les fichiers `passwd`, `group` et `hosts` doivent être cohérents.
- Configurez un service d'audit identique sur tous les systèmes. Pour des informations sur l'affichage et la modification des paramètres du service, reportez-vous à la page de manuel `auditconfig`(1M).
- Utilisez les mêmes fichiers `audit_warn`, `audit_event` et `audit_class` pour tous les systèmes.

Reportez-vous à la section “Planification des personnes et objets à auditer” à la page 30 pour des informations supplémentaires sur l'activation de l'audit sur les systèmes.

Planification de l'audit dans les zones

Si votre système comporte des zones non globales, elles peuvent être auditées simultanément avec la zone globale ou bien vous pouvez configurer, activer et désactiver le service d'audit de chaque zone non globale séparément. Par exemple, vous êtes libre de soumettre à l'audit uniquement les zones non globales, pas la zone globale.

Pour une description des compromis, reportez-vous à la section “Audit sur un système avec Oracle Solaris Zones” à la page 25.

Les options suivantes sont disponibles lors de l'implémentation de l'audit dans les zones.

Implémentation 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 est créée lorsque vous utilisez le plug-in `audit_binfile` ou `audit_remote` et que 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 l'unique service d'audit sur un système et recueille les enregistrements d'audit pour chaque zone. Vous pouvez personnaliser les fichiers `audit_class` et `audit_event` uniquement dans la zone globale, puis copier ces fichiers dans chaque zone non globale.

Vous devez respecter les conditions suivantes lors de la configuration d'un service d'audit pour l'ensemble des zones.

- Utilisez le même service de noms pour chaque zone.

Remarque - Si les fichiers du service de noms sont personnalisés dans des zones non globales, et si 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.

- Activez les enregistrements d'audit pour inclure le nom de la zone.

  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 consulter 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 “Planification des personnes et objets à auditer” à la page 30. Commencez à la première étape. L'administrateur de la zone globale doit également réserver du stockage, comme décrit dans la section “Planification de l'espace disque pour les enregistrements d'audit” à la page 33.

Implémentation d'un service d'audit par zone

Sélectionnez l'option de configuration d'audit par zone si différentes zones utilisent différentes bases de données de service de noms ou si les administrateurs de zone souhaitent contrôler l'audit dans leurs zones.

Remarque - Pour auditer les zones non globales, la stratégie `perzone` doit être définie, mais il n'est pas nécessaire que le service d'audit soit activé dans la zone globale. L'audit de la zone non globale est configuré, et son service d'audit est activé et désactivé séparément de la zone globale.

- Lors de la configuration de l'audit par zone, vous configurez la stratégie d'audit `perzone` dans la zone globale. Si une zone non globale n'a pas encore été initialisée au moment de la définition de l'audit par zone, son audit commence à son initialisation initiale. Pour définir la stratégie d'audit, reportez-vous à la section “Configuration de l'audit par zone” à la page 72.

- Chaque administrateur configure l'audit de la zone qu'il gère.

  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.
- Pour générer des enregistrements qui peuvent être retracés jusqu'à leur zone d'origine lors de la révision, définissez la stratégie d'audit `zonename`.

Remarque - Dans l'audit perzone, si le plug-in `audit_binfile` est actif, chaque administrateur de zones doit également réserver du stockage pour chaque zone, comme décrit dans la section “Planification de l'espace disque pour les enregistrements d'audit” à la page 33. Pour les tâches complémentaires de planification, reportez-vous à la section “Planification des personnes et objets à auditer” à la page 30.

Planification de l'audit

La liste suivante présente les principales tâches à effectuer pour planifier l'espace disque et définir les événements à enregistrer.

TABLEAU 2-1 Liste des tâches de la planification de l'audit

Tâche	Pour obtenir des instructions
Détermination des personnes et objets à auditer	“Planification des personnes et objets à auditer” à la page 30
Planification de l'espace de stockage pour la piste d'audit	“Planification de l'espace disque pour les enregistrements d'audit” à la page 33
Planification de la transmission d'une piste d'audit à un serveur distant	“Préparation de la diffusion des enregistrements d'audit vers le stockage distant” à la page 34

▼ Planification des personnes et objets à auditer

Avant de commencer Si vous implémentez des zones non globales, consultez la section “Planification de l'audit dans les zones” à la page 28 avant d'utiliser cette procédure.

1. **Déterminez la stratégie d'audit.**

   Par défaut, seule la stratégie `cnt` est activée.

   Utilisez la commande `auditconfig -lspolicy` pour afficher une description des options de stratégie disponibles.

   - Pour connaître les effets des options de stratégie, reportez-vous à la section “Principes de la stratégie d'audit” à la page 35.

- Pour connaître l'effet de la stratégie `cnt`, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones” à la page 125.
- Pour définir la stratégie d'audit, reportez-vous à la section “Modification de la stratégie d'audit” à la page 51.

2. **Déterminez si vous souhaitez modifier les mappages des événements aux classes.**

   Dans la majorité des 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, il est conseillé de modifier les mappages entre les événements et les classes.

   La section “Modification de l'appartenance à une classe d'un événement d'audit” à la page 58 présente un exemple.

3. **Déterminez les classes d'audit à présélectionner.**

   Le meilleur moment pour ajouter des classes d'audit ou modifier des classes par défaut est avant la connexion des utilisateurs au système.

   Les classes d'audit que vous présélectionnez avec les options `-setflags` et `- setnaflags` pour la commande `auditconfig` s'appliquent à tous les utilisateurs et processus. Vous pouvez présélectionner une classe pour la réussite, l'échec ou les deux.

   Pour obtenir la liste des classes d'audit, lisez le fichier `/etc/security/audit_class`.

4. **Déterminez les modifications utilisateur à apporter aux présélections à l'échelle du système.**

   Si vous décidez que certains utilisateurs doivent faire l'objet d'un audit différent de celui du système, vous pouvez modifier l'attribut de sécurité `audit_flags` pour des utilisateurs individuels ou un profil de droits. Le masque de présélection utilisateur est modifié pour les utilisateurs dont les indicateurs d'audit sont définis de manière explicite ou auxquels est affecté un profil de droits avec des indicateurs d'audit explicites.

   Pour obtenir cette procédure, reportez-vous à la section “Configuration des caractéristiques d'audit d'un utilisateur” à la page 47. Pour connaître les valeurs d'indicateur d'audit en vigueur, reportez-vous à la section “ Ordre de recherche pour Assigned Rights ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

5. **Déterminez la façon de gérer les alias de messagerie `audit_warn`.**

   Le script `audit_warn` est exécuté chaque fois que le système d'audit détecte 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 56.

6. **Décidez du format et de l'emplacement de collecte des enregistrements d'audit.**

Vous disposez de trois possibilités.

- Par défaut, stockez les enregistrements d'audit binaire localement. Le répertoire par défaut de stockage est `/var/audit`. Pour continuer à configurer le plug-in `audit_binfile`, reportez-vous à la section “Création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 78.
- Diffusez les enregistrements d'audit binaires vers un référentiel protégé distant à l'aide du plug-in `audit_remote`. Vous devez disposer d'un récepteur pour les enregistrements. Pour la configuration requise, reportez-vous à la section “Gestion d'un référentiel distant” à la page 20. Pour obtenir cette procédure, reportez-vous à la section “Envoi des fichiers d'audit à un référentiel distant” à la page 85.
- Envoyez les résumés d'enregistrement d'audit à `syslog` à l'aide du plug-in `audit_syslog`. Pour obtenir cette procédure, reportez-vous à la section “Configuration des journaux d'audit `syslog`” à la page 91.

  Pour obtenir une comparaison des formats binaire et `syslog`, reportez-vous à la section “Journaux d'audit” à la page 17.

7. Déterminez à quel moment avertir l'administrateur de la réduction de l'espace disque.

Remarque - Cette étape s'applique uniquement au plug-in `audit_binfile`.

Lorsque l'espace disque disponible sur un système de fichiers d'audit passe en dessous du pourcentage d'espace libre minimal, ou limite dépassable, le service d'audit bascule vers le répertoire d'audit disponible suivant. Le service envoie alors un message d'avertissement indiquant que cette limite a été dépassée.

Pour savoir comment régler un pourcentage d'espace libre minimal, voir l'Exemple 4-7, “Définition d'une limite dépassable pour les avertissements”.

8. Déterminez la mesure à prendre lorsque tous les répertoires d'audit sont pleins.

Remarque - Cette étape s'applique uniquement au plug-in `audit_binfile`.

Dans la configuration par défaut, le plug-in `audit_binfile` est actif et la stratégie `cnt` est définie. Dans cette configuration, lorsque la file d'attente d'audit du noyau est saturée, le système continue à 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.

Toutefois, si la file d'attente `audit_binfile` est complète alors que la file d'attente d'un autre plug-in actif ne l'est pas, la file d'attente du noyau continue à envoyer des enregistrements vers le plug-in qui n'est pas complet. Lorsque la file d'attente `audit_binfile` peut accepter à nouveau des enregistrements, le service d'audit recommence à lui envoyer des enregistrements.

Pour une description des options de stratégie `cnt` et `ahlt`, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones” à la page 125. Pour savoir comment configurer ces options de stratégie, voir l'Exemple 3-10, “Définition de l'option de stratégie d'audit `ahlt`”.

Remarque - La stratégie `cnt` ou `ahlt` n'est pas déclenchée si la file d'attente d'au moins un plug-in accepte des enregistrements d'audit.

Planification de l'espace disque pour les enregistrements d'audit

Le plug-in `audit_binfile` crée une piste d'audit. La piste d'audit requiert un espace de fichiers dédié. Cet espace doit être disponible et sécurisé. Le système utilise le système de fichiers `/var/audit` pour le stockage initial. Vous êtes libre de configurer d'autres systèmes de fichiers d'audit pour les fichiers d'audit. La procédure suivante décrit les problèmes à résoudre lorsque vous planifiez le stockage de la piste d'audit.

▼ Planification de l'espace disque pour les enregistrements d'audit

Avant de commencer

Si vous implémentez des zones non globales, suivez “Planification de l'audit dans les zones” à la page 28 avant d'utiliser cette procédure.

Cette procédure suppose que vous utilisez le plug-in `audit_binfile`.

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 38 et “Gestion efficace de l'audit” à la page 40.

   Pour connaître les étapes à suivre, reportez-vous aux sections “Le volume des enregistrements d'audit est important” à la page 112, “Compression des fichiers d'audit sur un système de fichiers dédié” à la page 66 etExemple 5-4, “Association et réduction des fichiers d'audit”.

2. **Déterminez les systèmes à soumettre à l'audit et configurez leurs systèmes de fichiers d'audit.**

   Créez une liste de tous les systèmes de fichiers que vous prévoyez d'utiliser. Pour obtenir des instructions sur la configuration, reportez-vous à la section “Stockage et gestion de la piste

d'audit” à la page 19 et à la page de manuel `auditreduce`(1M). Pour spécifier les systèmes de fichiers d'audit, reportez-vous à la section “Affectation de l'espace d'audit pour la piste d'audit” à la page 82.

3. **Synchronisez les horloges de tous les systèmes.**

   Pour plus d'informations, reportez-vous à la section “Garantie de la fiabilité de l'horodatage” à la page 20.

Préparation de la diffusion des enregistrements d'audit vers le stockage distant

Le plug-in `audit_remote` envoie la piste d'audit binaire à un serveur ARS dans le même format que celui utilisé par le plug-in `audit_binfile` pour écrire dans les fichiers d'audit locaux. Le plug-in `audit_remote` utilise la bibliothèque `libgss` pour authentifier le serveur ARS, et un mécanisme GSS-API pour assurer la confidentialité et l'intégrité de la transmission. Pour obtenir des informations de référence, reportez-vous à la section “ Description du service Kerberos ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ” et à la section“ Utilitaires Kerberos ” du manuel “ Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.2 ”.

Le seul mécanisme GSS-API actuellement pris en charge est `kerberosv5`. Pour plus d'informations, reportez-vous à la page de manuel `mech`(4).

▼ Préparation de la diffusion des enregistrements d'audit vers le stockage distant

Remarque - Si vous disposez d'un domaine Kerberos configuré avec un serveur ARS identifié et de tous les systèmes audités au sein du domaine, vous pouvez ignorer cette procédure. Les procédures de configuration du serveur ARS et des systèmes audités sont décrites dans les sections “Configuration d'un référentiel distant pour les fichiers d'audit” à la page 87 et “Envoi des fichiers d'audit à un référentiel distant” à la page 85.

Pour vérifier si un domaine utilisant le protocole Kerberos est configuré, émettez la commande suivante. L'exemple de sortie indique que Kerberos n'est pas installé sur le système.

```
# pkg info system/security/kerberos-5
pkg: info: no packages matching these patterns are installed on the system.
```

Avant de commencer Cette procédure suppose que vous utilisez le plug-in `audit_remote`.

1. **Installez le package KDC (Key Distribution Center) maître.**
   Vous pouvez utiliser le système qui servira de serveur ARS, ou utiliser un système situé à proximité. Le serveur ARS envoie un volume considérable de trafic d'authentification au package KDC principal.

   ```
   # pkg install pkg:/system/security/kerberos-5
   ```

   Sur le KDC maître, vous devez utiliser les commandes `kdcmgr` et `kadmin` Kerberos pour gérer le domaine. Pour plus d'informations, reportez-vous aux pages de manuel `kdcmgr`(1M) et `kadmin`(1M).

2. **Sur chaque système audité qui envoie des enregistrements d'audit au serveur ARS, installez le package KDC maître.**

   ```
   # pkg install pkg:/system/security/kerberos-5
   ```

   Ce package inclut la commande `kclient`. Sur ces systèmes, vous devez exécuter la commande `kclient` pour vous connecter au package KDC. Pour plus d'informations, reportez-vous à la page de manuel `kclient`(1M).

3. **Synchronisez les horloges avec le domaine KDC.**
   Si l'écart d'horloge est trop grand entre les systèmes audités et le serveur ARS, la tentative de connexion échoue. Une fois la connexion établie, l'heure locale du serveur ARS détermine les noms des fichiers d'audit stockés, comme décrit à la section “Conventions relatives aux noms de fichiers d'audit binaires” à la page 127.
   Pour plus d'informations sur les horloges, reportez-vous à la section “Garantie de la fiabilité de l'horodatage” à la page 20.

Principes de la stratégie d'audit

La stratégie d'audit détermine les caractéristiques des enregistrements d'audit pour le système local. Vous utilisez la commande `auditconfig` pour définir ces stratégies. Pour plus d'informations, reportez-vous à la page de manuel `auditconfig`(1M).

La plupart des options de la stratégie d'audit sont désactivées par défaut afin de minimiser les exigences en matière de stockage et de réduire le nombre de demandes de traitement du système. Ces options appartiennent du service d'audit et déterminent les stratégies en vigueur à l'initialisation du système. Pour plus d'informations, reportez-vous à la page de manuel `auditconfig`(1M).

Utilisez le tableau suivant pour déterminer si les besoins de votre site justifient le temps système supplémentaire résultant de l'activation d'une ou de plusieurs options de stratégie d'audit.

TABLEAU 2-2 Effets des options de stratégie d'audit

Nom de stratégie	Description	Remarques relatives à la 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. Si elle est activée, cette stratégie arrête le système lorsque la file d'audit est saturée. 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 réinitialiser 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 judicieuse dans un environnement où la sécurité est primordiale. Pour obtenir de plus amples renseignements, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones” à la page 125.
`arge`	Lorsqu'elle est désactivée, cette stratégie omet les variables d'environnement d'un programme exécuté dans l'enregistrement d'audit `execve`. Lorsqu'elle est activée, cette stratégie ajoute les variables d'environnement d'un programme exécuté à l'enregistrement d'audit `execve`. 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. Pour obtenir une comparaison, reportez-vous à la section “Audit de toutes les commandes par les utilisateurs” à la page 60. L'option activée est pratique lorsque vous auditez un petit nombre d'utilisateurs. Elle est également utile lorsque vous avez des doutes concernant les variables d'environnement utilisées dans les programmes de la classe d'audit `ex`.
`argv`	Lorsqu'elle est désactivée, cette stratégie omet les arguments d'un programme exécuté dans l'enregistrement d'audit `execve`. Lorsqu'elle est activée, cette stratégie ajoute les arguments d'un programme exécuté pour l'enregistrement d'audit `execve`. 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. Pour obtenir une comparaison, reportez-vous à la section “Audit de toutes les commandes par les utilisateurs” à la page 60. L'option activée est pratique lorsque vous auditez un petit nombre d'utilisateurs. Elle est également utile lorsque vous avez des raisons de penser que des programmes inhabituels dans la classe d'audit `ex` 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, en raison de la saturation de la file d'attente d'audit. Lorsqu'elle est activée, 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 judicieuse dans un environnement où la sécurité est primordiale. L'option activée est judicieuse lorsque la disponibilité du système est plus importante que la sécurité. Pour obtenir de plus amples renseignements, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones” à la page 125.
`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 judicieuse lorsque vous devez auditer les groupes supplémentaires auquel le sujet appartient.

Nom de stratégie	Description	Remarques relatives à la stratégie
`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 service d'audit s'exécute dans la zone globale. Des événements d'audit de zones spécifiques peuvent résider dans l'enregistrement d'audit si le jeton d'audit `zonename` a été présélectionné. 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 service d'audit 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 utile lorsque vous ne pouvez pas contrôler votre système efficacement en examinant tout simplement les enregistrements d'audit avec le jeton d'audit `zonename`.
`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. Vous pouvez également utiliser la commande `auditstat` pour visualiser les enregistrements rejetés.
`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 avec le jeton `sequence`. Le jeton `trailer` contribue à la restauration des pistes d'audit endommagées.
`zonename`	Lorsqu'elle est désactivée, cette stratégie n'inclut pas de jeton `zonename` dans les enregistrements d'audit.	L'option désactivée est utile lorsque vous n'avez pas besoin d'effectuer le suivi du comportement d'audit par zone.

Nom de stratégie	Description	Remarques relatives à la stratégie
	Lorsqu'elle est activée, cette stratégie comprend un jeton `zonename` dans chaque enregistrement d'audit.	L'option activée est utile lorsque vous souhaitez isoler et comparer le comportement d'audit des différentes zones par postsélection des enregistrements en fonction de la zone.

Contrôle des coûts d'audit

Etant 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

Si vous utilisez le plug-in par défaut, `audit_binfile`, vous devez également tenir compte du 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. Si vous utilisez le plug-in `audit_binfile`, les administrateurs d'audit peuvent déplacer les tâches de postsélection du système ayant fait l'objet d'un audit vers les systèmes dédiés à l'analyse des données d'audit. Enfin, le service d'audit n'a aucun impact mesurable sur les performances du système, sauf si les événements du noyau sont présélectionnés.

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.

Pour les enregistrements recueillis par le plug-in `audit_binfile`, le coût inclut également le temps nécessaire à l'archivage des enregistrements et de leurs bases de données de services de noms, et à la conservation des enregistrements dans un endroit sûr. `groups`, `hosts` et `passwd` sont quelques-unes des bases de données de support.

Le temps requis pour analyser la piste d'audit est d'autant plus court que le nombre d'enregistrements générés est faible. Les sections “Coût du stockage des données d'audit” à la page 39 et “Gestion efficace de l'audit” à la page 40 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

Si vous utilisez le plug-in `audit_binfile`, le coût du stockage est le plus significatif de l'audit. La quantité des données d'audit dépend des facteurs suivants :

- Nombre d'utilisateurs
- Nombre de systèmes
- Degré d'utilisation
- Degré de traçabilité et de responsabilité requis

Etant 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 :

- 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.
- 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 l'espace disque 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`.
- Si vous utilisez le plug-in `audit_binfile`, il est également important de gérer efficacement les fichiers d'audit. Par exemple, vous pouvez compresser un système de fichiers ZFS dédié aux fichiers d'audit.
- Développez une philosophie d'audit pour votre site.

  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 entreprise tout en améliorant l'efficacité de l'audit.

- Présélectionnez autant de classes d'audit que possible uniquement au niveau des utilisateurs et des rôles, non du système.
- Auditez de manière aléatoire uniquement un certain pourcentage d'utilisateurs à un moment donné.
- Si le plug-in `audit_binfile` est actif, réduisez l'espace de stockage requis sur le disque pour les fichiers d'audit par filtrage, fusion et compression des fichiers. Développez des procédures pour l'archivage des fichiers, le transfert des fichiers vers des médias amovibles et le stockage des fichiers hors ligne.
- Contrôlez les données d'audit en temps réel pour identifier des comportements inhabituels.
  - Plug-in `audit_syslog` : 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`.
  - plug-in `audit_binfile` : vous pouvez définir des procédures pour contrôler 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 les systèmes faisant l'objet d'un 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 systèmes de fichiers 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 3

Gestion du service d'audit

Ce chapitre fournit les procédures pour vous aider à configurer et gérer l'audit sur un système Oracle Solaris. Le chapitre décrit les tâches suivantes :

- “Configuration par défaut du service d'audit” à la page 41
- “Configuration du service d'audit” à la page 44
- “Personnalisation des objets audités” à la page 59
- “Configuration du service d'audit dans les zones” à la page 69
- “Exemple : Configuration de l'audit Oracle Solaris” à la page 73

En outre, les chapitres suivants décrivent d'autres tâches de gestion d'audit :

- Chapitre 4, Surveillance de l'activité du système
- Chapitre 5, Utilisation des données d'audit
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Pour obtenir une présentation générale du service d'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Configuration par défaut du service d'audit

Le service d'audit a une configuration par défaut et est immédiatement opérationnel sur la zone globale après avoir installé Oracle Solaris 11.2. Aucune action n'est obligatoire pour activer ou configurer le service pour pouvoir l'utiliser. Avec la configuration par défaut, le service d'audit enregistre les opérations suivantes :

- Opérations de connexion et déconnexion
- Utilisation de la commande `su`
- Opérations de verrouillage et déverrouillage de l'écran

Etant donné que la configuration par défaut du service n'a aucun impact sur les performances sur le système, la désactivation du service pour des raisons de performance n'est pas nécessaire.

A condition de disposer des droits d'audit appropriés, notamment ceux du profil Audit Review (vérification d'audit), vous pouvez consulter les journaux d'audit. Les journaux sont stockés dans `/var/audit/`*hostname*. Vous affichez ces fichiers à l'aide des commandes `praudit` et `auditreduce`. Pour plus d'informations, reportez-vous à la section “Affichage des données de la piste d'audit” à la page 95.

Les sections ci-après dans ce chapitre d'audit fournissent des instructions pour la personnalisation de la configuration du service d'audit, si la configuration par défaut ne suffit pas à répondre à vos besoins spécifiques.

Affichage de paramètres par défaut du service d'audit

Le service d'audit est régulé par les paramètres suivants :

- Classes d'événements attribuables et non attribuables
- Stratégie d'audit
- Plug-ins d'audit
- Contrôles de file d'attente

Pour afficher les paramètres par défaut du service d'audit, vous devez généralement utiliser la sous-commande `auditconfig -get*`. Cette sous-commande affiche la configuration actuelle du paramètre qui est représentée par l'astérisque (*), telle que `-getflags` `-getpolicy` ou `-getqctrl`. Pour afficher des informations sur les classes pour les événements non attribuables, utilisez la sous-commande . `auditconfig -getnaflags`.

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

Remarque - Pour afficher la configuration du service d'audit, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Configuration (Configuration de l'audit) ou Audit Control (Contrôle de l'audit). Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

Les exemples suivants montrent la syntaxe de commande appropriée à utiliser pour afficher les paramètres de configuration d'audit par défaut.

EXEMPLE 3-1 Affichage de la classe par défaut pour les événements

Dans cet exemple, deux sous-commandes sont utilisées pour afficher les classes présélectionnées pour les événements attribuables et non attribuables respectivement. Pour

afficher les événements qui sont affectés à une classe, et par conséquent, les événements qui sont en cours d'enregistrement, exécutez la commande `auditrecord -c` *class*.

```
# auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
```

`lo` est l'indicateur pour la classe d'audit `login/logout`. Le format de sortie du masque est (*success,failure*).

```
# auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

EXEMPLE 3-2 Affichage de la stratégie d'audit par défaut

```
$ auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

La stratégie *active* est la stratégie en cours, mais la valeur de la stratégie n'est pas stockée par le service d'audit. La stratégie *configurée* est enregistrée par le service d'audit, de sorte qu'elle est restaurée lorsque vous redémarrez le service d'audit.

EXEMPLE 3-3 Affichage des plug-ins d'audit par défaut

```
$ auditconfig -getplugin
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=0;p_minfree=1;

Plugin: audit_syslog (inactive)
Attributes: p_flags=;

Plugin: audit_remote (inactive)
Attributes: p_hosts=;p_retries=3;p_timeout=5;
```

Le plug-in `audit_binfile` est actif par défaut.

EXEMPLE 3-4 Affichage des contrôles de la file d'attente de l'audit

```
$ auditconfig -getqctrl
no configured audit queue hiwater mark
no configured audit queue lowater mark
no configured audit queue buffer size
no configured audit queue delay
active audit queue hiwater mark (records) = 100
active audit queue lowater mark (records) = 10
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

Le contrôle de la file d'attente *actif* est celui qui est actuellement utilisé par le noyau. La chaîne `no configured` indique que le système utilise les valeurs par défaut.

Activation et désactivation du service d'audit

Le service d'audit est activé par défaut. Si la stratégie d'audit `perzone` est définie, les administrateurs de zone doivent activer, actualiser ou désactiver le service d'audit dans chaque zone non globale si besoin. Si la stratégie d'audit `perzone` n'est pas définie, l'activation, l'actualisation ou la désactivation du service d'audit à partir de la zone globale est valide pour toutes les zones non globales.

Pour désactiver ou activer le service d'audit, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Control (contrôle d'audit). Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Pour désactiver le service d'audit, utilisez la commande suivante :

```
# audit -t
```

Pour activer le service d'audit, utilisez la commande suivante :

```
# audit -s
```

Pour vérifier que le service d'audit est en cours d'exécution, utilisez la commande suivante :

```
# auditconfig -getcond
audit condition = auditing
```

Si la stratégie d'audit `perzone` est définie, vous devez effectuez cette vérification dans les zones non globales où vous avez activé l'audit.

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

Configuration du service d'audit

Avant d'activer l'audit sur votre réseau, vous pouvez modifier les valeurs par défaut afin de répondre aux exigences en matière d'audit de votre site. Il est recommandé de personnaliser la configuration de l'audit autant que possible avant la connexion des premiers utilisateurs.

Si vous avez mis en oeuvre des zones, vous pouvez choisir d'auditer toutes les zones à partir de la zone globale ou les zones non globales une à une. Pour obtenir une présentation générale, reportez-vous à la section "Audit et Oracle Solaris Zones" à la page 121. Pour la

planification, reportez-vous à la section “Planification de l'audit dans les zones” à la page 28. Pour connaître les procédures, reportez-vous à la section “Configuration du service d'audit dans les zones” à la page 69.

Pour configurer le service d'audit, vous devez généralement utiliser la sous-commande `auditconfig`. La configuration définie avec ces sous-commandes s'applique à l'ensemble du système.

- `auditconfig -get*` affiche la configuration en cours du paramètre qui est représentée par l'astérisque (*), comme illustré dans les exemples de la section “Affichage de paramètres par défaut du service d'audit” à la page 42.
- `auditconfig -set*` affecte une valeur au paramètre qui sera représentée par l'astérisque (*), notamment `-setflags`, `-setpolicy` ou `-setqctrl`. Pour configurer des classes pour les événements non attribuables, vous utilisez la sous-commande `auditconfig setnaflags`.

Vous pouvez également personnaliser l'audit à appliquer à des utilisateurs ou profils, plutôt qu'à l'ensemble du système. Les présélections de classe d'audit pour chaque utilisateur sont spécifiées par l'attribut de sécurité `audit_flags`. Ces valeurs spécifiques à l'utilisateur, conjointement aux classes présélectionnées pour le système, déterminent le masque d'audit de l'utilisateur, comme décrit dans la section “Caractéristiques de l'audit de processus” à la page 126.

La présélection de classes par utilisateur plutôt que par système permet parfois de réduire l'impact de l'audit sur les performances du système. En outre, il peut être utile d'auditer des utilisateurs spécifiques de manière légèrement différente du système.

Pour configurer l'audit à appliquer à des utilisateurs ou profils, vous utilisez les commandes suivantes :

- `usrattr` affiche la valeur `audit_flags` qui est définie pour les utilisateurs. Par défaut, les utilisateurs sont soumis à un audit pour les paramètres à l'échelle du système uniquement.
- `usermod -K` définit les indicateurs qui s'appliquent à des utilisateurs.
- `profile` définit les indicateurs qui s'appliquent à des profils.

Pour obtenir une description de la commande `userattr`, reportez-vous à la page de manuel `userattr`(1). Pour obtenir une description du mot-clé `audit_flags`, reportez-vous à la page de manuel `user_attr`(4).

La liste des tâches suivante présente les procédures de configuration de l'audit. Toutes les tâches sont facultatives.

TABLEAU 3-1 Liste des tâches de configuration du service d'audit

Tâche	Description	Pour obtenir des instructions
Sélection des événements qui font l'objet d'un audit.	Présélectionne les classes d'audit à l'échelle du système. Si un événement est attribuable, tous les utilisateurs sont soumis à un audit pour cet événement.	“Présélection des classes d'audit” à la page 46

Tâche	Description	Pour obtenir des instructions
Sélection des événements qui font l'objet d'un audit pour des utilisateurs spécifiques.	Définit les différences utilisateur à partir des classes d'audit à l'échelle du système.	“Configuration des caractéristiques d'audit d'un utilisateur” à la page 47
Spécification de la stratégie d'audit.	Définit d'autres données d'audit dont votre site a besoin.	“Modification de la stratégie d'audit” à la page 51
Spécification des contrôles de file d'attente.	Modifie la taille de la mémoire tampon par défaut, les enregistrements d'audit dans la file d'attente et l'intervalle entre l'écriture des enregistrements d'audit dans la mémoire tampon.	“Modification des contrôles de file d'attente d'audit” à la page 54
Création de l'alias de messagerie `audit_warn`.	Définit le destinataire des avertissements électroniques lorsque le service d'audit requiert l'attention d'un utilisateur.	“Configuration de l'alias de messagerie `audit_warn` ” à la page 56
Configuration des journaux d'audit.	Configure l'emplacement des enregistrements d'audit pour chaque plug-in.	“Configuration des journaux d'audit” à la page 77
Ajout des classes d'audit.	Réduit le nombre d'enregistrements d'audit en créant une nouvelle classe d'audit pour contenir les événements critiques.	“Ajout d'une classe d'audit” à la page 57
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 58

▼ Présélection des classes d'audit

Présélectionnez les classes d'audit qui contiennent les événements que vous voulez surveiller. Les événements qui ne sont pas dans des classes présélectionnées ne sont pas enregistrés.

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

1. Déterminez les classes présélectionnées actuelles.

```
# auditconfig -getflags
...

# auditconfig -getnaflags
,,,
```

Pour obtenir une explication de la sortie, reportez-vous à la section “Affichage de paramètres par défaut du service d'audit” à la page 42.

2. Présélectionnez les classes attribuables.

```
# auditconfig -setflags lo,ps,fw
```

```
user default audit flags = ps,lo,fw(0x101002,0x101002)
```

Cette commande audite les événements des classes `login/logout`, `process start/stop` et `file write` pour en vérifier la réussite et l'échec.

Remarque - La commande `auditconfig -setflags` *remplace* la présélection actuelle, de sorte que vous devez spécifier toutes les classes à présélectionner.

---

3. Présélectionnez les classes non attribuables.

La classe `na` contient des montages non attribuables, d'initialisation et de PROM, parmi d'autres événements.

```
# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

`lo` et `na` sont les seuls arguments utiles de l'option `-setnaflags`.

Remarque - La commande `auditconfig -setnaflags` *remplace* la présélection actuelle, de sorte que vous devez spécifier toutes les classes à présélectionner.

▼ Configuration des caractéristiques d'audit d'un utilisateur

Les caractéristiques d'audit propres à l'utilisateur définies dans cette procédure sont combinées aux classes présélectionnées pour le système. Réunies, elles déterminent le masque d'audit de l'utilisateur, tel que décrit à la section “Caractéristiques de l'audit de processus” à la page 126.

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

1. (Facultatif) Affichez les classes d'audit qui sont actuellement sélectionnées pour les utilisateurs existants.

a. Affichez la liste des utilisateurs.

```
# who
adoe    pts/1        Oct 10 10:20 (:0.0)
adoe    pts/2        Oct 10 10:20 (:0.0)
jdoe    pts/5        Oct 12 12:20 (:0.0)
jdoe    pts/6        Oct 12 12:20 (:0.0)
...
```

b. **Affichez la valeur d'attribut `audit_flags` de chaque utilisateur.**

```
# userattr audit_flags adoe
# userattr audit_flags jdoe
```

2. **Définissez les indicateurs d'audit dans la base de données `user_attr` ou `prof_attr`.**

   Par exemple, vous pouvez créer un profil de droits qui définit les droits d'un sous-ensemble de vos utilisateurs. Les utilisateurs auxquels ce profil de droits est affecté font l'objet d'un audit identique.

   - **Pour définir les indicateurs d'audit d'un utilisateur, utilisez la commande `usermod`.**

     ```
     # usermod -K audit_flags=fw:no jdoe
     ```

     Le format du mot-clé `audit_flags` est *always-audit*:*never-audit*.

     always-audit — Répertorie les classes d'audit qui font l'objet d'un audit pour cet utilisateur. Les modifications apportées aux classes à l'échelle du système sont précédées d'un caret (^). Les classes qui sont ajoutées aux classes à l'échelle du système ne sont pas précédées d'un caret.

     never-audit — Répertorie les classes d'audit qui ne font jamais l'objet d'un audit pour l'utilisateur, même si ces événements d'audit sont audités à l'échelle du système. Les modifications apportées aux classes à l'échelle du système sont précédées d'un caret (^).

     Pour spécifier plusieurs classes d'audit, séparez les classes par une virgule. Pour plus d'informations, reportez-vous à la page de manuel `audit_flags`(5).

   - **Pour définir des indicateurs d'audit pour un profil de droits, utilisez la commande `profiles`.**

     ```
     # profiles -p "System Administrator"
     profiles:System Administrator> set name="Audited System Administrator"
     profiles:Audited System Administrator> set always_audit=fw,as
     profiles:Audited System Administrator> end
     profiles:Audited System Administrator> exit
     ```

     Lorsque vous affectez le profil de droits Audited System Administrator (administrateur de système audité) à un utilisateur ou à un rôle, celui-ci fait l'objet d'un audit pour ces indicateurs, en fonction de l'ordre de recherche décrit à la section " Ordre de recherche pour Assigned Rights " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Exemple 3-5 Modification des événements à auditer pour un utilisateur

Dans cet exemple, le masque de présélection d'audit pour tous les utilisateurs est le suivant :

```
# auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Aucun utilisateur, sauf l'administrateur, n'est connecté.

Pour réduire l'impact de l'événement d'audit `AUE_PFEXEC` sur les ressources système, l'administrateur n'effectue pas d'audit de cet événement au niveau du système. Au lieu de cela, l'administrateur présélectionne la classe `pf` pour un utilisateur, `jdoe`. La classe `pf` est créée dans l'Exemple 3-15, “Création d'une nouvelle classe d'audit”.

```
# usermod -K audit_flags=pf:no jdoe
```

La commande `userattr` affiche l'ajout.

```
# userattr audit_flags jdoe
pf:no
```

Lorsque l'utilisateur `jdoe` se connecte, le masque de présélection d'audit `jdoe` est une combinaison des valeurs `audit_flags` et des valeurs par défaut du système. `289` est le PID du shell de connexion de `jdoe` .

```
# auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = ss,pf,lo(0x0100000008011000,0x0100000008011000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

Exemple 3-6 Modification de l'exception de présélection d'audit pour un utilisateur

Dans cet exemple, le masque de présélection d'audit pour tous les utilisateurs est le suivant :

```
# auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Aucun utilisateur, sauf l'administrateur, n'est connecté.

L'administrateur décide de ne pas collecter les événements `ss` qui ont échoué pour l'utilisateur `jdoe`.

```
# usermod -K audit_flags=^-ss:no jdoe
```

La commande `userattr` affiche l'exception.

```
# userattr audit_flags jdoe
```

```
^-ss:no
```

Lorsque l'utilisateur `jdoe` se connecte, le masque de présélection d'audit `jdoe` est une combinaison des valeurs `audit_flags` et des valeurs par défaut du système. `289` est le PID du shell de connexion de `jdoe` .

```
# auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = +ss,lo(0x11000,0x1000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

Exemple 3-7 Audit des utilisateurs sélectionnés, pas d'audit à l'échelle du système

Dans cet exemple, les activités de connexion et de rôle de quatre utilisateurs sélectionnés sont auditées sur ce système. Aucune classe d'audit n'est présélectionnée pour le système.

Tout d'abord, l'administrateur supprime tous les indicateurs à l'échelle du système.

```
# auditconfig -setflags no
user default audit flags = no(0x0,0x0)
```

Ensuite, il présélectionne deux classes d'audit pour les quatre utilisateurs. La classe `pf` est créée dans l'Exemple 3-15, “Création d'une nouvelle classe d'audit”.

```
# usermod -K audit_flags=lo,pf:no jdoe
# usermod -K audit_flags=lo,pf:no kdoe
# usermod -K audit_flags=lo,pf:no pdoe
# usermod -K audit_flags=lo,pf:no zdoe
```

Ensuite, l'administrateur présélectionne la classe `pf` pour le rôle `root`.

```
# userattr audit_flags root
# rolemod -K audit_flags=lo,pf:no root
# userattr audit_flags root
lo,pf:no
```

Pour continuer d'enregistrer l'intrusion injustifiée, l'administrateur ne change pas l'audit des connexions non attribuables.

```
# auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

Exemple 3-8 Suppression des indicateurs d'audit d'un utilisateur

Dans l'exemple suivant, l'administrateur supprime tous les indicateurs d'audit spécifiques à l'utilisateur. Les processus existants d'utilisateurs qui sont actuellement connectés continuent à faire l'objet d'un audit.

L'administrateur exécute la commande `usermod` avec le mot-clé `audit_flags` défini sur aucune valeur.

```
# usermod -K audit_flags= jdoe
# usermod -K audit_flags= kdoe
# usermod -K audit_flags= ldoe
```

Ensuite, l'administrateur vérifie la suppression.

```
# userattr audit_flags jdoe
# userattr audit_flags kdoe
# userattr audit_flags ldoe
```

Exemple 3-9 Création d'un profil de droits pour un groupe d'utilisateurs

L'administrateur souhaite que tous les profils de droits d'administration du site auditent explicitement la classe `pf`. Pour chaque profil de droits à affecter, l'administrateur crée une version spécifique au site dans LDAP, qui inclut les indicateurs d'audit.

Tout d'abord, l'administrateur clone un profil de droits existant, puis change le nom et ajoute des indicateurs d'audit.

```
# profiles -p "Network Wifi Management" -S ldap
profiles: Network Wifi Management> set name="Wifi Management"
profiles: Wifi Management> set desc="Audited wifi management"
profiles: Wifi Management> set audit_always=pf
profiles: Wifi Management> exit
```

Après avoir reproduit cette procédure pour chaque profil de droits à utiliser, l'administrateur répertorie les informations dans le profil Wifi Management (gestion Wifi).

```
# profiles -p "Wifi Management" -S ldap info
name=Wifi Management
desc=Audited wifi management
auths=solaris.network.wifi.config
help=RtNetWifiMngmnt.html
always_audit=pf
```

▼ Modification de la stratégie d'audit

Il peut être utile de modifier la stratégie d'audit par défaut pour enregistrer des informations détaillées sur les commandes auditées, ajouter un nom de zone à chaque enregistrement ou satisfaire aux exigences d'autres sites en matière de sécurité.

Avant de commencer

Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Configuration (configuration d'audit). Pour plus d'informations, reportez-vous à la section “ A

l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

1. **Affichez la stratégie d'audit actuelle.**

```
$ auditconfig -getpolicy
...
```

Pour obtenir une explication de la sortie, reportez-vous à la section “Affichage de paramètres par défaut du service d'audit” à la page 42.

2. **Affichez les options de stratégie disponibles.**

```
$ auditconfig -lspolicy
policy string    description:
ahlt             halt machine if it can not record an async event
all              all policies for the zone
arge             include exec environment args in audit recs
argv             include exec command line args in audit recs
cnt              when no more space, drop recs and keep a cnt
group            include supplementary groups in audit recs
none             no policies
path             allow multiple paths per event
perzone          use a separate queue and auditd per zone
public           audit public files
seq              include a sequence number in audit recs
trail            include trailer token in audit recs
windata_down     include downgraded window information in audit recs
windata_up       include upgraded window information in audit recs
zonename         include zonename token in audit recs
```

Remarque - Les options de stratégie et `ahlt` peuvent être définies uniquement dans la zone globale. Pour que les compromis utilisent une option de stratégie particulière, reportez-vous à la section “Principes de la stratégie d'audit” à la page 35.

3. **Activez ou désactivez les options de stratégie d'audit sélectionnées.**

```
# auditconfig [ -t ] -setpolicy [prefix]policy[,policy...]
```

`-t` — Optionnel. Crée une stratégie temporaire ou *active*. Vous pouvez définir une stratégie temporaire à des fins de débogage ou de test.

Une politique temporaire reste en vigueur jusqu'à ce que le service d'audit soit actualisé ou que la stratégie soit modifiée par la commande `auditconfig -setpolicy`.

prefix — La valeur *prefix* + ajoute la liste des stratégies à la stratégie actuelle. La valeur *prefix* - supprime la liste des stratégies de la stratégie actuelle. Sans préfixe, la stratégie d'audit est réinitialisée. Cette option vous permet de conserver les stratégies d'audit en cours.

policy Sélectionne la stratégie à activer ou désactiver.

Exemple 3-10 Définition de l'option de stratégie d'audit `ahlt`

Dans cet exemple, la sécurité stricte du site requiert la stratégie `ahlt`.

```
# auditconfig -setpolicy -cnt
# auditconfig -setpolicy +ahlt
```

Le signe plus (+) avant la stratégie `ahlt` ajoute la stratégie aux paramètres de stratégie en cours. Sans le signe plus, la stratégie `ahlt` remplace toutes les stratégies d'audit actuelles.

Exemple 3-11 Définition d'une stratégie d'audit temporaire

Dans cet exemple, la stratégie d'audit `ahlt` est configurée. A des fins de débogage, l'administrateur ajoute la stratégie d'audit `trail` à la stratégie active (`+trail`) temporairement (`-t`). La stratégie `trail` contribue à la restauration des pistes d'audit endommagées.

```
$ auditconfig -setpolicy ahlt
$ auditconfig -getpolicy
configured audit policies = ahlt
active audit policies = ahlt
$ auditconfig -t -setpolicy +trail
configured audit policies = ahlt
active audit policies = ahlt,trail
```

L'administrateur désactive la stratégie `trail` lorsque le débogage est terminé.

```
$ auditconfig -setpolicy -trail
$ auditconfig -getpolicy
configured audit policies = ahlt
active audit policies = ahlt
```

L'actualisation du service d'audit à l'aide de la commande `audit -s` supprime également cette stratégie temporaire, ainsi que d'autres valeurs temporaires dans le service d'audit. Pour obtenir des exemples d'autres valeurs temporaires, reportez-vous à la section “Modification des contrôles de file d'attente d'audit” à la page 54.

Exemple 3-12 Définition de la stratégie d'audit `perzone`

Dans cet exemple, la stratégie d'audit `perzone` est ajoutée à la stratégie existante dans la zone globale. Le paramètre de stratégie `perzone` est stocké en tant que propriété permanente, de sorte que la stratégie `perzone` est en vigueur au cours de la session et au redémarrage du service d'audit. Pour les zones, la stratégie est disponible à la prochaine initialisation de zone.

```
$ auditconfig -getpolicy
```

```
configured audit policies = cnt
active audit policies = cnt
$ auditconfig -setpolicy +perzone
$ auditconfig -getpolicy
configured audit policies = perzone,cnt
active audit policies = perzone,cnt
```

Exemple 3-13 Pour la collecte des auditeurs externes des enregistrements d'audit

Dans cet exemple, l'administrateur collecte des enregistrements d'audit pour satisfaire les exigences des auditeurs externes. L'administrateur décide d'utiliser un serveur ARS pour collecter des informations sur les activités d'administration. L'administrateur collecte également des actions qui ne peuvent pas être attribuées à un utilisateur, telles que l'initialisation.

L'administrateur configure le serveur ARS. En plus d'auditer la classe `cusa`, l'administrateur ajoute des règles à la configuration de l'audit.

```
# auditconfig -setflags cusa
user default audit flags = ex,xa,ua,as,ss,ap,lo,ft(0x80475080,0x80475080)
# auditconfig -setpolicy ahlt,argv,argeauditconfig # auditconfig -getpolicy
configured audit policies = ahlt,arge,argv
active audit policies = ahlt,arge,argv
# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

Lorsque l'administrateur active le plug-in`audit_remote` et actualise le service d'audit, les enregistrements sont collectés.

▼ Modification des contrôles de file d'attente d'audit

Le service d'audit fournit des valeurs par défaut pour les paramètres de file d'attente d'audit. Vous pouvez examiner, modifier définitivement et modifier temporairement ces valeurs à l'aide de la commande `auditconfig`.

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

1. Affichez les valeurs actuelles des contrôles de file d'attente d'audit.

```
$ auditconfig -getqctrl
...
```

Pour obtenir une explication de la sortie, reportez-vous à la section "Affichage de paramètres par défaut du service d'audit" à la page 42.

2. **Modifiez les contrôles de file d'attente d'audit sélectionnés.**

   Pour obtenir des exemples et une description des contrôles de file d'attente d'audit, reportez-vous à la page de manuel `auditconfig`(1M).

   - Pour modifier certains ou tous les contrôles de file d'attente d'audit, utilisez l'option `-setqctrl`.

     ```
     # auditconfig [ -t ] -setqctrl hiwater lowater bufsz interval
     ```

     Les valeurs `hiwater` (limite supérieure) et `lowater` (limite inférieure) indiquent les points auxquels les processus sont respectivement en attente et en reprise. Les points sont mesurés en ce qui concerne le nombre d'enregistrements d'audit non distribués. La taille du tampon (`bufsz`) fait référence à la taille du tampon de la file d'attente. `Interval` indique le délai, mesuré en nombre de repères entre les générations de sortie d'audit.

     Par exemple, définissez la valeur *interval* sur `10` sans définir les autres contrôles.

     ```
     # auditconfig -setqctrl 0 0 0 10
     ```

   - Pour modifier un contrôle de file d'attente d'audit donné, spécifiez son option. L'option `-setqdelay` est l'équivalent de *interval* `-setqctrl 0 0 0`, comme dans **`auditconfig -setqdelay 10`**.

     ```
     # auditconfig [ -t ] -setqhiwater value
     # auditconfig [ -t ] -setqlowater value
     # auditconfig [ -t ] -setqbufsz value
     # auditconfig [ -t ] -setqdelay value
     ```

Exemple 3-14 Rétablissement de la valeur par défaut d'un contrôle de file d'attente d'audit

L'administrateur définit tous les contrôles de file d'attente d'audit, puis remplace la valeur *lowater* dans le référentiel par la valeur par défaut.

```
# auditconfig -setqctrl 200 5 10216 10
# auditconfig -setqctrl 200 0 10216 10
configured audit queue hiwater mark (records) = 200
no configured audit queue lowater mark
configured audit queue buffer size (bytes) = 10216
configured audit queue delay (ticks) = 10
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 5
active audit queue buffer size (bytes) = 10216
active audit queue delay (ticks) = 10
```

Par la suite, l'administrateur définit la valeur *lowater* par la valeur par défaut pour la session en cours.

```
# auditconfig -setqlowater 10
# auditconfig -getqlowater
configured audit queue lowater mark (records) = 10
active audit queue lowater mark (records) = 10
```

Configuration de l'alias de messagerie audit_warn

Le script /etc/security/audit_warn génère un message pour informer l'administrateur d'incidents d'audit qui nécessitent son attention. Vous pouvez personnaliser le script et envoyer le message à un compte autre que root.

Si la stratégie perzone est définie, l'administrateur de la zone non globale doit configurer l'alias de messagerie audit_warn dans la zone non globale.

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

- **Configurez l'alias de messagerie audit_warn.**

  Procédez de l'une des manières suivantes :

  - Remplacez l'alias de messagerie audit_warn par un autre compte de messagerie dans le script audit_warn.

    Remplacez l'alias de messagerie audit_warn dans la ligne ADDRESS du script par une autre adresse :

    ```
    #ADDRESS=audit_warn           # standard alias for audit alerts
    ADDRESS=audadmin               # role alias for audit alerts
    ```

    Remarque - Pour des informations sur les effets de la modification d'un fichier de configuration d'audit, reportez-vous à la section "Fichiers de configuration d'audit et empaquetage" à la page 121.

  - Redirigez la messagerie audit_warn vers un autre compte de messagerie.

    Ajoutez 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. L'entrée /etc/mail/aliases doit ressembler à ce qui suit si les comptes de messagerie électronique root et audadmin ont été ajoutés en tant que membres de l'alias de messagerie audit_warn :

    ```
    audit_warn: root,audadmin
    ```

    Ensuite, exécutez la commande newaliases pour reconstruire la base de données d'accès aléatoire pour le fichier alias.

    ```
    # newaliases
    /etc/mail/aliases: 14 aliases, longest 10 bytes, 156 bytes total
    ```

▼ 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. Cette stratégie peut réduire le nombre d'enregistrements qui sont collectés ainsi que le bruit de la piste d'audit.

Lorsque vous ajoutez la classe sur un seul système, copiez la modification sur tous les systèmes audités. Il est préférable de créer les classes d'audit avant la connexion des premiers utilisateurs.

Pour des informations sur les effets de la modification d'un fichier de configuration d'audit, reportez-vous à la section “Fichiers de configuration d'audit et empaquetage” à la page 121.

Astuce - Dans Oracle Solaris, vous pouvez créer votre propre package contenant des fichiers et remplacer les packages Oracle Solaris par les fichiers personnalisés de votre site. Lorsque vous définissez l'attribut `preserve` sur `true` dans votre package, les sous-commandes `pkg`, telles que verify, fix, revert, etc., sont exécutées par rapport à vos packages. Pour plus d'informations, reportez-vous aux pages de manuel `pkg`(1) et `pkg`(5).

Avant de commencer Choisissez des bits libres pour votre entrée unique. Vérifiez quels bits sont disponibles pour l'usage par des clients dans le fichier `/etc/security/fichier audit_class`.

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

1. **(Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_class`.**

   ```
   # cp /etc/security/audit_class /etc/security/audit_class.orig
   ```

2. **Ajoutez de nouvelles entrées au fichier `audit_class`.**

   Chaque entrée possède le format suivant :

   `0x`*64bitnumber*`:`*flag*`:`*description*

   Pour une description des champs, reportez-vous à la page de manuel `audit_class`(4). Pour obtenir la liste des classes existantes, consultez le fichier `/etc/security/audit_class`.

Exemple 3-15 Création d'une nouvelle classe d'audit

Cet exemple crée une classe pour contenir les commandes d'administration exécutées dans le cadre d'un rôle. L'entrée ajoutée au fichier `audit_class` se présente comme suit :

```
0x0100000000000000:pf:profile command
```

L'entrée crée la nouvelle classe d'audit `pf`. L'Exemple 3-16, “Mappage d'événements d'audit existants sur une nouvelle classe” montre comment renseigner la nouvelle classe d'audit.

Erreurs fréquentes

Si vous avez personnalisé le fichier `audit_class`, assurez-vous que tous les indicateurs d'audit qui sont assignés directement à des utilisateurs ou des profils de droits correspondent aux nouvelles classes d'audit. Des erreurs se produisent lorsqu'une valeur `audit_flags` n'est pas un sous-ensemble du fichier `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.

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.

Lorsque vous reconfigurez les mappages événements-classes d'audit d'un système, copiez la modification sur tous les systèmes audités. Il est vivement conseillé de modifier les mappages événements-classes avant que les premiers utilisateurs ne se connectent.

Remarque - Pour des informations sur les effets de la modification d'un fichier de configuration d'audit, reportez-vous à la section “Fichiers de configuration d'audit et empaquetage” à la page 121.

Astuce - Dans Oracle Solaris, vous pouvez créer votre propre package contenant des fichiers et remplacer les packages Oracle Solaris par les fichiers personnalisés de votre site. Lorsque vous définissez l'attribut `preserve` sur `true` dans votre package, les sous-commandes `pkg`, telles que verify, fix, revert, etc., sont exécutées par rapport à vos packages. Pour plus d'informations, reportez-vous aux pages de manuel `pkg`(1) et `pkg`(5).

Avant de commencer

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

1. **(Facultatif) Enregistrez une copie de sauvegarde du fichier `audit_event`.**

```
# cp /etc/security/audit_event /etc/security/audit_event.orig
```

2. **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 3-16 Mappage d'événements d'audit existants sur une nouvelle classe

Dans cet exemple, un événement d'audit existant est mappé à la nouvelle classe créée dans l'Exemple 3-15, “Création d'une nouvelle classe d'audit”. Par défaut, l'événement d'audit `AUE_PFEXEC` est mappé à plusieurs classes d'audit. En créant la nouvelle classe, l'administrateur peut auditer les événements `AUE_PFEXEC` sans auditer les événements dans les autres classes.

```
# grep pf /etc/security/audit_class
0x0100000000000000:pf:profile command
# grep AUE_PFEXEC /etc/security/audit_event
116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
# pfedit /etc/security/audit_event
#116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
116:AUE_PFEXEC:execve(2) with pfexec enabled:pf
# auditconfig -setflags lo,pf
user default audit flags = pf,lo(0x0100000000001000,0x0100000000001000)
```

Personnalisation des objets audités

La liste des tâches suivante répertorie les procédures permettant de configurer l'audit selon vos besoins.

TABLEAU 3-2 Liste des tâches de la personnalisation de l'audit

Tâche	Description	Pour obtenir des instructions
Audit de toutes les opérations effectuées par l'utilisateur sur le système.	Auditez un ou plusieurs utilisateurs pour chaque commande.	“Audit de toutes les commandes par les utilisateurs” à la page 60
Modification des événements d'audit enregistrés et application de la modification aux sessions existantes.	Mettez à jour un masque de présélection utilisateur.	“Mise à jour du masque de présélection des utilisateurs connectés” à la page 64

Tâche	Description	Pour obtenir des instructions
Accès aux modifications apportées à des fichiers donnés.	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 62
Utilisation de moins d'espace du système de fichiers pour les fichiers d'audit.	Utilisez la compression et les quotas ZFS.	“Compression des fichiers d'audit sur un système de fichiers dédié” à la page 66
Suppression des événements d'audit du fichier `audit_event`.	Mettez correctement à jour le fichier `audit_event`.	“Suppression de l'audit d'événements spécifiques” à la page 65

▼ Audit de toutes les commandes par les utilisateurs

Dans le cadre de leur stratégie de sécurité, certains sites nécessitent des enregistrements d'audit de toutes les commandes exécutées par les rôles d'administration et le compte `root`. Certains sites peuvent nécessiter des enregistrements d'audit pour toutes les commandes exécutées par tous les utilisateurs. En outre, les sites peuvent nécessiter que les arguments de commande et l'environnement soient enregistrés.

Avant de commencer Pour présélectionner les classes d'audit et définir la stratégie d'audit, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Configuration (configuration d'audit). Pour affecter les indicateurs d'audit aux utilisateurs, rôles et profils de droits, vous devez prendre le rôle `root`.

1. Affichez les informations sur l'événement au niveau des utilisateurs pour 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`.

```
% auditconfig -lsevent | grep " lo "
AUE_login                       6152 lo login - local
AUE_logout                      6153 lo logout
AUE_telnet                      6154 lo login - telnet
AUE_rlogin                      6155 lo login - rlogin
AUE_rshd                        6158 lo rsh access
AUE_su                          6159 lo su
AUE_rexecd                      6162 lo rexecd
AUE_passwd                      6163 lo passwd
AUE_rexd                        6164 lo rexd
AUE_ftpd                        6165 lo ftp access
AUE_ftpd_logout                 6171 lo ftp logout
AUE_ssh                         6172 lo login - ssh
```

```
AUE_role_login                  6173 lo role login
AUE_newgrp_login                6212 lo newgrp login
AUE_admin_authenticate          6213 lo admin login
AUE_screenlock                  6221 lo screenlock - lock
AUE_screenunlock                6222 lo screenlock - unlock
AUE_zlogin                      6227 lo login - zlogin
AUE_su_logout                   6228 lo su logout
AUE_role_logout                 6229 lo role logout
AUE_smbd_session                6244 lo smbd(1m) session setup
AUE_smbd_logoff                 6245 lo smbd(1m) session logoff
AUE_ClientConnect               9101 lo client connection to x server
AUE_ClientDisconnect            9102 lo client disconn. from x server

% auditconfig -lsevent | egrep " ex |,ex |ex,"
AUE_EXECVE                       23 ex,ps execve(2)
```

2. Auditez les classes `lo` et `ex`.

- **Pour auditer ces classes pour les rôles d'administration, modifiez les attributs de sécurité des rôles.**

  Dans l'exemple suivant, `root` est un rôle. Le site a créé trois rôles, `sysadm`, `auditadm` et `netadm`. Tous les rôles sont soumis à un audit pour la réussite et l'échec d'événements dans les classes `ex` et `lo`.

  ```
  # rolemod -K audit_flags=lo,ex:no root

  # rolemod -K audit_flags=lo,ex:no sysadm

  # rolemod -K audit_flags=lo,ex:no auditadm

  # rolemod -K audit_flags=lo,ex:no netadm
  ```

- **Pour auditer ces classes pour tous les utilisateurs, définissez les indicateurs à l'échelle du système.**

  ```
  # auditconfig -setflags lo,ex
  ```

  La sortie se présente de la manière suivante :

  ```
  header,129,2,AUE_EXECVE,,mach1,2010-10-14 12:17:12.616 -07:00
  path,/usr/bin/ls
  attribute,100555,root,bin,21,320271,18446744073709551615
  subject,jdoe,root,root,root,root,2486,50036632,82 0 mach1
  return,success,0
  ```

3. Fournissez des informations supplémentaires à enregistrer sur l'utilisation des commandes.

- **Pour enregistrer les arguments de commande, ajoutez la stratégie `argv`.**

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

Le jeton `exec_args` enregistre les arguments de commande :

```
header,151,2,AUE_EXECVE,,mach1,2010-10-14 12:26:17.373 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args
,2,ls,/etc/security
subject,jdoe,root,root,root,root,2494,50036632,82 0 mach1
return,success,0
```

- **Pour enregistrer l'environnement dans lequel la commande est exécutée, ajoutez la stratégie `arge`.**

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

  Le jeton `exec_env` enregistre l'environnement de commande :

  ```
  header,1460,2,AUE_EXECVE,,mach1,2010-10-14 12:29:39.679 -07:00
  path,/usr/bin/ls
  attribute,100555,root,bin,21,320271,18446744073709551615
  exec_args,2,ls,/etc/security
  exec_env
  ,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
  LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLVL=2,
  HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8,
  PRINTER=example-dbl,...,_=/usr/bin/ls
  subject,jdoe,root,root,root,root,2502,50036632,82 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.

Avant de commencer

Le rôle `root` peut effectuer toutes les tâches de cette procédure.

Si des droits d'administration sont répartis dans votre entreprise, notez les éléments suivants :

- Un administrateur disposant du profil de droits Audit Configuration (configuration d'audit) peut exécuter la commande `auditconfig`.
- Un administrateur disposant du profil de droits Audit Review (vérification d'audit) peut exécuter la commande `auditreduce`.
- Seul le rôle `root` peut attribuer des indicateurs d'audit.

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

1. **Effectuez l'une des étapes suivantes pour effectuer un audit des modifications apportées aux fichiers.**

   - Effectuez un audit de la classe `fw`.

     L'ajout de la classe `fw` aux indicateurs d'audit d'un utilisateur ou d'un rôle génère moins d'enregistrements que l'ajout de cette classe au masque de présélection d'audit à l'échelle du système. Effectuez l'une des étapes suivantes :

     - Ajoutez la classe `fw` à des rôles spécifiques.

       ```
       # rolemod -K audit_flags=fw:no root
       # rolemod -K audit_flags=fw:no sysadm
       # rolemod -K audit_flags=fw:no auditadm
       # rolemod -K audit_flags=fw:no netadm
       ```

     - Ajoutez la classe `fw` aux indicateurs à l'échelle du système.

       ```
       # auditconfig -getflags
       active user default audit flags = lo(0x1000,0x1000)
       configured user default audit flags = lo(0x1000,0x1000)

       # auditconfig -setflags lo,fw
       user default audit flags = lo,fw(0x1002,0x1002)
       ```

   - Auditez les écritures sur fichiers réussies.

     L'audit des réussites génère un nombre inférieur d'enregistrements que l'audit des échecs et des réussites. Effectuez l'une des étapes suivantes :

     - Ajoutez l'indicateur `+fw` à des rôles spécifiques.

       ```
       # rolemod -K audit_flags=+fw:no root
       # rolemod -K audit_flags=+fw:no sysadm
       # rolemod -K audit_flags=+fw:no auditadm
       # rolemod -K audit_flags=+fw:no netadm
       ```

     - Ajoutez l'indicateur `+fw` aux indicateurs à l'échelle du système.

       ```
       # auditconfig -getflags
       active user default audit flags = lo(0x1000,0x1000)
       configured user default audit flags = lo(0x1000,0x1000)

       # auditconfig -setflags lo,+fw
       user default audit flags = lo,+fw(0x1002,0x1000)
       ```

2. **Obtenez les enregistrements d'audit pour des fichiers spécifiques à l'aide de la commande `auditreduce`.**

```
# 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`. La 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=` *pathname*.

3. **Lisez le fichier `filechg` à l'aide de la commande `praudit`.**

```
# praudit *filechg
```

▼ Mise à jour du masque de présélection des utilisateurs connectés

Cette procédure décrit les étapes à suivre pour effectuer un audit des utilisateurs déjà connectés pour les modifications apportées au masque de présélection d'audit à l'échelle du système. En règle générale, vous pouvez accomplir cette tâche en demandant aux utilisateurs de se déconnecter puis de se reconnecter. Vous pouvez également, dans un rôle auquel est attribué le profil de droits Process management (Gestion des processus), mettre fin manuellement aux sessions actives à l'aide de la commande `kill`. La nouvelle session va hériter du nouveau masque présélection.

L'arrêt des sessions utilisateur n'est toutefois pas très pratique. Vous pouvez également utiliser la commande `auditconfig` pour modifier de façon dynamique le masque de présélection de chaque utilisateur connecté.

La procédure suivante part du principe que vous avez modifié le masque de présélection d'audit à l'échelle du système pour passer de `lo` à `lo,ex` en exécutant la commande suivante :

```
# auditconfig -setflags lo,ex
```

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

1. **Répertoriez les utilisateurs standard qui sont connectés et leur ID de processus.**

```
# who -a
```

```
jdoe  - vt/2         Jan 25 07:56  4:10   1597   (:0)
jdoe  + pts/1        Jan 25 10:10   .     1706   (:0.0)
...
jdoe  + pts/2        Jan 25 11:36  3:41   1706   (:0.0)
```

2. **A des fins de comparaison ultérieure, affichez le masque de présélection de chaque utilisateur.**

```
# auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = lo(0x1000,0x1000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

3. **Modifiez le masque de présélection approprié en exécutant l'une ou plusieurs des commandes suivantes :**

```
# auditconfig -setpmask 1706 lo,ex              /* for this process */

# auditconfig -setumask jdoe lo,ex              /* for this user */

# auditconfig -setsmask 103203403 lo,ex         /* for this session */
```

4. **Vérifiez que le masque de présélection de l'utilisateur a changé.**

   Par exemple, vérifiez un processus qui existait avant la modification du masque.

```
# auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = ex,lo(0x40001000,0x40001000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

▼ Suppression de l'audit d'événements spécifiques

Pour des raisons de maintenance, il arrive parfois qu'un site veuille empêcher les événements d'être soumis à un audit.

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

1. **Changez la classe de l'événement pour la classe `no`.**

Remarque - Pour des informations sur les effets de la modification d'un fichier de configuration d'audit, reportez-vous à la section "Fichiers de configuration d'audit et empaquetage" à la page 121.

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 que ces événements ne soient plus soumis à un audit, vous devez mettre à jour les masques de présélection des utilisateurs en suivant les instructions décrites dans la section “Mise à jour du masque de présélection des utilisateurs connectés” à la page 64.

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. **Actualisez les événements du noyau.**

```
# auditconfig -conf
Configured 283 kernel events.
```

Compression des fichiers d'audit sur un système de fichiers dédié

Les fichiers d'audit peuvent devenir très volumineux. Vous pouvez définir une limite supérieure à la taille d'un fichier, comme illustré dans l'Exemple 4-3, “Limitation de la taille des fichiers pour le plug-in `audit_binfile`”. Dans cette procédure, vous réduisez la taille par compression.

Avant de commencer Vous devez vous connecter en tant qu'administrateur disposant des profils de droits ZFS File System Management (gestion de système de fichiers ZFS) et ZFS Storage Management (gestion de stockage ZFS). Le dernier profil vous permet de créer des pools de stockage. Pour plus

d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

1. **Dédiez un système de fichiers ZFS aux fichiers d'audit.**

   Pour obtenir la procédure, reportez-vous à la section "Création de systèmes de fichiers ZFS pour les fichiers d'audit" à la page 78.

2. **Compressez le pool de stockage ZFS à l'aide de l'une des options suivantes.**

   Avec ces deux options, le système de fichiers d'audit est compressé. Une fois le service d'audit actualisé, le taux de compression s'affiche.

   Dans les exemples suivants, le pool ZFS `auditp/auditf` est le jeu de données.

   - **Utilisez l'algorithme de compression par défaut.**

     ```
     # zfs set compression=on auditp/auditf
     # audit -s
     # zfs get compressratio auditp/auditf
     NAME           PROPERTY       VALUE  SOURCE
     auditp/auditf  compressratio  4.54x  -
     ```

   - **Utilisez un algorithme de compression plus élevé.**

     ```
     # zfs set compression=gzip-9 auditp/auditf
     # zfs get compression auditp/auditf
     NAME           PROPERTY     VALUE     SOURCE
     auditp/auditf  compression  gzip-9    local
     ```

     L'algorithme de compression `gzip-9` génère des fichiers qui occupent un tiers d'espace de moins qu'avec l'algorithme de compression par défaut `lzjb`. Pour plus d'informations, reportez-vous au Chapitre 5, " Gestion des systèmes de fichiers Oracle Solaris ZFS " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ".

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

   ```
   # audit -s
   ```

4. **(Facultatif) Vérifiez le nouveau paramètre de compression.**

   Par exemple, si vous avez utilisé l'algorithme de compression plus élevé, les informations doivent ressembler à ce qui suit :

   ```
   # zfs get compressration auditp/auditf
   NAME           PROPERTY       VALUE  SOURCE
   auditp/auditf  compressratio  16.89x  -
   ```

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 audité par présélection de la classe d'audit `ft`. Les connexions aux deux services peuvent faire l'objet d'un audit.

Remarque - Pour des informations sur la journalisation de commandes et transferts de fichiers du service FTP, reportez-vous à la page de manuel `proftpd`(8).

Pour connaître les options de journalisation disponibles, visitez la page ProFTPD Logging (http://www.proftpd.org/docs/howto/Logging.html).

- **Effectuez l'une des opérations suivantes selon que vous souhaitez effectuer un audit SFTP ou FTP.**

  - Pour journaliser l'accès et les transferts de fichier `sftp`, modifiez la classe `ft`.

    La classe `ft` comprend les transactions SFTP suivantes :

    ```
    % auditrecord -c ft
    file transfer: chmod ...
    file transfer: chown ...
    file transfer: get ...
    file transfer: mkdir ...
    file transfer: put ...
    file transfer: remove ...
    file transfer: rename ...
    file transfer: rmdir ...
    file transfer: session start ...
    file transfer: session end ...
    file transfer: symlink ...
    file transfer: utimes
    ```

  - Pour enregistrer l'accès au serveur FTP, auditez la classe `lo`.

    Comme indiqué dans l'exemple de sortie suivant, la connexion et la déconnexion du démon `proftpd` génèrent des enregistrements d'audit.

    ```
    % auditrecord -c lo | more
    ...
    FTP server login
    program     proftpd             See in.ftpd(1M)
    event ID    6165                AUE_ftpd
    class       lo                  (0x0000000000001000)
    header
    subject
    [text]                      error message
    ```

```
return

FTP server logout
program     proftpd             See in.ftpd(1M)
event ID    6171                AUE_ftpd_logout
class       lo                  (0x0000000000001000)
header
subject
return
...
```

Configuration du service d'audit dans les zones

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 configurer l'audit par zone. Pour plus d'informations, reportez-vous à la section “Planification de l'audit dans les zones” à la page 28.

Lorsque vous auditez les zones non globales de la même manière que vous auditez la zone globale, les administrateurs des zones non globales risquent de ne pas avoir accès aux enregistrements d'audit. L'administrateur de la zone globale peut également modifier les masques de présélection d'audit des utilisateurs dans les zones non globales.

Lorsque vous auditez les zones non globales séparément, les enregistrements d'audit sont visibles pour la zone non globale et pour la zone globale à partir du root de zone non globale.

▼ 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.

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

1. **Configurez la zone globale pour l'audit.**

   Effectuez les tâches de la section “Configuration du service d'audit” à la page 44, à l'exception des points suivants :

- N'activez pas la stratégie d'audit `perzone`.
- Définissez la stratégie `zonename`. Cette stratégie permet d'ajouter le nom de la zone à chaque enregistrement d'audit.

  ```
  # auditconfig -setpolicy +zonename
  ```

2. **Si vous avez modifié les fichiers de configuration de l'audit, copiez-les de la zone globale vers chaque zone non globale.**

   Si vous avez modifié le fichier `audit_class` ou `audit_event`, copiez-le de l'une des deux façons suivantes :

   - Vous pouvez monter en loopback les fichiers.
   - Vous pouvez copier les fichiers.

   La zone non globale doit être en cours d'exécution.

   - **Montez les fichiers `audit_class` et `audit_event` modifiés en tant que système de fichiers loopback (`lofs`).**

     a. **A 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
     zone: add fs
     zone/fs: set special=/etc/security/audit-file
     zone/fs: set dir=/etc/security/audit-file
     zone/fs: set type=lofs
     zone/fs: add options [ro,nodevices,nosetuid]
     zone/fs: commit
     zone/fs: end
     zone: exit
     #
     ```

     c. **Pour valider les changements, initialisez la zone non globale.**

     ```
     # zoneadm -z non-global-zone boot
     ```

     Par la suite, si vous modifiez un fichier de configuration d'audit dans la zone globale, réinitialisez chaque zone pour actualiser les fichiers montés en loopback dans les zones non globales.

   - **Copiez les fichiers.**

a. A partir de la zone globale, répertoriez le répertoire `/etc/security` dans chaque zone non globale.

```
# ls /zone/zonename/root/etc/security/
```

b. Copiez les fichiers `audit_class` et `audit_event` modifiés dans le répertoire `/etc/security` de chaque zone.

```
# cp /etc/security/audit-file /zone/zonename/root/etc/security/audit-file
```

Par la suite, si vous modifiez l'un de ces fichiers dans la zone globale, vous devez copier le fichier modifié dans les zones non globales.

Les zones non globales sont auditées au redémarrage du service d'audit dans la zone globale ou lorsque les zones sont réinitialisées.

Exemple 3-17 Montage des fichiers de configuration d'audit en tant que montage loopback dans une zone

Dans cet exemple, l'administrateur système a modifié les fichiers `audit_class`, `audit_event` et `audit_warn`.

Le fichier `audit_warn` est lu dans la zone globale uniquement, de sorte qu'il n'a pas à être monté 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 modification des fichiers de configuration d'audit. Si l'administrateur modifie ultérieurement les fichiers, la zone doit être réinitialisée pour relire les montages en loopback.

```
# zoneadm -z machine1-webserver halt
# zoneadm -z machine1-appserver halt
# zonecfg -z machine1-webserver
webserver: add fs
webserver/fs: set special=/etc/security/audit_class
webserver/fs: set dir=/etc/security/audit_class
webserver/fs: set type=lofs
webserver/fs: add options [ro,nodevices,nosetuid]
webserver/fs: commit
webserver/fs: end
webserver: add fs
webserver/fs: set special=/etc/security/audit_event
webserver/fs: set dir=/etc/security/audit_event
webserver/fs: set type=lofs
webserver/fs: add options [ro,nodevices,nosetuid]
webserver/fs: commit
webserver/fs: end
webserver: exit
#
```

```
# zonecfg -z machine1-appserver
appserver: add fs
appserver/fs: set special=/etc/security/audit_class
appserver/fs: set dir=/etc/security/audit_class
appserver/fs: set type=lofs
appserver/fs: add options [ro,nodevices,nosetuid]
appserver/fs: commit
appserver/fs: end
appserver: exit
```

Lorsque les zones non globales sont réinitialisées, les fichiers `audit_class` et `audit_event` 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).

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

1. **Dans la zone globale, configurez l'audit.**

   a. **Réalisez les tâches de la section "Configuration du service d'audit" à la page 44.**

   b. **Ajoutez la stratégie d'audit `perzone`. Pour la commande, reportez-vous à l'Exemple 3-12, "Définition de la stratégie d'audit `perzone`".**

   Remarque - Vous n'êtes pas obligé d'activer le service d'audit dans la zone globale.

2. **Dans chaque zone non globale que vous envisagez d'auditer, configurez les fichiers d'audit.**

   a. **Réalisez les tâches de la section "Configuration du service d'audit" à la page 44.**

   b. **Ne configurez pas les paramètres d'audit système.**

En particulier, n'ajoutez pas la stratégie `perzone` ou `ahlt` à la zone non globale.

3. **Activez l'audit dans votre zone.**

```
myzone# audit -s
```

Exemple 3-18 Désactivation de l'audit dans une zone non globale

Cet exemple fonctionne si la stratégie d'audit `perzone` est définie. L'administrateur de zone de la zone `noaudit` désactive l'audit pour cette zone.

```
noauditzone # auditconfig -getcond
audit condition = auditing
noauditzone # audit -t
noauditzone # auditconfig -getcond
audit condition = noaudit
```

Exemple : Configuration de l'audit Oracle Solaris

La présente section donne un exemple de configuration et d'implémentation de l'audit de Oracle Solaris. Elle commence par la configuration de différents attributs du service en fonction des besoins et exigences spécifiques. Une fois la configuration terminée, le service d'audit est démarré pour appliquer les paramètres de configuration. Chaque fois que vous devez vérifier une configuration d'audit existante pour répondre à de nouveaux besoins, suivez la même séquence d'opérations que dans l'exemple ci-dessous :

1. Configurez les paramètres d'audit.
2. Actualisez le service d'audit.
3. Vérifiez la nouvelle configuration d'audit.

- Tout d'abord, l'administrateur ajoute une stratégie temporaire.

```
# auditconfig -t -setpolicy +zonename
# auditconfig -getpolicy
configured audit policies = ahlt,arge,argv,perzone
active audit policies = ahlt,arge,argv,perzone,zonename
```

- Ensuite, l'administrateur spécifie les contrôles de file d'attente.

```
# auditconfig -setqctrl 200 20 0 0
# auditconfig -getqctrl
configured audit queue hiwater mark (records) = 200
configured audit queue lowater mark (records) = 20
configured audit queue buffer size (bytes) = 8192
configured audit queue delay (ticks) = 20
```

```
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 20
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

- Ensuite, l'administrateur spécifie les attributs de plug-in.
  - Pour le plug-in `audit_binfile`, l'administrateur supprime la valeur `qsize`.

    ```
    # auditconfig -getplugin audit_binfile
    Plugin: audit_binfile
    Attributes: p_dir=/audit/sys1.1,/var/audit;
    p_minfree=2;p_fsize=4G;
    Queue size: 200
    # auditconfig -setplugin audit_binfile  "" 0
    # auditconfig -getplugin audit_binfile
    Plugin: audit_binfile
    Attributes: p_dir=/audit/sys1.1,/var/audit
    p_minfree=2;p_fsize=4G;
    ```

  - Pour le plug-in `audit_syslog`, l'administrateur indique l'envoi des événements de connexion et de déconnexion et des exécutables qui ont échoué à `syslog`. La valeur de l'attribut `qsize` pour ce plug-in est définie sur 150.

    ```
    # auditconfig -setplugin audit_syslog active p_flags=+lo,-ex 150
    # auditconfig -getplugin audit_syslog
    auditconfig -getplugin audit_syslog
    Plugin: audit_syslog
    Attributes: p_flags=+lo,-ex;
    Queue size: 150
    ```

  - L'administrateur ne configure pas ou n'utilise pas le plug-in `audit_remote` .
- Ensuite, l'administrateur actualise le service d'audit et vérifie la configuration.
  - La stratégie temporaire `zonename` n'est plus définie.

    ```
    # audit -s
    # auditconfig -getpolicy
    configured audit policies = ahlt,arge,argv,perzone
    active audit policies = ahlt,arge,argv,perzone
    ```

  - Les contrôles de file d'attente restent identiques.

    ```
    # auditconfig -getqctrl
    configured audit queue hiwater mark (records) = 200
    configured audit queue lowater mark (records) = 20
    configured audit queue buffer size (bytes) = 8192
    configured audit queue delay (ticks) = 20
    active audit queue hiwater mark (records) = 200
    active audit queue lowater mark (records) = 20
    active audit queue buffer size (bytes) = 8192
    ```

```
active audit queue delay (ticks) = 20
```

- Le plug-in `audit_binfile` n'a pas une taille de file d'attente spécifiée. Le plug-in `audit_syslog` a une taille de file d'attente spécifiée.

```
# auditconfig -getplugin
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;

Plugin: audit_syslog
Attributes: p_flags=+lo,-ex;
Queue size: 50
...
```

♦ ♦ ♦ CHAPITRE 4

Surveillance de l'activité du système

Ce chapitre fournit des procédures pour vous aider à configurer les journaux d'audit qui vous permettent de surveiller l'activité du système. En outre, les chapitres suivants décrivent d'autres tâches de gestion d'audit :

- Chapitre 3, Gestion du service d'audit
- Chapitre 5, Utilisation des données d'audit
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Pour obtenir une présentation générale du service d'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Configuration des journaux d'audit

Deux plug-ins d'audit, `audit_binfile` et `audit_syslog` , permettent de créer des journaux d'audit locaux. Les tâches suivantes expliquent comment configurer ces journaux.

Configuration des journaux d'audit

La liste des tâches suivante indique les procédures de configuration des journaux d'audit pour les différents plug-ins. La configuration de journaux pour le plug-in `audit_binfile` est facultative. Les journaux des autres plug-ins doivent être configurés par un administrateur.

TABLEAU 4-1 Liste des tâches de configuration des journaux d'audit

Tâche	Description	Pour obtenir des instructions
Ajout d'espace de stockage local pour le plug-in `audit_binfile`	Crée de l'espace disque supplémentaire pour les fichiers d'audit et les protège à l'aide d'autorisations de fichiers	“Création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 78

Tâche	Description	Pour obtenir des instructions
Assignation d'espace de stockage pour le plug-in `audit_binfile`	Identifie les répertoires pour les enregistrements d'audit binaires	“Affectation de l'espace d'audit pour la piste d'audit” à la page 82
Configuration de la transmission des enregistrements d'audit vers un système distant	Vous permet d'envoyer des enregistrements d'audit à un référentiel distant par le biais d'un mécanisme protégé	“Envoi des fichiers d'audit à un référentiel distant” à la page 85
Configuration d'un stockage distant pour les fichiers d'audit	Vous permet de recevoir des enregistrements d'audit sur un système distant	“Configuration d'un référentiel distant pour les fichiers d'audit” à la page 87
Configuration d'espace de stockage pour le plug-in `audit_syslog`	Vous permet de diffuser les événements d'audit au format texte à `syslog`	“Configuration des journaux d'audit `syslog`” à la page 91

▼ Création de systèmes de fichiers ZFS pour les fichiers d'audit

La procédure suivante décrit la création d'un pool ZFS pour les fichiers d'audit, ainsi que les systèmes de fichiers et points de montage correspondants. Par défaut, le système de fichiers `/var/audit` contient les fichiers d'audit pour le plug-in `audit_binfile`.

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

1. Déterminez 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, il peut être beaucoup plus important que le chiffre indiqué.

Remarque - La présélection de classe par défaut crée des fichiers dans `/var/audit` qui augmentent d'environ 80 octets pour chaque instance enregistrée d'un événement dans la classe `lo`, notamment la prise de rôle, la connexion ou la déconnexion.

---

2. Créez un pool de stockage ZFS mis en miroir.

La commande `zpool create` crée un pool de stockage, c'est-à-dire un conteneur pour les systèmes de fichiers ZFS. Pour plus d'informations, reportez-vous au Chapitre 1, “ Système de fichiers Oracle Solaris ZFS (introduction) ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.

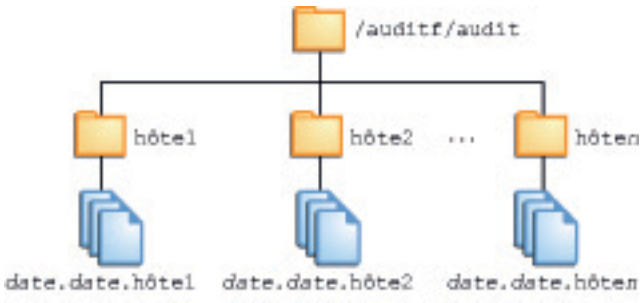
```
# zpool create audit-pool mirror disk1 disk2
```

Par exemple, créez le pool `auditp` à partir de deux disques, `c3t1d0` et `c3t2d0`, et mettez-les en miroir.

```
# zpool create auditp mirror c3t1d0 c3t2d0
```

3. **Créez un système de fichiers ZFS et un point de montage pour les fichiers d'audit.**

   Vous créez le système de fichiers et le point de montage à l'aide d'une seule commande. Au moment de la création, le système de fichiers est monté. Par exemple, l'illustration suivante indique le stockage de la piste d'audit, trié par nom d'hôte.



Remarque - Si vous envisagez de chiffrer le système de fichiers, vous devez le faire lors de sa création. Pour un exemple, reportez-vous à l'Exemple 4-1, “Création d'un système de fichiers chiffré pour les fichiers d'audit”.

Le chiffrement doit être géré. Par exemple, une phrase de passe est nécessaire au moment du montage. Pour plus d'informations, reportez-vous à la section “ Chiffrement des systèmes de fichiers ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.

```
# zfs create -o mountpoint=/mountpoint audit-pool/mountpoint
```

Par exemple, créez le point de montage `/audit` pour le système de fichiers `auditf`.

```
# zfs create -o mountpoint=/audit auditp/auditf
```

4. **Créez un système de fichiers ZFS pour les fichiers d'audit.**

```
# zfs create -p auditp/auditf/system
```

Par exemple, créez un système de fichiers ZFS non chiffré pour le système `sys1`.

```
# zfs create -p auditp/auditf/sys1
```

5. **(Facultatif) Créez des systèmes de fichiers supplémentaires pour les fichiers d'audit.**

   Une des raisons de créer des systèmes de fichiers supplémentaires est d'empêcher un débordement d'audit. Vous pouvez définir un quota ZFS par système de fichiers, comme illustré à l'Étape 8. L'alias électronique `audit_warn` vous avertit lorsque chaque quota est atteint. Pour libérer de l'espace, vous pouvez déplacer les fichiers d'audit fermés vers un serveur distant.

   ```
   # zfs create -p auditp/auditf/sys1.1

   # zfs create -p auditp/auditf/sys1.2
   ```

6. **Protégez le système de fichiers d'audit parent.**

   Les propriétés ZFS suivantes sont définies sur `off` pour tous les systèmes de fichiers du pool :

   ```
   # zfs set devices=off auditp/auditf

   # zfs set exec=off auditp/auditf

   # zfs set setuid=off auditp/auditf
   ```

7. **Compressez les fichiers d'audit dans le pool.**

   En règle générale, la compression est définie dans ZFS au niveau du système de fichiers. Toutefois, dans la mesure où tous les systèmes de fichiers présents dans ce pool contiennent les fichiers d'audit, la compression est définie au niveau du jeu de données supérieur du pool.

   ```
   # zfs set compression=on auditp
   ```

   Reportez-vous également à la section " Interactions entre les propriétés de compression, de suppression des doublons et de chiffrement ZFS " du manuel " Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ".

8. **Définissez des quotas.**

   Vous pouvez définir des quotas sur le système de fichiers parent, les systèmes de fichiers descendants, ou les deux. Si vous définissez un quota sur le système de fichiers d'audit parent, les quotas sur les systèmes de fichiers descendants imposent une limite supplémentaire.

   a. **Définissez un quota sur le système de fichiers d'audit parent.**

      Dans l'exemple ci-dessous, lorsque les deux disques dans le pool `auditp` atteignent le quota, le script `audit_warn` notifie l'administrateur de l'audit.

      ```
      # zfs set quota=510G auditp/auditf
      ```

   b. **Définissez un quota sur les systèmes de fichiers d'audit descendants.**

      Dans l'exemple ci-dessous, lorsque le quota pour le système de fichiers `auditp/auditf/`*`system`* est atteint, le script `audit_warn` notifie l'administrateur de l'audit.

      ```
      # zfs set quota=170G auditp/auditf/sys1
      ```

```
# zfs set quota=170G auditp/auditf/sys1.1

# zfs set quota=165G auditp/auditf/sys1.2
```

9. **Pour un grand pool, limitez la taille des fichiers d'audit.**

   Par défaut, un fichier d'audit peut atteindre la taille du pool. Pour faciliter la gestion, limitez la taille des fichiers d'audit. Voir l'Exemple 4-3, “Limitation de la taille des fichiers pour le plug-in `audit_binfile`”.

Exemple 4-1 Création d'un système de fichiers chiffré pour les fichiers d'audit

Afin d'être en conformité avec les exigences de sécurité du site, l'administrateur effectue les opérations suivantes :

1. Crée si nécessaire un nouveau pool ZFS pour stocker les journaux d'audit chiffrés.
2. Génère une clé de chiffrement.
3. Crée le système de fichiers d'audit avec le chiffrement activé pour stocker les journaux d'audit et définit le point de montage.
4. Configure l'audit de façon à utiliser le répertoire chiffré.
5. Actualise le service d'audit pour appliquer les nouveaux paramètres de configuration.

```
# zpool create auditp mirror disk1 disk2


# pktool genkey keystore=file outkey=/filename keytype=aes keylen=256

# zfs create -o encryption=aes-256-ccm \
-o keysource=raw,file:///filename \
-o compression=on -o mountpoint=/audit auditp/auditf

# auditconfig -setplugin audit_binfile p_dir=/audit/

# audit -s
```

Vous devez sauvegarder et protéger le fichier contenant la clé, comme par exemple le *filename* dans l'exemple.

Lorsque l'administrateur crée d'autres systèmes de fichiers sous le système de fichiers `auditf`, ces systèmes de fichiers descendants sont également chiffrés.

Exemple 4-2 Définition d'un quota sur le répertoire `/var/audit`

Dans cet exemple, l'administrateur définit un quota sur le système de fichiers d'audit par défaut. Lorsque ce quota est atteint, le script `audit_warn` avertit l'administrateur de l'audit.

```
# zfs set quota=252G rpool/var/audit
```

Affectation de l'espace d'audit pour la piste d'audit

Dans cette procédure, vous utilisez des attributs pour le plug-in `audit_binfile` pour affecter plus d'espace sur le disque à la piste d'audit.

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

1. **Déterminez les attributs du plug-in `audit_binfile`.**

   Lisez la section `OBJECT ATTRIBUTES` de la page de manuel `audit_binfile`(5).

   ```
   # man audit_binfile

   ...
   OBJECT ATTRIBUTES
   The p_dir attribute specifies where the audit files will be created.
   The directories are listed in the order in which they are to be used.

   The p_minfree attribute defines the percentage of free space that the
   audit system requires before the audit daemon invokes the audit_warn
   script.

   The p_fsize attribute defines the maximum size that an audit
   file can become before it is automatically closed and a new
   audit file is opened. ... The format of the p_fsize value can
   be specified as an exact value in bytes or in a human-readable
   form with a suffix of  B,  K, M, G, T, P, E, Z (for bytes,
   kilobytes, megabytes, gigabytes, terabytes,  petabytes, exabytes,
   or zettabytes, respectively). Suffixes of KB, MB, GB, TB, PB, EB,
   and ZB are also accepted.
   ```

2. **Pour ajouter des répertoires à la piste d'audit, spécifiez l'attribut `p_dir`.**

   Le système de fichiers par défaut est `/var/audit`.

   ```
   # auditconfig -setplugin audit_binfile p_dir=/audit/sys1.1,/var/audit
   ```

   La commande ci-dessus définit le système de fichiers `/audit/sys1.1` en tant que répertoire principal pour les fichiers d'audit et le système de fichiers par défaut `/var/audit` en tant que répertoire secondaire. Dans ce scénario, `/var/audit` est le répertoire de dernier recours. Pour que cette configuration réussisse, le système de fichiers `/audit/sys1.1` doit exister.

Vous avez créé un système de fichiers similaire à la section “Création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 78.

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

   La commande `auditconfig -setplugin` définit la valeur *configurée*. Cette valeur est une propriété du service d'audit, de sorte qu'elle est restaurée lorsque le service est actualisé ou redémarré. La valeur configurée devient *active* lorsque le service d'audit est actualisé ou redémarré. Pour plus d'informations sur les valeurs configurées et actives, reportez-vous à la page de manuel `auditconfig`(1M).

   ```
   # audit -s
   ```

Exemple 4-3 Limitation de la taille des fichiers pour le plug-in `audit_binfile`

Dans l'exemple suivant, la taille d'un fichier d'audit binaire est définie sur une taille spécifique. La taille est exprimée en méga-octets.

```
# auditconfig -setplugin audit_binfile p_fsize=4M

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1;
```

Par défaut, un fichier d'audit peut augmenter sans limite. Pour créer des fichiers d'audit plus petits, l'administrateur spécifie une limite de taille de fichier de 4 Mo. Le service d'audit crée un nouveau fichier lorsque la limite de taille est atteinte. La limite de taille de fichier entre en vigueur une fois le service d'audit actualisé par l'administrateur.

```
# audit -s
```

Exemple 4-4 Définition de périodes de rotation des journaux

Dans l'exemple suivant, une limite de temps est définie pour un fichier d'audit. La limite de temps est exprimée en heures, jours, semaines, mois ou années.

```
# auditconfig -setplugin audit_binfile "p_age=1w"

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_age=1w;
Queue size: 200
```

Par défaut, un fichier d'audit n'a pas de limite de temps. Le fichier reste ouvert indéfiniment jusqu'à ce qu'une opération externe entraîne une rotation de fichier. L'administrateur définit la limite de temps du fichier sur une semaine, au-delà de laquelle un nouveau fichier d'audit est ouvert. Pour implémenter les nouvelles limite de temps, l'administrateur actualise le service d'audit.

```
# audit -s
```

Exemple 4-5 Spécification de plusieurs modifications d'un plug-in d'audit

Dans l'exemple suivant, l'administrateur d'un système doté d'un débit élevé et d'un pool ZFS volumineux modifie la taille de file d'attente, la taille de fichier binaire et l'avertissement de la limite dépassable du plug-in `audit_binfile`. L'administrateur autorise les fichiers d'audit à augmenter jusqu'à 4 Go, est averti lorsqu'il reste 2 % du pool ZFS et double la taille autorisée de la file d'attente. La taille par défaut de la file d'attente correspond au seuil supérieur de la file d'attente d'audit du noyau, `100`, comme dans `active audit queue hiwater mark (records) = 100`. Le fichier d'audit est également défini de façon à avoir une limite de temps de 2 semaines.

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=2G;p_minfree=1;

# auditconfig -setplugin audit_binfile \
      "p_minfree=2;p_fsize=4G;p_age=2w" 200

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;p_age=2w;
Queue size: 200
```

Les spécifications modifiées entrent en vigueur, une fois le service d'audit actualisé par l'administrateur.

```
# audit -s
```

Exemple 4-6 Suppression de la taille de la file d'attente d'un plug-in d'audit

Dans l'exemple suivant, la taille de la file d'attente pour le plug-in `audit_binfile` est supprimée.

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
Queue size: 200

# auditconfig -setplugin audit_binfile "" 0

# auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
```

Les guillemets vides (`""`) conservent les valeurs d'attribut actuelles. Le `0` final définit la taille de la file d'attente pour le plug-in sur la valeur par défaut.

Le changement de la spécification `qsize` pour le plug-in entre en vigueur une fois que l'administrateur a actualisé le service d'audit.

```
# audit -s
```

Exemple 4-7 Définition d'une limite dépassable pour les avertissements

Dans cet exemple, l'espace libre minimum pour tous les systèmes de fichiers d'audit est défini pour qu'un avertissement soit émis lorsque 2 % du système de fichiers restent disponibles.

```
# auditconfig -setplugin audit_binfile p_minfree=2
```

Le pourcentage par défaut est un (1). Pour un pool ZFS volumineux, choisissez un pourcentage raisonnablement faible. Par exemple, 10 % d'un pool de 16 To correspond environ à 16 Go ; l'administrateur de l'audit est averti lorsqu'il reste une grande quantité d'espace sur le disque. La valeur 2 envoie le message `audit_warn` lorsqu'il reste environ 2 Go d'espace sur le disque.

L'alias électronique `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 56.

Pour un pool de grande taille, l'administrateur limite également la taille du fichier à 3 Go.

```
# auditconfig -setplugin audit_binfile p_fsize=3G
```

Les spécifications `p_minfree` et `p_fsize` pour le plug-in entrent en vigueur lorsque l'administrateur actualise le service d'audit.

```
# audit -s
```

▼ Envoi des fichiers d'audit à un référentiel distant

Dans cette procédure, vous utilisez des attributs du plug-in `audit_remote` pour envoyer la piste d'audit à un référentiel d'audit distant. Pour configurer un référentiel distant sur un système Oracle Solaris, reportez-vous à la section “Configuration d'un référentiel distant pour les fichiers d'audit” à la page 87.

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

1. **Déterminez les attributs du plug-in `audit_remote`.**

   Lisez la section `OBJECT ATTRIBUTES` de la page de manuel `audit_remote`(5).

   ```
   # man audit_remote

   ...
   OBJECT ATTRIBUTES
   The p_hosts attribute specifies the remote servers.
   ```

```
You can also specify the port number and the GSS-API
mechanism.

The p_retries attribute specifies the number of retries for
connecting and sending data. The default is 3.

The p_timeout attribute specifies the number of seconds
in which a connection times out.
```

Le port par défaut est le port affecté par l'IANA`solaris_audit`, `16162/tcp`. Le mécanisme par défaut est `kerberos_v5`. Le délai d'attente par défaut est `5` secondes. Vous pouvez également spécifier une taille de file d'attente pour le plug-in.

2. **Pour spécifier le système récepteur distant, utilisez l'attribut `p_hosts`.**

   Dans cet exemple, le système récepteur utilise un autre port.

   ```
   # auditconfig -setplugin audit_remote \
        p_hosts=ars.example.com:16088:kerberos_v5
   ```

3. **Définissez d'autres attributs du plug-in à modifier.**

   Par exemple, la commande suivante indique des valeurs pour tous les attributs facultatifs :

   ```
   # auditconfig -setplugin audit_remote "p_retries=;p_timeout=3" 300
   ```

4. **Vérifiez les valeurs, puis activez le plug-in.**

   Par exemple, les commandes suivantes indiquent et vérifient les valeurs du plug-in :

   ```
   # auditconfig -getplugin audit_remote
   Plugin: audit_remote (inactive)
   Attributes: p_hosts=ars.example.com:16088:kerberos_v5;p_retries=5;p_timeout=3;
   Queue size: 300

   # auditconfig -setplugin audit_remote active
   ```

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

   Le service d'audit lit la modification du plug-in d'audit lors de l'actualisation.

   ```
   # audit -s
   ```

Exemple 4-8 Réglage de la taille de tampon de la file d'attente d'audit

Dans cet exemple, la file d'attente d'audit est saturée derrière le plug-in `audit_remote` . Ce système audité est configuré pour auditer de nombreuses classes et effectue la transmission sur un réseau lent où le trafic est intense. L'administrateur accroît la taille de tampon du plug-in pour permettre l'augmentation de la taille de la file d'attente et éviter le dépassement de la limite du tampon avant que les enregistrements ne soient supprimés de la file.

```
audsys1 # auditconfig -setplugin audit_remote "" 1000
```

```
audsys1 # audit -s
```

Configuration d'un référentiel distant pour les fichiers d'audit

Dans cette procédure, vous devez configurer un système distant, le serveur d'audit à distance (ARS), pour recevoir et stocker des enregistrements d'audit à partir d'un ou de plusieurs systèmes audités. Vous devez ensuite activer le démon d'audit sur le serveur distant.

La configuration se fait en deux temps. Tout d'abord, vous configurez les mécanismes de sécurité sous-jacents pour transporter les données d'audit en toute sécurité, et ce en configurant le KDC. Vous configurez ensuite le service d'audit sur le système d'audit et le serveur ARS. Cette procédure illustre un scénario avec un client audité et un serveur ARS, où ce dernier et le KDC se trouvent sur le même serveur. Des scénarios plus complexes peuvent être configurés de la même manière. Les quatre premières étapes décrivent la configuration du KDC, alors que la dernière étape décrit la configuration du service d'audit.

Avant de commencer

Assurez-vous d'avoir effectué les opérations suivantes. Vous devez prendre le rôle `root`.

- Vous avez pris le rôle `root`.
- Vous avez installé les packages Kerberos, comme décrit à la section “Préparation de la diffusion des enregistrements d'audit vers le stockage distant” à la page 34.
- Vous travaillez avec un administrateur qui a configuré le système audité, comme décrit à la section “Envoi des fichiers d'audit à un référentiel distant” à la page 85.

1. **Si votre site n'a pas encore configuré de KDC, faites-le.**

   Vous avez besoin d'un KDC sur un système que le système audité et le serveur ARS peuvent utiliser, d'un hôte principal pour chaque système et d'un principal de service `audit`. L'exemple ci-dessous illustre une stratégie de configuration de KDC :

   ```
   arstore # kdcmgr -a audr/admin -r EXAMPLE.COM create master
   ```

   Cette commande utilise le principal d'administration `audr/admin` pour créer un KDC maître dans le domaine `EXAMPLE.COM`, active le KDC maître et démarre le service Kerberos.

2. **Vérifiez que le KDC est disponible.**

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

   ```
   # kdcmgr status

   KDC Status Information
   ------------------------------------------
   svc:/network/security/krb5kdc:default (Kerberos key distribution center)
   State: online since Wed Feb 29 01:59:27 2012
   ```

```
See: man -M /usr/share/man -s 1M krb5kdc
See: /var/svc/log/network-security-krb5kdc:default.log
Impact: None.

KDC Master Status Information
-----------------------------------------
svc:/network/security/kadmin:default (Kerberos administration daemon)
State: online since Wed Feb 29 01:59:28 2012
See: man -M /usr/share/man -s 1M kadmind
See: /var/svc/log/network-security-kadmin:default.log
Impact: None.

Transaction Log Information
-----------------------------------------

Kerberos update log (/var/krb5/principal.ulog)
Update log dump :
Log version # : 1
Log state : Stable
Entry block size : 2048
Number of entries : 13
First serial # : 1
Last serial # : 13
First time stamp : Wed Feb 29 01:59:27 2012
Last time stamp : Mon Mar 5 19:29:28 2012


Kerberos Related File Information
-----------------------------------------
(Displays any missing files)
```

3. Ajoutez le principal de service `audit` au fichier keytab du KDC.

Vous pouvez ajouter le principal en tapant la commande `kadmin.local` sur le système KDC. Vous pouvez également ajouter le principal à distance en tapant la commande `kadmin` et en fournissant un mot de passe. Dans cet exemple, le système `arstore` exécute le KDC.

```
# kadmin -p audr/admin

kadmin: addprinc -randkey audit/arstore.example.com@EXAMPLE.COM

kadmin: ktadd audit/arstore.example.com@EXAMPLE.COM
```

4. Sur chaque système audité, ajoutez des clés.

Le récepteur et l'expéditeur doivent disposer de clés.

```
enigma # kclient

.. Enter the Kerberos realm:
EXAMPLE.COM

.. KDC hostname for the above realm:
arstore.example.com
```

```
.. Will this client need service keys ? [y/n]:
y
```

5. **Configurez le service d'audit sur le serveur ARS.**

   - **Pour créer un groupe qui accepte les enregistrements d'audit de n'importe quel système audité dans le domaine Kerberos, nommez un groupe de connexion.**

     ```
     # auditconfig -setremote group create Bank_A
     ```

     `Bank_A` est un groupe de connexion. Dans la mesure où l'attribut `hosts` n'est pas défini, ce groupe accepte toutes les connexions, ce qui signifie qu'il s'agit d'un groupe de *caractères génériques*. Dans le domaine Kerberos, tous les systèmes audités peuvent atteindre ce serveur ARS à condition que leur plug-in `audit_remote` soit correctement configuré.

   - **Pour limiter les connexions à ce groupe, indiquez les systèmes audités pouvant utiliser ce référentiel.**

     ```
     # auditconfig -setremote group Bank_A "hosts=enigma.example.com"
     ```

     Le groupe de connexion `Bank_A` accepte désormais uniquement les connexions à partir du système `enigma`. Une connexion depuis tout autre hôte est refusée.

   - **Pour limiter la taille d'un fichier d'audit de ce groupe, définissez une taille maximale.**

     ```
     # auditconfig -setremote group Bank_A "binfile_fsize=4GB"

     # auditconfig -getremote
     Audit Remote Server
     Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;
     Connection group: Bank_A (inactive)
     Attributes: binfile_dir=/var/audit;binfile_fsize=4GB;binfile_minfree=1;
     hosts=enigma.example.com;
     ```

6. **Configurez le service d'audit sur le système audité.**

   Pour spécifier le serveur ARS, utilisez l'attribut `p_hosts`.

   ```
   enigma # auditconfig -setplugin audit_remote \
        active p_hosts=arstore.example.com

   enigma # auditconfig -getplugin audit_remote
   Plugin: audit_remote
   Attributes: p_retries=3;p_timeout=5;p_hosts=arstore.example.com;
   ```

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

   Le service d'audit lit la modification du plug-in d'audit lors de l'actualisation.

```
# audit -s
```

Le KDC gère désormais la connexion entre le système audité `enigma` et le serveur ARS.

Exemple 4-9 Transmission des enregistrements d'audit vers des emplacements de fichiers différents sur le même serveur ARS

Cet exemple complète l'exemple présenté dans la procédure. L'administrateur sépare les enregistrements d'audit par hôte sur le serveur ARS en créant deux groupes de connexion.

Les fichiers d'audit de `audsys1` sont transmis au groupe de connexion `Bank_A` sur ce serveur ARS.

```
arstore # auditconfig -setremote group create Bank_A

arstore # auditconfig -setremote group active Bank_A "hosts=audsys1" \
   "hosts=audsys1;binfile_dir=/var/audit/audsys1;binfile_fsize=4M;"
```

Les fichiers d'audit de `audsys2` sont transmis au groupe de connexion `Bank_B`.

```
arstore # auditconfig -setremote group create Bank_B

arstore # auditconfig -setremote group active Bank_B \
"hosts=audsys2;binfile_dir=/var/audit/audsys2;binfile_fsize=4M;"
```

Pour simplifier la maintenance, l'administrateur définit les autres valeurs d'attribut de manière identique.

```
arstore # auditconfig -getremote
Audit Remote Server
Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;

Connection group: Bank_A
Attributes: binfile_dir=/var/audit/audsys1;binfile_fsize=4M;binfile_minfree=1;
hosts=audsys1

Connection group: Bank_B
Attributes: binfile_dir=/var/audit/audsys2;binfile_fsize=4M;binfile_minfree=1;
hosts=audsys2
```

Exemple 4-10 Placement du serveur ARS sur un système autre que le KDC

Dans cet exemple, l'administrateur place le serveur ARS sur un système autre que le KDC. Tout d'abord, l'administrateur crée et configure le KDC maître.

```
kserv # kdcmgr -a audr/admin -r EXAMPLE.COM create master

kserv # kadmin.local -p audr/admin

kadmin: addprinc -randkey \
audit/arstore.example.com@EXAMPLE.COM
```

```
kadmin: ktadd -t /tmp/krb5.keytab.audit \
     audit/arstore.example.com@EXAMPLE.COM
```

Après avoir transmis le fichier /tmp/krb5.keytab.audit au serveur ARS de manière sécurisée, arstore, l'administrateur déplace le fichier vers l'emplacement approprié.

```
arstore # chown root:root krb5.keytab.audit

arstore # chmod 600 krb5.keytab.audit

arstore # mv krb5.keytab.audit /etc/krb5/krb5.keytab
```

Au lieu de réécrire le fichier, l'administrateur a également la possibilité d'utiliser la commande ktutil sur le serveur ARS pour fusionner le fichier krb5.keytab.audit du KDC avec les clés existantes du fichier /etc/krb5/krb5.keytab de arstore.

Enfin, l'administrateur génère les clés sur le système audité.

```
enigma # kclient

.. Enter the Kerberos realm: EXAMPLE.COM

.. KDC hostname for the above realm: kserv.example.com

.. Will this client need service keys ? [y/n]: y
```

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 l'utilitaire syslog. Si vous enregistrez les résumés de type texte et de type données d'audit binaires, les données binaires fournissent un enregistrement d'audit complet, tandis que les résumés filtrent les données pour examen en temps réel.

Avant de commencer Pour configurer le plug-in audit_syslog, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Configuration (configuration d'audit). Pour configurer l'utilitaire syslog et créer le fichier auditlog, vous devez prendre le rôle root.

1. Sélectionnez les classes d'audit à envoyer au plug-in audit_syslog et activez le plug-in.

Remarque - Les classes d'audit p_flags doivent être présélectionnées en tant que valeurs par défaut du système ou dans les indicateurs d'audit d'un utilisateur ou d'un profil de droits. Les enregistrements ne sont pas collectés pour une classe qui n'est pas présélectionnée.

```
# auditconfig -setplugin audit_syslog \
     active p_flags=lo,+as,-ss
```

2. **Configurez l'utilitaire `syslog`.**

   a. **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
   ```

   b. **Créez le fichier journal.**

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

   c. **Définissez les droits d'accès au fichier journal à 640.**

   ```
   # chmod 640 /var/adm/auditlog
   ```

   d. **Vérifiez l'instance de service system-log en cours d'exécution sur le système.**

   ```
   # svcs system-log

   STATE        STIME      FMRI
   online       Nov_27     svc:/system/system-log:default
   disabled     Nov 27     svc:/system/system-log:rsyslog
   ```

   e. **Actualisez les informations de configuration de l'instance de service `syslog` active.**

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

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

   ```
   # audit -s
   ```

4. **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 4-11 Spécification des classes d'audit pour la sortie `syslog`

Dans l'exemple suivant, l'utilitaire `syslog` collecte un sous-ensemble des classes d'audit présélectionnées. La classe `pf` est créée dans l'Exemple 3-15, “Création d'une nouvelle classe d'audit”.

```
# auditconfig -setnaflags lo,na
```

```
# auditconfig -setflags lo,ss

# usermod -K audit_flags=pf:no jdoe

# auditconfig -setplugin audit_syslog \
    active p_flags=lo,+na,-ss,+pf
```

Les arguments de la commande `auditconfig` demandent au système de recueillir tous les enregistrements d'audit de connexion/déconnexion, non attribuables et de modification de l'état du système. L'entrée de plug-in `audit_syslog.` demande à l'utilitaire `syslog` de recueillir toutes les connexions, les événements non attribuables ayant réussi et les modifications de l'état du système ayant échoué.

Pour l'utilisateur `jdoe`, l'utilitaire binaire collecte les appels à la commande `pfexec` ayant réussi et ayant échoué. L'utilitaire `syslog` collecte les appels réussis à la commande `pfexec`.

Exemple 4-12 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 `sys1.1`. Le système distant est `remote1`.

```
sys1.1 # 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
```

♦ ♦ ♦ CHAPITRE 5

Utilisation des données d'audit

Ce chapitre fournit les procédures pour vous aider sur les données d'audit générées à partir de plusieurs systèmes locaux. Ce chapitre comprend les sections suivantes :

- “Affichage des données de la piste d'audit” à la page 95
- “Gestion des enregistrements d'audit sur les systèmes locaux” à la page 103

En outre, les chapitres suivants décrivent d'autres tâches de gestion d'audit :

- Chapitre 3, Gestion du service d'audit
- Chapitre 4, Surveillance de l'activité du système
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Pour obtenir une présentation générale du service d'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Affichage des données de la piste d'audit

Le plug-in par défaut `audit_binfile` crée une piste d'audit. La piste peut contenir de grandes quantités de données. Les sections suivantes expliquent comment utiliser ces données.

Affichage des définitions d'enregistrement d'audit

Pour afficher des définitions d'enregistrements d'audit, utilisez la commande. `auditrecord`. Les définitions fournissent le nombre d'événements d'audit, la classe d'audit, le masque de sélection et le format d'enregistrement d'un événement d'audit.

```
% auditrecord -options
```

La sortie d'écran générée par la commande varie selon l'option que vous ajoutez, comme indiqué dans la liste partielle ci-dessous.

- L'option `-p` affiche les définitions d'enregistrements d'audit d'un programme.

- L'option -c affiche les définitions d'enregistrements d'audit d'une classe d'audit.
- L'option -a répertorie toutes les définitions d'événements d'audit.

Vous pouvez également imprimer la sortie affichée dans un fichier.

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

EXEMPLE 5-1 Affichage des définitions d'enregistrement d'audit d'un programme

Dans cet exemple, la définition de tous les enregistrements d'audit générés par le programme `login` est affichée. Les programmes de connexion incluent `rlogin`, `telnet`, `newgrp` et la fonction Shell sécurisé de Oracle Solaris.

```
% auditrecord -p login
...
login: logout
program     various              See login(1)
event ID    6153                 AUE_logout
class       lo                  (0x0000000000001000)
...
newgrp
program     newgrp               See newgrp login
event ID    6212                 AUE_newgrp_login
class       lo                  (0x0000000000001000)
...
rlogin
program     /usr/sbin/login      See login(1) - rlogin
event ID    6155                 AUE_rlogin
class       lo                   (0x0000000000001000)
...
/usr/lib/ssh/sshd
program     /usr/lib/ssh/sshd    See login - ssh
event ID    6172                 AUE_ssh
class       lo                   (0x0000000000001000)
...
telnet login
program     /usr/sbin/login      See login(1) - telnet
event ID    6154                 AUE_telnet
class       lo                   (0x0000000000001000)
…
```

EXEMPLE 5-2 Affichage des définitions d'enregistrement d'audit d'une classe d'audit

Dans cet exemple, les définitions de tous les enregistrements d'audit dans la classe `pf` qui a été créée dans l'Exemple 3-15, “Création d'une nouvelle classe d'audit” s'affichent.

```
% auditrecord -c pf
pfexec
system call pfexec               See execve(2) with pfexec enabled
```

```
event ID    116                 AUE_PFEXEC
class       pf                  (0x0100000000000000)
header
path                    pathname of the executable
path                    pathname of working directory
[privileges]            privileges if the limit or inheritable set are changed
[privileges]            privileges if the limit or inheritable set are changed
[process]               process if ruid, euid, rgid or egid is changed
exec_arguments
[exec_environment]      output if arge policy is set
subject
[use_of_privilege]
return
```

Le jeton `use_of_privilege` est enregistré lorsque le privilège est utilisé. Les jetons `privileges` sont enregistrés si la limite ou l'ensemble héritable sont modifiés. Le jeton `processus` est enregistré si un ID est modifié. Aucune option de stratégie n'est requise pour que ces jetons soient inclus dans l'enregistrement.

EXEMPLE 5-3 Impression dans un fichier des définitions d'enregistrement d'audit

Dans cet exemple, l'option `-h` est ajoutée pour placer toutes les définitions d'enregistrements d'audit dans un fichier au format HTML. Lorsque vous affichez le fichier HTML dans un navigateur, utilisez l'outil de recherche du navigateur pour rechercher des définitions d'enregistrements d'audit spécifiques.

```
% auditrecord -ah > audit.events.html
```

Sélection des événements d'audit à afficher

En tant qu'administration disposant du profil de droits Audit Review (vérification d'audit), vous pouvez filtrer les enregistrements d'audit pour les examiner à l'aide de la commande `auditreduce`. Cette commande peut éliminer les enregistrements moins intéressants, car elle combine les fichiers d'entrée.

auditreduce -*option argument* **[***optional-file***]**

où *argument* correspond à l'argument dont une option a besoin.

La liste suivante répertorie les options de *sélection d'enregistrements* et leurs arguments correspondants :

`-c` Sélectionne une classe d'audit où *argument* correspond à une classe d'audit, telle que `ua`.

`-d` Sélectionne tous les événements à une date donnée. Le format de date pour *argument* est *yyymmdd*. D'autres options de date, telles que `-b` et

-a, sélectionnent les événements avant et après une date particulière, respectivement.

`-u` Sélectionne tous les événements attribuables à un utilisateur particulier. Pour cette option, indiquez un nom d'utilisateur. Une autre option utilisateur, `-e`, sélectionne tous les événements attribuables à un ID d'utilisateur effectif.

`-g` Sélectionne tous les événements attribuables à un groupe particulier. Pour cette option, indiquez un nom de groupe.

`-c` Sélectionne tous les événements d'une classe d'audit présélectionnée. Pour utiliser cette option, indiquez un nom de classe d'audit.

`-m` Sélectionne toutes les instances d'un événement d'audit.

`-o` Sélectionne par type d'objet. Utilisez cette option pour sélectionner par fichier, groupe, propriétaire de fichiers, FMRI, PID et autres types d'objets.

optional-file Nom d'un fichier d'audit.

La commande utilise également les options de *sélection de fichiers* qui sont toutes en majuscules comme indiqué dans les exemples suivants. Pour obtenir la liste complète des options, reportez-vous à la page de manuel `auditreduce`(1M).

EXEMPLE 5-4 Association et réduction des fichiers d'audit

Dans cet exemple, seuls les enregistrements de connexion et déconnexion des fichiers d'audit datant de plus d'un mois sont conversés. L'exemple part du principe que la date actuelle est le 27 septembre. Si vous avez besoin de récupérer la piste d'audit complète, vous pouvez le faire à partir d'un média de sauvegarde. L'option `-O` oriente la sortie de la commande vers un fichier nommé `lo.summary`.

```
# cd /var/audit/audit_summary
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

EXEMPLE 5-5 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 de connexion. L'option `-O` oriente la sortie vers le fichier `tamiko`.

```
# cd /var/audit/audit_summary
# auditreduce -e tamiko -O tamiko
```

Vous pouvez affiner davantage les informations affichées. Dans l'exemple suivant, les éléments suivants sont filtrés et imprimés dans un fichier nommé. `tamikolo`.

- Heure de connexion et déconnexion de l'utilisateur indiquée par l'option `-c`.
- Date du 7 septembre 2013 indiquée par l'option `-d`. La forme abrégée de la date est *yyyymmdd*.
- Nom d'utilisateur tamiko indiqué par l'option `-u`.
- Nom de l'ordinateur indiqué par l'option `-M`.

```
# auditreduce -M tamiko -O tamikolo -d 20130907 -u tamiko -c lo
```

EXEMPLE 5-6 Fusion des enregistrements sélectionnés dans un fichier unique

Dans cet exemple, les enregistrements de connexion et déconnexion pour un jour particulier sont sélectionnés dans la piste d'audit. Les enregistrements sont fusionnés dans un fichier cible. Le fichier cible est écrit dans un système de fichiers autre que le système de fichiers qui contient le répertoire root d'audit.

```
# auditreduce -c lo -d 20130827 -O /var/audit/audit_summary/logins

# ls /var/audit/audit_summary/*logins
/var/audit/audit_summary/20130827183936.20130827232326.logins
```

Affichage du contenu des fichiers d'audit binaires

En tant qu'administrateur disposant du profil de droits Audit Review (vérification d'audit), vous pouvez afficher le contenu de fichiers d'audit binaires à l'aide de la commande `praudit`.

```
# praudit options
```

La liste suivante répertorie quelques-unes des options. Vous pouvez combiner l'une de ces options avec l'option `-l` pour afficher chaque enregistrement sur une seule ligne.

`-s` Affiche les enregistrements d'audit dans un format court, un jeton par ligne.

`-r` Affiche les enregistrements d'audit au format brut, un jeton par ligne.

`-x` Affiche les enregistrements d'audit au format XML, un jeton par ligne. Cette option est utile pour un traitement supplémentaire.

Vous pouvez également utiliser les commandes `auditreduce` et `praudit` en envoyant la sortie `praudit` à partir de la commande `auditreduce`.

EXEMPLE 5-7 Affichage des enregistrements d'audit dans un format court

Dans cet exemple, les événements de connexion et de déconnexion extraits par la commande `auditreduce` s'affichent dans un format court.

```
# auditreduce -c lo | praudit -s

header,69,2,AUE_screenlock,,mach1,2010-10-14 08:02:56.348 -07:00
subject,jdoe,root,staff,jdoe,staff,856,50036632,82 0 mach1
return,success,0
sequence,1298
```

EXEMPLE 5-8 Affichage des enregistrements d'audit dans un format brut

Dans cet exemple, les événements de connexion et de déconnexion extraits par la commande `auditreduce` s'affichent dans un format brut.

```
# auditreduce -c lo | praudit -r

21,69,2,6222,0x0000,10.132.136.45,1287070091,698391050
36,26700,0,10,26700,10,856,50036632,82 0 10.132.136.45
39,0,0
47,1298
```

EXEMPLE 5-9 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
```

De même, vous pouvez afficher les enregistrements d'audit filtrés par la commande `auditreduce` au format XML.

```
# auditreduce -c lo | praudit -x
<record version="2" event="screenlock - unlock" host="mach1"
iso8601="2010-10-14 08:28:11.698 -07:00">
<subject audit-uid="jdoe" uid="root" gid="staff" ruid="jdoe
rgid="staff" pid="856" sid="50036632" tid="82 0 mach1"/>
<return errval="success" retval="0"/>
<sequence seq-num="1298"/>
</record>
```

Le contenu du fichier peut être exécuté par un script pour extraire les informations pertinentes.

EXEMPLE 5-10 Rendre les enregistrements d'audit au format XML lisibles dans un navigateur

Vous pouvez reformater les enregistrements du fichier XML pour pouvoir les lire quel que soit le navigateur à l'aide de l'outil `xsltproc`. Cet outil applique des définitions de style au contenu du fichier. Pour placer le contenu reformaté dans un autre fichier, saisissez ce qui suit :

```
# auditreduce -c lo | praudit -x | xsltproc - > logins.html
```

Dans un navigateur, le contenu de `logins.html` s'affiche dans un format semblable à ce qui suit :

```
                    Audit Trail Data

File: time: 2013-11-04 12:54:28.000 -08:00

Event: login - local
time: 2013-11-04 12:54:28.418 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: jdoe gid: staff ruid: jdoe rgid: staff
      pid: 1534 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: connect to RAD
time: 2013-11-04 12:54:52.029 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: jdoe gid: staff ruid: jdoe rgid: staff
      pid: 1835 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: role login
time: 2013-11-08 08:42:52.286 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: root gid: root ruid: root rgid: root
      pid: 4265 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: role logout
time: 2013-11-08 08:43:37.125 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jdoe uid: root gid: root ruid: root rgid: root
      pid: 4265 sid: 3583012893 tid: 0 0 host
RETURN errval: success retval: 0

Event: login - ssh
time: 2013-12-23 12:24:37.292 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: jsmith gid: staff ruid: jsmith rgid: staff
      pid: 2002 sid: 39351741 tid: 14632 202240 host.example.com
RETURN errval: success retval: 0

Event: role login
time: 2013-12-23 12:25:07.345 -08:00 vers: 2 mod: fe host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2023 sid: 39351741 tid: 14632 202240 host.example.com
RETURN errval: failure retval: Permission denied

Event: su
time: 2013-12-23 17:19:24.031 -08:00 vers: 2 mod: na host: host
RETURN errval: success retval: 0

Event: su logout
time: 2013-12-23 17:19:24.362 -08:00 vers: 2 mod: na host: host
RETURN errval: success retval: 0

Event: login - ssh
```

```
time: 2013-12-23 17:27:21.306 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: jsmith gid: staff ruid: jsmith rgid: staff
      pid: 2583 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0

Event: role login
time: 2013-12-23 17:27:28.361 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2593 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0

Event: role logout
time: 2013-12-23 17:30:39.029 -08:00 vers: 2 mod: host: host
SUBJECT audit-uid: jsmith uid: root gid: root ruid: root rgid: root
      pid: 2593 sid: 3401970889 tid: 13861 5632 host.example.com
RETURN errval: success retval: 0
```

Other events

EXEMPLE 5-11 Affichage des enregistrements `pfedit` uniquement

Vous pouvez utiliser des filtres pour extraire et visualiser uniquement les enregistrements dans la piste d'audit spécifique. Dans cet exemple, les enregistrements qui capturent l'utilisation de la commande `pfedit` sont filtrés. Supposons que le fichier de résumé soit `20130827183936.20130827232326.logins`. L'utilisation de la commande `pfedit` génère l'événement `AUE_admin_edit`. Par conséquent, pour extraire des enregistrements `pfedit`, exécutez la commande suivante :

```
auditreduce -m AUE_admin_edit 20130827183936.20130827232326.logins | praudit
```

EXEMPLE 5-12 Impression de la piste d'audit complète

A l'aide d'un tube sur la commande d'impression, la sortie de la piste d'audit complète est dirigée vers l'imprimante. Pour des raisons de sécurité, l'imprimante a un accès limité.

```
# auditreduce | praudit | lp -d example.protected.printer
```

EXEMPLE 5-13 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/logins

# praudit 20100827183936.20100827232326.logins | more
```

EXEMPLE 5-14 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 par exemple 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
#  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.

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.sys1.1 to stdin.
```

Exécutez la commande `praudit` dans un shell de profil. Vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Review (vérification d'audit). Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Gestion des enregistrements d'audit sur les systèmes locaux

La liste des tâches suivante présente les procédures de sélection, d'analyse et de gestion des enregistrements d'audit.

TABLEAU 5-1 Liste des tâches de gestion des enregistrements d'audit sur les systèmes locaux

Tâche	Description	Pour obtenir des instructions
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 104
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 106
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 107

▼ Fusion des fichiers d'audit de la piste d'audit

En fusionnant les fichiers d'audit de tous les répertoires d'audit, vous pouvez analyser le contenu de la piste d'audit entière.

Remarque - Dans la mesure où les horodatages de la piste d'audit sont définis en temps universel (UTC), la date et l'heure doivent être converties au 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`.

Avant de commencer

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

1. Créez un système de fichiers pour stocker les fichiers d'audit fusionnés.

Afin de diminuer les risques d'atteindre la limite d'espace disque, ce système de fichiers doit se trouver dans un *zpool différent* des systèmes de fichiers que vous avez créés à la section “Création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 78 pour stocker les fichiers d'origine.

2. Fusionnez les enregistrements d'audit de la piste d'audit.

Accédez au répertoire de stockage des fichiers d'audit. A partir de ce répertoire, fusionnez les enregistrements d'audit dans un fichier nommé avec un suffixe. Tous les répertoires dans la piste d'audit sur le système local sont fusionnés et sont placés dans ce répertoire.

```
# cd audit-storage-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.
`-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.
`-R` *pathname*	Indique que les fichiers d'audit doivent être lus dans *pathname*, un autre répertoire root d'audit.
`-S` *server*	Indique que les fichiers d'audit doivent être lus à partir du serveur spécifié.

Pour obtenir la liste complète des options, reportez-vous à la page de manuel `auditreduce`(1M).

Exemple 5-15 Copie des fichiers d'audit pour un fichier résumé

Dans l'exemple ci-dessous, un administrateur à qui est affecté le profil de droits System Administrator (administrateur système) copie tous les fichiers de la piste d'audit dans un fichier fusionné sur un système de fichiers différent. Le système de fichiers `/var/audit/storage` réside sur un disque distinct du système de fichiers `/var/audit`, le système de fichiers root d'audit.

```
$ cd /var/audit/storage
$ auditreduce -A -O All
$ ls /var/audit/storage/*All
20100827183214.20100827215318.All
```

Dans l'exemple suivant, seuls les fichiers complets sont copiés de la piste d'audit dans un fichier fusionné. Le chemin d'accès complet est spécifié comme valeur de l'option `-0`. Le dernier composant du chemin, `Complete`, est utilisé comme suffixe.

```
$ auditreduce -C -O /var/audit/storage/Complete

$ ls /var/audit/storage/*Complete
20100827183214.20100827214217.Complete
```

Dans l'exemple suivant, grâce à l'ajout de l'option `-D`, les fichiers d'audit originaux sont supprimés.

```
$ auditreduce -C -O daily_sys1.1 -D sys1.1
```

```
$ ls *sys1.1
20100827183214.20100827214217.daily_sys1.1
```

▼ Nettoyage d'un fichier d'audit not_terminated

Lorsque des interruptions du système anormales surviennent, le service d'audit s'arrête alors que son fichier d'audit est toujours ouvert. Ou, un système de fichiers devient inaccessible et force le système à passer à un nouveau système de fichiers. 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.

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

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 */* | 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 5-16 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 */* | grep not_terminated
…/egret.1/20100908162220.not_terminated.egret
```

```
…/egret.1/20100827215359.not_terminated.egret

# cd */egret.1
# auditreduce -O egret 20100908162220.not_terminated.egret
# ls -1t
20100908162220.not_terminated.egret      Current audit file

20100827230920.20100830000909.egret      Cleaned-up audit file

20100827215359.not_terminated.egret      Input (old) audit file

# 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, empêchez la perte d'enregistrement d'audit en observant les règles de bonne pratique suivantes.

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

- Définissez une taille libre minimale sur le plug-in `audit_binfile`.

  Utilisez l'attribut `p_minfree`.

  L'alias de messagerie `audit_warn` envoie un avertissement lorsque l'espace disque remplit la taille libre minimale. Voir l'Exemple 4-7, "Définition d'une limite dépassable pour les avertissements".
- Planifiez l'archivage régulier des fichiers d'audit.

  Archivez les fichiers d'audit en sauvegardant les fichiers sur un média 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 au format texte. Pour plus d'informations, reportez-vous à la page de manuel `logadm`(1M).
- Planifiez la suppression des fichiers d'audit archivés du système de fichiers d'audit.
- Enregistrez et stockez les informations auxiliaires.

Archivez les informations nécessaires pour interpréter les enregistrements d'audit ainsi que de la piste d'audit. Au minimum, vous enregistrez les fichiers `passwd`, `group` et `hosts`. Vous pouvez également archiver les fichiers `audit_event` et `audit_class`.

- Consignez les fichiers d'audit qui ont été archivés.
- Stockez correctement le média d'archivage.
- Réduisez la capacité requise du système de fichiers en activant la compression ZFS.

  Sur un système de fichiers ZFS dédié aux fichiers d'audit, la compression réduit la taille des fichiers de manière significative. Pour obtenir un exemple, reportez-vous à la section “Compression des fichiers d'audit sur un système de fichiers dédié” à la page 66.

  Reportez-vous également à la section “ Interactions entre les propriétés de compression, de suppression des doublons et de chiffrement ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”.
- 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 aux Exemple 5-4, “Association et réduction des fichiers d'audit” etExemple 5-6, “Fusion des enregistrements sélectionnés dans un fichier unique”.

♦ ♦ ♦ CHAPITRE 6

Analyse et correction des problèmes de service d'audit

Ce chapitre fournit des procédures pour vous aider à résoudre les problèmes liés à l'audit. En outre, les chapitres suivants décrivent d'autres tâches de gestion d'audit :

- Chapitre 3, Gestion du service d'audit
- Chapitre 4, Surveillance de l'activité du système
- Chapitre 5, Utilisation des données d'audit

Pour obtenir une présentation générale du service d'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour obtenir des informations de référence, reportez-vous au Chapitre 7, Référence d'audit.

Dépannage du service d'audit

Cette section couvre différents messages d'erreur et préférences de l'audit et décrit l'audit proposé par d'autres outils pour vous aider à déboguer les problèmes d'audit.

En général, différents avis sont envoyés pour vous alerter des erreurs du service d'audit. Reportez-vous à votre messagerie et aux fichiers journaux si vous pensez que le service d'audit présente des problèmes.

- Lisez l'e-mail envoyé à l'alias `audit_warn`.

  Le script `audit_warn` envoie des messages d'alerte à l'alias de messagerie `audit_warn`. En l'absence d'un alias configuré correctement, les messages sont envoyés au compte `root`.
- Examinez les fichiers journaux pour le service d'audit.

  La sortie de la commande `svcs -s auditd` indique le chemin d'accès complet aux journaux d'audit que le service d'audit produit.
- Passez en revue les fichiers journaux du système.

  Le script `audit_warn` écrit les messages `daemon.alert` dans le fichier `/var/log/syslog`.

Le fichier `/var/adm/messages` peut contenir des informations.

Après avoir localisé et résolu les problèmes, activez ou redémarrez le service d'audit.

```
# audit -s
```

Les sections suivantes décrivent les problèmes possibles et la manière de les résoudre.

Remarque - Avant d'exécuter une des tâches de dépannage, assurez-vous de disposer de l'autorisation appropriée. Par exemple, pour configurer l'audit, vous devez vous connecter en tant qu'administrateur disposant du profil de droits Audit Configuration (configuration d'audit). Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

Les enregistrements d'audit ne sont pas journalisés

L'audit est activé par défaut. Si vous pensez que l'audit n'a pas été désactivé, mais qu'aucun enregistrement d'audit n'est envoyé au plug-in actif, les raisons peuvent être un ou plusieurs des facteurs abordés dans cette section. Remarque : pour modifier un fichier système, vous devez disposer de l'autorisation `solaris.admin.edit/`*path-to-system-file*. Par défaut, le rôle root dispose de cette autorisation.

Le service d'audit ne fonctionne pas

Pour vérifier si l'audit est en cours d'exécution, utilisez l'une des méthodes suivantes :

- Vérifiez la condition d'audit en cours.

  La sortie suivante indique que l'audit n'est pas en cours d'exécution :

  ```
  # auditconfig -getcond
  audit condition = noaudit
  ```

  La sortie suivante indique que l'audit est en cours d'exécution :

  ```
  # auditconfig -getcond
  audit condition = auditing
  ```

- Assurez-vous que le service d'audit est en cours d'exécution.

  La sortie 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 Sun Oct 10 10:10:10 2010
Reason: Disabled by an administrator.
See: http://support.oracle.com/msg/SMF-8000-05
See: auditd(1M)
See: audit(1M)
See: auditconfig(1M)
See: audit_flags(5)
See: audit_binfile(5)
See: audit_syslog(5)
See: audit_remote(5)
See: /var/svc/log/system-auditd:default.log
Impact: This service is not running.
```

La sortie 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
```

Si le service d'audit n'est pas activé, activez-le. Pour connaître la procédure, reportez-vous à la section “Activation et désactivation du service d'audit” à la page 44.

Aucun plug-in d'audit actif

Utilisez la commande suivante pour vérifier si des plug-ins sont actifs. Au moins un plug-in doit être actif pour que le service d'audit fonctionne.

```
# audit -v
audit: no active plugin found
```

Si aucun plug-in n'est actif, activez-en un.

```
# auditconfig -setplugin audit_binfile active
# audit -v
configuration ok
```

Classe d'audit non définie

Vous tentez peut-être d'utiliser une classe d'audit qui n'a pas été définie. 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 57.

Par exemple, la liste d'indicateurs suivante contient la classe `pf`, que le logiciel Oracle Solaris n'a pas fournie :

```
# auditconfig -getflags
active user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
configured user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
```

Si vous ne souhaitez pas définir la classe, exécutez la commande `auditconfig -setflags` avec des valeurs valides pour réinitialiser les indicateurs actuels. Dans le cas contraire, vérifiez les points suivants lors de la définition d'une classe :

- Vérifiez que la classe est définie dans le fichier `audit_class`.

  ```
  # grep pf /etc/security/audit_class
      Verify class exists

  0x0100000000000000:pf:profile
  ```

- Le masque est unique. S'il n'est pas unique, remplacez le masque.

  ```
  # grep 0x0100000000000000 /etc/security/audit_class
      Ensure mask is unique

  0x0100000000000000:pf:profile
  ```

Aucun événement attribué à la classe d'audit

La classe personnalisée que vous utilisez, bien que définie, peut ne pas avoir d'événement associé.

Pour vérifier si des événements sont affectés à la classe personnalisée, utilisez l'une des méthodes suivantes :

```
# auditconfig -lsevent | egrep " pf|,pf|pf,"
AUE_PFEXEC      116 pf execve(2) with pfexec enabled

# auditrecord -c pf
    List of audit events assigned to pf class
```

Si aucun événement n'est pas affecté à la classe, affectez-y les événements appropriés.

Le volume des enregistrements d'audit est important

Une fois que vous avez déterminé les événements à auditer sur votre site, utilisez les suggestions suivantes pour créer des fichiers d'audit contenant uniquement les informations

dont vous avez besoin. Remarque : pour affecter des indicateurs aux utilisateurs, rôles et profils de droits, vous devez prendre le rôle `root`.

- Evitez en particulier d'ajouter des événements et des jetons d'audit à la piste d'audit. Les stratégies suivantes augmentent la taille de la piste d'audit.

`arge`	Ajoute des variables d'environnement aux événements d'audit `execv`. Même si l'audit des événements `execv` peut coûter cher, l'ajout de variables à l'enregistrement d'audit ne l'est pas.
argv	Ajoute des paramètres de commande aux événements d'audit `execv`. L'ajout des paramètres de commande à l'enregistrement d'audit ne coûte pas cher.
group	Ajoute un jeton de groupe aux événements d'audit qui comprennent un jeton `newgroups` facultatif.
path	Ajoute un jeton `path` aux événements d'audit qui comprennent un jeton `path` facultatif.
public	Si des événements de fichier sont audités, ajoute un événement à la piste d'audit à chaque fois qu'un événement auditable se produit sur un objet 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 concepts de l'audit” à la page 10.
seq	Ajoute un jeton sequence à chaque événement d'audit.
trail	Ajoute un jeton trailer à chaque événement d'audit.
windata_down	Sur un système qui est configuré avec Trusted Extensions, ajoute des événements lorsque les informations d'une fenêtre étiquetée sont rétrogradées.
windata_up	Sur un système qui est configuré avec Trusted Extensions, ajoute des événements lorsque les informations d'une fenêtre étiquetée sont mises à niveau.
zonename	Ajoute le nom de zone à chaque événement d'audit. Si la zone globale est la seule zone configurée, ajoute la chaîne `zone, global` à chaque événement d'audit.

  L'enregistrement d'audit suivant montre l'utilisation de la commande `ls`. La classe `ex` est auditée et la stratégie par défaut est en cours d'utilisation :

```
header,129,2,AUE_EXECVE,,mach1,2010-10-14 11:39:22.480 -07:00
```

```
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
subject,jdoe,root,root,root,root,2404,50036632,82 0 mach1
return,success,0
```

Ci-dessous, le même enregistrement lorsque toutes les stratégies sont activées :

```
header,1578,2,AUE_EXECVE,,mach1,2010-10-14 11:45:46.658 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
exec_env,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLVL=2,
HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8, PRINTER=example-dbl,
...
path,/lib/ld.so.1
attribute,100755,root,bin,21,393073,18446744073709551615
subject,jdoe,root,root,root,root,2424,50036632,82 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,197
trailer,1578
```

- Utilisez le plug-in `audit_syslog` pour envoyer des événements d'audit à `syslog`.

  N'envoyez pas ces événements d'audit au plug-in `audit_binfile` ou `audit_remote`. 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`.

- Définissez moins d'indicateurs d'audit système et d'utilisateurs individuels d'audit.

  Diminuez l'audit pour l'ensemble des utilisateurs en réduisant le nombre de classes d'audit qui font l'objet d'un audit à l'échelle du système.

  Utilisez le mot-clé `audit_flags` pour les commandes `roleadd`, `rolemod`, `useradd` et `usermod` afin d'auditer les événements pour des utilisateurs et des rôles spécifiques. Pour consulter des exemples, reportez-vous à l'Exemple 4-11, “Spécification des classes d'audit pour la sortie `syslog`” et à la page de manuel `usermod`(1M).

  Utilisez les propriétés `always_audit` et `never_audit` de la commande `profiles` afin d'auditer les événements pour des profils de droits spécifiques. Pour plus d'informations, reportez-vous à la page de manuel `profiles`(1).

Remarque - A l'instar d'autres attributs de sécurité, les indicateurs d'audit sont affectés par ordre de recherche. Pour plus d'informations, reportez-vous à la section “ Ordre de recherche pour Assigned Rights ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

- Créez votre propre classe d'audit.

  Vous pouvez créer des classes d'audit sur votre site. Dans ces classes, placez uniquement les événements d'audit qu'il vous faut surveiller. Pour connaître cette procédure, reportez-vous à la section “Ajout d'une classe d'audit” à la page 57.

Remarque - Pour des informations sur les effets de la modification d'un fichier de configuration d'audit, reportez-vous à la section “Fichiers de configuration d'audit et empaquetage” à la page 121.

La taille des fichiers d'audit binaires augmente sans limite

En tant qu'administrateur disposant du profil de droits Audit Review (vérification d'audit), vous pouvez limiter la taille des fichiers binaires pour faciliter l'archivage et la recherche. Vous pouvez également créer des fichiers binaires plus petits à partir du fichier d'origine à l'aide de l'une des options décrites dans cette section.

- Utilisez l'attribut `p_fsize` pour limiter la taille de chaque fichier d'audit binaire.

  Pour obtenir une description de l'attribut `p_fsize`, reportez-vous à la section OBJECT ATTRIBUTES de la page de manuel `audit_binfile`(5).

  Pour consulter un exemple, reportez-vous à l'Exemple 4-3, “Limitation de la taille des fichiers pour le plug-in `audit_binfile`”.
- Utilisez la commande `auditreduce` pour sélectionner des enregistrements et les écrire dans un fichier plus petit pour une analyse plus approfondie.

  Les options `auditreduce` *-lowercase* recherchent des enregistrements spécifiques.

  Les options `auditreduce` *-Uppercase* écrivent vos sélections vers un fichier. Pour plus d'informations, reportez-vous à la page de manuel `auditreduce`(1M). Reportez-vous également à la section “Affichage des données de la piste d'audit” à la page 95.

Connexions à partir d'autres systèmes d'exploitation non soumis à un audit

Le SE Oracle Solaris peut auditer toutes les connexions, quelle que soit la source. Si les connexions ne sont pas en cours d'audit, alors la classe `lo` pour les événements attribuables et non attribuables n'est probablement pas définie. Cette classe audite les connexions, déconnexions et verrouillages d'écran. Ces classes sont soumises à un audit par défaut.

Remarque - Pour effectuer l'audit des connexions `ssh`, votre système doit exécuter le démon `ssh` à partir d'Oracle Solaris. Ce démon est modifié pour le service d'audit sur un système Oracle Solaris. Pour plus d'informations, reportez-vous à la section " Shell sécurisé et OpenSSH " du manuel " Gestion de l'accès au shell sécurisé dans Oracle Solaris 11.2 ".

EXEMPLE 6-1 Vérification de l'audit des connexions

Dans cet exemple, la sortie des deux premières commandes montre que la classe `lo` pour les événements attribuables et non attribuables n'est pas définie. Ensuite, les deux dernières commandes permettent de définir la classe `lo` pour activer l'audit des événements de connexion.

```
# auditconfig -getflags
active user default audit flags = as,st(0x20800,0x20800)
configured user default audit flags = as,st(0x20800,0x20800)

# auditconfig -getnaflags
active non-attributable audit flags = na(0x400,0x400)
configured non-attributable audit flags = na(0x400,0x400)

# auditconfig -setflags lo,as,st
user default audit flags = as,lo,st(0x21800,0x21800)

# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

♦ ♦ ♦ CHAPITRE 7

Référence d'audit

Ce chapitre décrit les éléments importants de l'audit et traite des sujets suivants :

Pour une présentation de l'audit, reportez-vous au Chapitre 1, A propos de l'audit dans Oracle Solaris. Pour obtenir des suggestions de planification, reportez-vous au Chapitre 2, Planification de l'audit. Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous aux chapitres suivants :

- Chapitre 3, Gestion du service d'audit
- Chapitre 4, Surveillance de l'activité du système
- Chapitre 5, Utilisation des données d'audit
- Chapitre 6, Analyse et correction des problèmes de service d'audit

Service d'audit

Le service d'audit, `auditd`, est activé par défaut. Pour savoir comment activer, actualiser ou désactiver le service, reportez-vous à la section “Activation et désactivation du service d'audit” à la page 44.

Sans la configuration du client, les valeurs par défaut suivantes sont en place :

- Tous les événements de connexion font l'objet d'un audit.

  Les tentatives de connexion réussies ou non font l'objet d'un audit.
- Tous les utilisateurs font l'objet d'un audit portant sur les événements de connexion et de déconnexion, y compris la prise du rôle et le verrouillage de l'écran.
- Le plug-in `audit_binfile` est actif. Le répertoire `/var/audit` stocke les enregistrements d'audit, la taille d'un fichier d'audit n'est pas limitée et la taille de la file d'attente est de 100 enregistrements.
- La stratégie `cnt` est définie.

  Lorsque les enregistrements d'audit remplissent l'espace disque disponible, le système effectue le suivi du nombre d'enregistrements d'audit rejetés. Un avertissement est émis lorsqu'il reste 1 % d'espace disponible sur le disque.
- Les contrôles de la file d'attente d'audit suivants sont définis :
  - Nombre maximal d'enregistrements dans la file d'attente d'audit avant la génération des verrouillages des enregistrements : 100
  - Nombre minimal d'enregistrements dans la file d'attente d'audit avant le déblocage des processus d'audit bloqués : 10
  - Taille du tampon pour la file d'attente d'audit : 8 192 octets.
  - Intervalle entre l'écriture des enregistrements d'audit sur la piste d'audit : 20 secondes.

Pour afficher les valeurs par défaut, reportez-vous à la section “Affichage de paramètres par défaut du service d'audit” à la page 42.

Le service d'audit vous permet de définir des valeurs temporaires ou actives Ces valeurs peuvent être différentes des valeurs configurées ou de propriété.

- Les valeurs temporaires ne sont pas restaurées lors de l'actualisation ou du redémarrage du service d'audit.

  La stratégie d'audit et les contrôles de la file d'attente d'audit acceptent les valeurs temporaires. Les indicateurs d'audit ne disposent pas d'une valeur temporaire.
- Les valeurs configurées sont stockées en tant que valeurs de propriété du service, de sorte qu'elles sont restaurées lors de l'actualisation ou du redémarrage du service d'audit.

Les profils de droits contrôlent qui peut administrer le service d'audit. Pour plus d'informations, reportez-vous à la section “Profils de droits pour l'administration de l'audit” à la page 120.

Par défaut, toutes les zones font l'objet d'un audit identique. Reportez-vous à la section “Audit et Oracle Solaris Zones” à la page 121.

Pages de manuel du service d'audit

Le tableau suivant récapitule les pages de manuel d'administration principales pour le service d'audit.

Page de manuel	Résumé
audit(1M)	Commande qui contrôle les actions du service d'audit `audit -n` démarre un nouveau fichier d'audit pour le plug-in `audit_binfile`. `audit -s` active et actualise l'audit. `audit -t` désactive l'audit. `audit -v` vérifie qu'au moins un plug-in est actif.
audit_binfile(5)	Plug-in d'audit par défaut, qui envoie les enregistrements d'audit dans un fichier binaire. Reportez-vous également à la section “Plug-ins d'audit” à la page 123.
audit_remote(5)	Plug-in d'audit qui envoie les enregistrements d'audit à un récepteur distant.
audit_syslog(5)	Plug-in d'audit qui envoie les récapitulatifs au format texte des enregistrements d'audit à l'utilitaire `syslog` .
audit_class(4)	Fichier qui contient les définitions des classes d'audit. Les huit bits d'ordre élevé sont à la disposition des clients pour créer de nouvelles classes d'audit. Pour obtenir plus d'informations sur l'effet de la modification de ce fichier sur la mise à niveau du système, reportez-vous à la section “Ajout d'une classe d'audit” à la page 57.
audit_event(4)	Fichier qui contient les définitions des événements d'audit et mappe les événements avec les classes d'audit. Le mappage peut être modifié. Pour obtenir plus d'informations sur l'effet de la modification de ce fichier sur la mise à niveau du système, reportez-vous à la section “Modification de l'appartenance à une classe d'un événement d'audit” à la page 58.
audit_flags(5)	Décrit la syntaxe de présélection de classe d'audit, les préfixes pour sélectionner uniquement les événements ayant échoué ou ceux ayant réussi, et les préfixes qui modifient une présélection existante.
audit.log(4)	Décrit l'attribution de noms aux fichiers d'audit binaires, la structure interne d'un fichier et la structure de chaque jeton d'audit.
audit_warn(1M)	Script qui notifie à un alias de messagerie une condition inhabituelle rencontrée par le service d'audit 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 indiquer comment gérer ces conditions automatiquement.
auditconfig(1M)	Commande qui extrait et définit les paramètres de configuration d'audit. Emettez cette commande `auditconfig` sans option pour afficher une liste des paramètres qui peuvent être extraits et définis.
auditrecord(1M)	Commande qui affiche la définition d'événements d'audit dans le fichier `/etc/security/audit_event`. Pour obtenir un exemple de sortie, reportez-vous à la section “Affichage des définitions d'enregistrement d'audit” à la page 95.
auditreduce(1M)	Commande qui postsélectionne et fusionne 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. Les enregistrements sont conservés dans un format binaire.

Page de manuel	Résumé
	Les options en majuscules influent sur la sélection des fichiers. Les options en minuscules influent sur la sélection des enregistrements.
auditstat(1M)	Commande qui affiche les statistiques de l'audit du noyau. Par exemple, la commande peut afficher le nombre d'enregistrements figurant dans la file d'attente d'audit du noyau, le nombre d'enregistrements rejetés et le nombre d'enregistrements d'audit que les processus utilisateur ont produit dans le noyau suite aux appels système.
praudit(1M)	Commande qui lit les enregistrements d'audit au 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 ou d'une liste de fichiers d'audit. L'entrée peut également être produite avec la commande `tail -0f` pour un fichier d'audit actuel. Pour obtenir un exemple de sortie, reportez-vous à la section “Affichage du contenu des fichiers d'audit binaires” à la page 99.
syslog.conf(4)	Fichier configuré pour envoyer des résumés au format texte d'enregistrements d'audit à l'utilitaire `syslog` pour le plug-in `audit_syslog`.

Profils de droits pour l'administration de l'audit

Oracle Solaris fournit des profils de droits pour la configuration du service d'audit, l'activation et la désactivation du service et l'analyse de la piste d'audit. Vous devez avoir des privilèges `root` pour modifier un fichier de configuration d'audit.

- **Configuration d'audit :** permet à un administrateur de configurer les paramètres du service d'audit et d'exécuter la commande `auditconfig`.
- **Contrôle d'audit :** permet à un administrateur de démarrer, actualiser et désactiver le service d'audit et d'exécuter la commande `audit` pour démarrer, actualiser ou arrêter le service.
- **Vérification d'audit :** permet à un administrateur d'analyser les enregistrements d'audit. Ce profil de droits accorde l'autorisation de lire les enregistrements d'audit avec les commandes `praudit` et `auditreduce`. Cet administrateur peut également exécuter la commande `auditstat`.
- **Administrateur système :** inclut le profil de droits Audit Review (vérification d'audit). Un administrateur 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 “ Création d’un rôle ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

Audit et Oracle Solaris Zones

Les zones non globales peuvent être auditées exactement comme la zone globale ou définir leurs propres indicateurs, stockage et stratégies d'audit.

Lorsque toutes les zones sont soumises au même audit, les fichiers `audit_class` et `audit_event` dans la zone globale fournissent les mappages classe-événement pour l'audit dans chaque zone. L'option de stratégie `+zonename` est utile pour effectuer la postsélection d'enregistrements par nom de zone.

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 service 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 avec Oracle Solaris Zones” à la page 25 et “Planification de l'audit dans les zones” à la page 28.

Pour plus d'informations sur les zones, reportez-vous à la section “ Présentation d’Oracle Solaris Zones ”.

Fichiers de configuration d'audit et empaquetage

Les fichiers de configuration d'audit dans Oracle Solaris sont marqués dans le package avec l'attribut de package `preserve=renamenew`. Cet attribut conserve toutes les modifications que vous apportez aux fichiers d'une mise à jour à l'autre. Pour des informations sur les effets des valeurs `preserve`, reportez-vous à la page de manuel `pkg` (5).

Ces fichiers de configuration sont marqués avec l'attribut de package `overlay=allow`. Cet attribut vous permet de créer votre propre package qui contient ces fichiers et de remplacer les fichiers Oracle Solaris par les fichiers de votre package. Lorsque vous définissez l'attribut `overlay` sur `true` dans votre package, les sous-commandes `pkg`, telles que `verify`, `fix`, `revert`, etc., retournent des résultats sur vos packages. Pour plus d'informations, reportez-vous aux pages de manuel `pkg`(1) et `pkg`(5).

Classes d'audit

Dans Oracle Solaris, les classes d'audit sont des conteneurs pratiques qui permettent de regrouper un grand nombre d'événements d'audit.

Vous pouvez reconfigurer les classes d'audit et en créer des nouvelles. 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. Pour plus d'informations, reportez-vous à la page de manuel `audit_class`(4) et à la section “Ajout d'une classe d'audit” à la page 57.

Attention - La classe `all` risque de générer de grandes quantités de données d'audit et remplir rapidement les disques. Utilisez la classe `all` uniquement lorsque vous avez des raisons d'auditer toutes les activités.

Syntaxe de classe d'audit

Les événements dans une classe d'audit peuvent être audités en cas de réussite, d'échec ou dans les deux cas.

- 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.
- Pour modifier une présélection actuelle, ajoutez un caret (^) précédant un préfixe ou un indicateur d'audit. Ainsi,
  - Si `ot` est présélectionné pour le système et que la présélection d'un utilisateur est `^ot`, cet utilisateur n'est pas soumis à un audit pour les événements dans la classe `other`.
  - Si `+ot` est présélectionné pour le système et que la présélection d'un utilisateur est `^ +ot`, cet utilisateur n'est pas soumis à un audit pour les événements qui ont réussi dans la classe `other`.
  - Si `-ot` est présélectionné pour le système et que la présélection d'un utilisateur est `^-ot`, cet utilisateur n'est pas soumis à un audit pour les événements qui ont échoué dans la classe `other`.

Pour consulter la syntaxe de présélection de classe d'audit, reportez-vous à la page de manuel `audit_flags`(5).

Les classes d'audit et leurs préfixes peuvent être spécifiés dans les commandes ci-après :

- En tant qu'arguments des options de la commande `auditconfig`, `-setflags` et `-setnaflags`.
- En tant que valeurs de l'attribut `p_flags` du plug-in `audit_syslog`. Vous spécifiez l'attribut en tant qu'option de la commande `auditconfig -setplugin audit_syslog active`.
- En tant que valeurs de l'option `-K audit_flags=`*always-audit-flags*`:`*never-audit-flags* pour les commandes `useradd`, `usermod`, `roleadd` et `rolemod`.

- En tant que valeurs des propriétés -`always_audit` et-`never_audit` de la commande `profiles`.

Plug-ins d'audit

Les plug-ins d'audit indiquent comment traiter les enregistrements d'audit dans la file d'attente d'audit. Les plug-ins d'audit sont spécifiés par nom : `audit_binfile`, `audit_remote` et `audit_syslog`, en tant qu'arguments de la commande `auditconfig -setplugin`. Les plug-ins peuvent être précisés par les attributs suivants :

- Plug-in `audit_binfile`

  Attribut `p_dir` : destination d'envoi des données binaires

  Attribut `p_minfree` : espace minimum restant sur un disque avant la notification à l'administrateur.

  Attribut `p_fsize` : taille maximale d'un fichier d'audit.
- Plug-in `audit_remote`

  Attribut`p_hosts` : serveur d'audit authentifié à distance sur lequel envoyer les données d'audit binaires.

  Attribut `p_retries` : nombre de tentatives d'accès à un serveur d'audit authentifié à distance.

  Attribut `p_timeout` : nombre de secondes entre les tentatives d'accès à un serveur d'audit authentifié à distance.
- Plug-in `audit_syslog`

  Attribut `p_flags` : sélection de résumés au format texte d'enregistrements d'audit à envoyer à `syslog`.
- Pour tous les plug-ins, le nombre maximal d'enregistrements d'audit mis en file d'attente pour le plug-in -attribut `qsize`

Reportez-vous aux pages de manuel `audit_binfile`(5), `audit_remote`(5), `audit_syslog`(5) et `auditconfig`(1M).

Serveur d'audit à distance

Le serveur d'audit à distance (ARS) reçoit les enregistrements d'audit des systèmes d'audit par le biais d'un lien sécurisé et les stocke.

La réception repose sur la configuration suivante :

- Domaine Kerberos avec des principaux d'audit spécifiques et un mécanisme GSS-API
- Serveur ARS avec au minimum un *groupe de connexion* configuré et actif
- Au minimum un système audité dans le groupe de connexion et un plug-in `audit_remote` configuré et actif

Un groupe de connexion est spécifié dans la propriété `group` du serveur ARS. Pour la gestion des fichiers, `group` peut limiter la taille d'un fichier d'audit et spécifier l'espace disponible minimal. La principale raison pour spécifier des groupes de connexion différents est d'indiquer des emplacements de stockage différents sur le serveur ARS, comme le montre l'Exemple 4-9, “Transmission des enregistrements d'audit vers des emplacements de fichiers différents sur le même serveur ARS”.

Pour plus d'informations sur le serveur ARS, reportez-vous à la page de manuel `ars`(5). Pour des informations sur la configuration du serveur ARS, reportez-vous aux options `- setremote` de la page de manuel `auditconfig`(1M).

Pour configurer les systèmes audités, reportez-vous à la page de manuel `audit_remote`(5) et à l'option `-setplugin` dans la page de manuel `auditconfig`(1M).

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 stratégies `windata_down` et `windata_up` sont utilisées par la fonction Trusted Extensions d'Oracle Solaris. Pour plus d'informations, reportez-vous au Chapitre 22, “ TrustedÂ Extensions et audit ” du manuel “ Configuration et administration de Trusted Extensions ”.

Les autres stratégies n'ajoutent pas de jetons. La stratégie `public` limite l'audit des fichiers publics. La stratégie `perzone` établit des files d'attente d'audit distinctes pour les zones non globales. Les stratégies `ahlt` et `cnt` déterminent ce qui se produit lorsque les enregistrements d'audit ne peuvent pas être remis. Pour plus de détails, reportez-vous à la section “Stratégies d'audit des événements asynchrones et synchrones” à la page 125.

Les effets des différentes options de stratégie d'audit sont décrits à la section “Principes de la stratégie d'audit” à la page 35. 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 de stratégie disponibles, exécutez la commande `auditconfig -lspolicy`. Pour obtenir la stratégie en cours, exécutez la commande `auditconfig -getpolicy`.

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.

Remarque - La stratégie `cnt` ou `ahlt` n'est pas déclenchée si la file d'attente d'au moins un plug-in peut accepter des enregistrements d'audit.

Les stratégies `cnt` et `ahlt` sont indépendantes et associées. La combinaison de ces stratégies a les effets suivants :

- `-ahlt +cnt` est la stratégie adoptée par défaut. Cette valeur par défaut permet le traitement d'un événement soumis à un audit même si l'événement ne peut pas être journalisé.

  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 asynchrone 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. 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.

Caractéristiques de l'audit de processus

Lors de la connexion initiale, l'audit est défini selon les caractéristiques suivantes :

- **Masque de présélection de processus :** combinaison du masque d'audit à l'échelle du système et du masque d'audit spécifique à l'utilisateur, si un masque d'audit utilisateur a été spécifié. Lorsqu'un utilisateur se connecte, le processus de connexion combine les classes présélectionnées afin d'établir le *masque de présélection* des processus utilisateur. Le masque de présélection du processus spécifie les événements générant des enregistrements d'audit.

  L'algorithme suivant décrit la façon dont le système obtient le masque de présélection de processus utilisateur :

  `(system-wide default flags  +` *always-audit-classes*`) -` *never-audit-classes*

  Ajoutez les classes d'audit système issues des résultats de la commande `auditconfig -getflags` aux classes issues de la valeur *always-audit-classes* pour le mot-clé `always_audit` de l'utilisateur. Ensuite, du total, soustrayez les classes de la valeur *never-audit-classes* de l'utilisateur. Reportez-vous également à la page de manuel `audit_flags`(5).
- **ID utilisateur d'audit :** un processus acquiert un ID utilisateur d'audit immuable à la connexion de l'utilisateur. Cet ID est hérité par tous les processus enfants qui ont été lancés par le processus initial de l'utilisateur. L'ID utilisateur d'audit permet d'appliquer la responsabilité. Même après qu'un utilisateur prenne un rôle, l'ID utilisateur d'audit reste

le même. L'ID utilisateur d'audit enregistré dans chaque enregistrement d'audit permet de toujours retracer les actions jusqu'à l'utilisateur de connexion.

- **ID de session d'audit :** l'ID de session d'audit est assigné lors de la connexion. Tous les processus enfants héritent de cet ID.
- **ID du terminal :** pour une connexion locale, l'ID du terminal est composé de l'adresse IP du système local, suivie 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 `0,0`. Pour une connexion à distance, l'ID du terminal est constitué de l'adresse IP de l'hôte distant, suivie du numéro du port distant et du numéro du port local.

Piste d'audit

La *piste d'audit* contient les fichiers d'audit binaires. La piste est créée par le plug-in `audit_binfile`. Le service d'audit recueille les enregistrements dans la file d'attente d'audit et les envoie au plug-in, qui les écrit sur le disque.

Conventions relatives aux noms de fichiers d'audit binaires

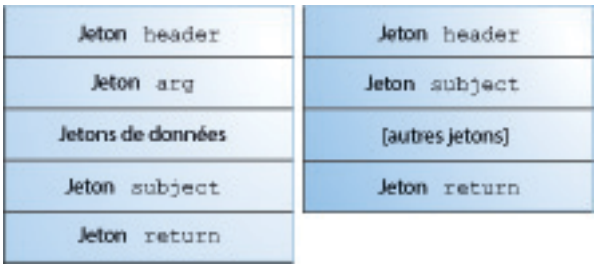
Le plug-in `audit_binfile` crée des fichiers d'audit binaires. Chaque fichier d'audit binaire est un ensemble d'enregistrements autonome. Le nom du fichier identifie l'intervalle de temps pendant lequel les enregistrements ont été générés et le système qui les a générés. Les horodatages indiquant l'intervalle de temps sont exprimés en temps universel (UTC) pour garantir l'ordre correct de triage, même sur plusieurs fuseaux horaires.

Pour plus d'informations, reportez-vous à la page de manuel `audit.log`(4). Pour consulter des exemples de noms de fichiers d'audit ouverts et fermés, reportez-vous à la section “Nettoyage d'un fichier d'audit `not_terminated`” à la page 106.

Structure de l'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 au niveau du noyau et un enregistrement d'audit standard au niveau de l'utilisateur.

FIGURE 7-1 Structures d'enregistrement d'audit standard



Analyse d'enregistrement d'audit

L'analyse d'enregistrement d'audit implique la postsélection des enregistrements dans la piste d'audit. Vous pouvez utiliser l'une des deux approches d'analyse syntaxique des données binaires collectées ci-dessous.

- Vous pouvez exécuter la commande `praudit`. Les options de la commande fournissent une sortie de texte différente. Par exemple, la commande `praudit -x` fournit du XML pour l'entrée dans les scripts et navigateurs. La sortie `praudit` n'inclut pas les champs dont le seul but est d'aider à analyser les données binaires. Notez que l'ordre et le format de la sortie `praudit` peuvent être différents selon la version d'Oracle Solaris.

  Pour obtenir des exemples de sortie `praudit`, reportez-vous à la section “Affichage du contenu des fichiers d'audit binaires” à la page 99.

  Pour obtenir des exemples de sortie `praudit` pour chaque jeton d'audit, reportez-vous aux différents jetons répertoriés dans la section “Formats de jeton d'audit” à la page 129.
- Vous pouvez écrire un programme pour analyser le flux de données binaires. Le programme doit prendre en compte les variantes d'un enregistrement d'audit. Par exemple, l'appel système `ioctl()` crée un enregistrement d'audit pour "Nom de fichier incorrect". Cet enregistrement contient différents jetons de l'enregistrement d'audit `ioctl()` 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).
  - Le fichier `/usr/include/bsm/audit.h` contient des valeurs de manifeste.
  - Pour afficher l'ordre des jetons dans un enregistrement d'audit, utilisez la commande `auditrecord`. La sortie de la commande `auditrecord` inclut les différents jetons des différentes valeurs de manifeste. Les crochets (`[]`) indiquent qu'un jeton

d'audit est facultatif. Pour plus d'informations, reportez-vous à la page de manuel auditrecord(1M).

Formats de jeton d'audit

Chaque jeton d'audit possède un identificateur de type de jeton, suivi de données spécifiques au jeton. 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 7-1 Jetons d'audit pour l'audit

Nom de jeton	Description	Pour plus d'informations
acl	Informations sur l'entrée de contrôle d'accès (ACE, Access Control Entry) et la liste de contrôle d'accès (ACL, Access Control List)	“Jeton acl” à la page 130
arbitrary	Données avec informations de format et de type	Page de manuel audit.log(4)
argument	Valeur de l'argument d'appel système	“Jeton argument” à la page 131
attribute	Informations sur le fichier vnode	“Jeton attribute” à la page 131
cmd	Arguments de commande et variables d'environnement	“Jeton cmd” à la page 131
exec_args	Arguments d'appel système Exec	“Jeton exec_args” à la page 132
exec_env	Variables d'environnement d'appel système Exec	“Jeton exec_env” à la page 132
exit	Informations sur la sortie du programme	Page de manuel audit.log(4)
file	Informations sur le fichier d'audit	“Jeton file” à la page 132
fmri	Identificateur de ressource de gestion de structure	“Jeton fmri” à la page 133
group	Informations sur les groupes de processus	“Jeton group” à la page 133
header	Indique le début de l'enregistrement d'audit	“Jeton header” à la page 133
ip	Informations sur l'en-tête IP	Page de manuel audit.log(4)
ip address	Adresse Internet	“Jeton ip address” à la page 134
ip port	Adresse du port Internet	“Jeton ip port” à la page 134
ipc	Informations sur l'IPC System V	“Jeton ipc” à la page 134
IPC_perm	Informations sur l'accès à l'objet IPC System V	“Jeton IPC_perm” à la page 135
opaque	Données non structurées (format non spécifié)	Page de manuel audit.log(4)
path	Informations relatives aux chemins	“Jeton path” à la page 135
path_attr	Informations relatives aux chemins d'accès	“Jeton path_attr” à la page 135
privilege	Informations sur le jeu de privilèges	“Jeton privilege” à la page 136

Nom de jeton	Description	Pour plus d'informations
`process`	Informations sur le processus	“Jeton `process`” à la page 136
`return`	Statut des appels système	“Jeton `return`” à la page 136
`sequence`	Numéro de séquence	“Jeton `sequence`” à la page 137
`socket`	Types de socket et adresses	“Jeton `socket`” à la page 137
`subject`	Informations sur subject (même format que `process`)	“Jeton `subject`” à la page 137
`text`	Chaîne de caractères ASCII	“Jeton `text`” à la page 138
`trailer`	Indique la fin de l'enregistrement d'audit	“Jeton `trailer`” à la page 138
`use of authorization`	Utilisation d'autorisation	“Jeton `use of authorization`” à la page 138
`use of privilege`	Utilisation de privilège	“Jeton `use of privilege`” à la page 139
`user`	ID utilisateur et nom de l'utilisateur	“Jeton `user`” à la page 139
`xclient`	Identification du client X	“Jeton `xclient`” à la page 139
`zonename`	Nom de la zone	“Jeton `zonename`” à la page 139
Jetons Trusted Extensions	Informations sur le système Window X et `label`	“ Référence de l’audit TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”

Les jetons suivants sont obsolètes :

- `liaison`
- `host`
- `tid`

Pour plus d'informations sur les jetons obsolètes, reportez -vous au matériel de référence de la version qui inclut le jeton.

Un enregistrement d'audit commence toujours par un jeton `header` indique l'emplacement vers lequel 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` utilise différents formats d'enregistrement d'informations sur ACE (Access Control Entries) pour un système de fichiers ZFS et sur ACL (Access Control Lists) pour un système de fichiers UFS hérité.

Lorsque le jeton `acl` est enregistré pour un système de fichiers UFS, la commande `praudit -x` affiche les champs comme suit :

```
<acl type="1" value="root" mode="6"/>
```

Lorsque le jeton `acl` est enregistré pour un jeu de données ZFS, la commande `praudit -x` affiche les champs comme suit :

```
<acl who="root" access_mask="default" flags="-i,-R" type="2"/>
```

Jeton `argument`

Le jeton `argument` 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.

La commande `praudit -x` affiche les champs du jeton `argument` comme suit :

```
<argument arg-num="2" value="0x5401" desc="cmd"/>
```

Jeton `attribute`

Le jeton `attribute` contient des informations issues du fichier `vnode`.

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, `vnode` ne permet pas 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`, comme suit :

```
<attribute mode="20620" uid="root" gid="tty" fsid="0" nodeid="9267" device="108233"/>
```

Jeton `cmd`

Le jeton `cmd` enregistre la liste d'arguments et la liste de variables d'environnement associées à une commande.

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 dans un appel système exec().

La commande praudit -x affiche les champs du jeton exec_args comme suit :

```
<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().

La commande praudit -x affiche les champs du jeton exec_env. La ligne dans l'exemple suivant est renvoyée à des fins d'affichage.

```
<exec_env><env>_=/usr/bin/hostname</env>
<env>LANG=C</env><env>PATH=/usr/bin</env>
<env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env>
<env>HOME=/home/jdoe</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 file

Le jeton file est un jeton spécial qui marque le début d'un nouveau fichier d'audit et la fin d'un ancien fichier d'audit lorsque ce dernier 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. Ces jetons "lient" les fichiers d'audit successifs dans une piste d'audit unique.

La commande praudit -x affiche les champs du jeton file. La ligne dans l'exemple suivant 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 `fmri`

Le jeton `fmri` enregistre l'utilisation d'un indicateur de ressource de gestion des pannes (FMRI, Fault Management Resource Indicator). Pour plus d'informations, reportez-vous à la page de manuel `smf(5)`.

La commande `praudit -x` affiche le contenu du jeton `fmri` comme suit :

```
<fmri service_instance="svc:/system/cryptosvc"</fmri>
```

Jeton `group`

Le jeton `group` enregistre les entrées de groupe dans les données d'identification du processus. Le jeton `group` s'affiche en sorte uniquement lorsque l'option de stratégie d'audit `group` est active.

La commande `praudit -x` affiche les champs du jeton `group` comme suit :

```
<group><gid>staff</gid><gid>other</gid></group>
```

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.

Parfois, un jeton `header` peut inclure un ou plusieurs modificateurs d'événement :

- `fe` indique un événement d'audit qui a échoué.
- `fp` indique l'échec de l'utilisation d'un privilège.
- `na` indique un événement non attribuable.

  ```
  header,52,2,system booted,na,mach1,2011-10-10 10:10:20.564 -07:00
  ```

- `rd` indique que les données sont lues à partir de l'objet.
- `sp` indique l'utilisation réussie d'un privilège.

  ```
  header,120,2,exit(2),sp,mach1,2011-10-10 10:10:10.853 -07:00
  ```

- `wr` indique que les données sont écrites sur l'objet.

La commande `praudit` affiche le jeton `header` de la manière suivante :

```
header,756,2,execve(2),,machine1,2010-10-10 12:11:10.209 -07:00
```

La commande `praudit -x` affiche les champs du jeton `header` au début de l'enregistrement d'audit. La ligne dans l'exemple suivant est renvoyée à des fins d'affichage.

```
<record version="2" event="execve(2)" host="machine1"
iso8601="2010-10-10 12:11:10.209 -07:00">
```

Jeton `ip address`

Le jeton `ip address` contient une adresse IP (Internet Protocol). L'adresse IP peut être affichée au 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 -x` affiche le contenu du jeton `ip address`, comme suit :

```
<ip_address>machine1</ip_address>
```

Jeton `ip port`

Le jeton `ip port` contient l'adresse de port TCP ou UDP.

La commande `praudit` affiche le jeton `ip port` de la manière suivante :

```
ip port,0xf6d6
```

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.

Les identificateurs d'objet IPC ne respectent pas la nature sans contexte des jetons d'audit. 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 7-2 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`, comme suit :

```
<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.

La commande `praudit -x` affiche les champs du jeton `IPC_perm`. La ligne dans l'exemple suivant 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 de la structure `IPC_perm` associée à l'objet IPC.

Jeton `path`

Le jeton `path` contient les informations de chemin d'accès pour un objet.

La commande `praudit -x` affiche le contenu du jeton `path`, comme suit :

```
<path>/export/home/srv/.xsession-errors</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 de fichiers d'attributs, reportez-vous à la page de manuel `fsattr`(5).

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 enregistré 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 " Processus Rights Management " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

La commande `praudit -x` affiche les champs du jeton `privilege`.

```
<privilege set-type="Inheritable">ALL</privilege>
```

Jeton `process`

Le jeton `process` contient des informations sur l'utilisateur associé à un processus, tels que le destinataire d'un signal.

La commande `praudit -x` affiche les champs du jeton `process`. La ligne dans l'exemple suivant est renvoyée à des fins d'affichage.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="567" sid="0" tid="0 0 0.0.0.0"/>
```

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` 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` comme suit :

```
<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. Le jeton `sequence` s'affiche en sortie uniquement lorsque l'option de stratégie d'audit `seq` est active. Ce jeton est utile pour le débogage.

La commande `praudit -x` affiche le contenu du jeton `sequence` :

```
<sequence seq-num="1292"/>
```

Jeton `socket`

Le jeton `socket` contient des informations qui décrivent un socket Internet. Dans certains cas, le jeton n'inclut que le port distant et l'adresse IP distante.

La commande `praudit -x` affiche cette instance du jeton `socket` comme suit :

```
socket,0x0002,0x83b1,localhost
```

Le jeton développé ajoute des informations, y compris sur le type de socket et le port local.

La commande `praudit -x` affiche cette instance du jeton `socket` de la manière suivante : La ligne dans l'exemple suivant 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` 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 dans l'exemple suivant 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"/>
```

Jeton `text`

Le jeton `text` contient une chaîne de texte.

La commande `praudit -x` affiche le contenu du jeton `text` comme suit :

```
<text>booting kernel</text>
```

Jeton `trailer`

Les deux jetons, `header` et `trailer`, sont spéciaux car ils distinguent les points de début et 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 un jeton facultatif et 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 jeton `trailer` pointe correctement vers l'en-tête d'enregistrement. Le jeton `trailer` prend en charge les recherches en arrière dans la piste d'audit.

La commande `praudit` affiche le jeton `trailer` comme suit :

```
trailer,136
```

Jeton `use of authorization`

Le jeton `use of authorization` enregistre l'utilisation des autorisations.

La commande `praudit` affiche le jeton `use of authorization` de la manière suivante :

```
use of authorization,solaris.role.delegate
```

Jeton `use of privilege`

Le jeton `use of privilege` enregistre l'utilisation des privilèges.

La commande `praudit -x` affiche les champs du jeton `use of privilege` comme suit :

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

Jeton `user`

Le jeton `user` enregistre le nom et l'ID de l'utilisateur. Ce jeton est présent si le nom d'utilisateur est différent de celui de l'appelant.

La commande `praudit -x` affiche les champs du jeton `user` comme suit :

```
<user uid="123456" username="tester1"/>
```

Jeton `xclient`

Le jeton `xclient` contient le numéro de la connexion client au serveur X.

La commande `praudit -x` affiche le contenu du jeton `xclient` comme suit :

```
<X_client>15</X_client>
```

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.

La commande `praudit -x` affiche le contenu du jeton `zonename` comme suit :

```
<zone name="graphzone"/>
```

Glossaire de la sécurité

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

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

algorithme cryptographique Voir algorithme.

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

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

API GSS 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.

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

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

authentificateur Des authentificateurs sont transmis par des clients lors de la demande de tickets (à un KDC) et de services (à un serveur). Ils contiennent des informations générées par l'utilisation d'une clé de session connue uniquement du client et du serveur, dont l'origine récente peut être prouvée, indiquant ainsi que la transaction est sécurisée. Lorsqu'un authentificateur est utilisé avec un ticket, il peut permettre d'authentifier un principal d'utilisateur. Un authentificateur inclut le nom du principal de l'utilisateur, l'adresse IP de l'hôte de l'utilisateur, ainsi qu'un horodatage. A la différence d'un ticket, un authentificateur ne peut servir qu'une seule fois, généralement lorsque l'accès à un service est demandé. Un authentificateur est chiffré à l'aide de la clé de session pour ce client et ce serveur.

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

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

2. Dans la gestion des droits d'utilisateur, droit pouvant être attribué à un rôle ou un utilisateur (ou intégré dans un profil de droits) en vue de l'exécution d'une classe d'opérations autrement interdite par la stratégie de sécurité. Les autorisations sont appliquées au niveau de l'application utilisateur et pas dans le noyau.

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

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

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

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

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

clé 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.

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

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

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.

droits Alternative au modèle tout ou rien des superutilisateurs. La gestion des droits des utilisateurs et la gestion des droits de processus permettent à une entreprise de répartir les privilèges du superutilisateur et de les affecter à des utilisateurs ou rôles. Les droits dans Oracle Solaris sont implémentés en tant que privilèges de noyau, d'autorisation et de capacité à exécuter un processus sous la forme d'un UID ou GID spécifique. Les droits peuvent être collectés dans un profil de droits et un rôle.

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

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

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

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. L'initialisation système initiale et les événements d'entrée et de sortie PROM sont des exemples d'événements asynchrones.

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

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

fichier de ticket Voir cache de référence.

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

fichier stash Un fichier stash contient une copie chiffrée de la clé principale pour le KDC. Cette clé principale est utilisée lorsqu'un serveur est réinitialisé pour authentifier automatiquement le

KDC avant qu'il ne démarre les processus `kadmind` et `krb5kdc`. Etant donné que le fichier stash inclut la clé principale, ce fichier et toutes ses sauvegardes doivent être sécurisés. Si le chiffrement est compromis, la clé peut être utilisée pour accéder à la base de données KDC ou la modifier.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MAC 1. Voir MAC.

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

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

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

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

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

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

mécanisme de sécurité Voir mécanisme.

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

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

modèle de superutilisateur Modèle de sécurité UNIX standard sur un système informatique. Dans le modèle de superutilisateur, un administrateur dispose d'un contrôle de type tout ou rien sur le système. En règle générale, pour l'administration de la machine, un utilisateur se connecte en tant que superutilisateur (`root`) et peut effectuer toutes les activités d'administration.

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

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

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

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

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

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

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

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

piste 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 (de modification de stratégies par exemple) qu'un principal d'utilisateur standard. Voir également nom de principal et principal d'utilisateur.

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

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

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

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

principe du moindre privilège Voir moindre privilège.

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

2. Droit discret dans le cadre d'un processus dans un système Oracle Solaris. Les privilèges offrent un contrôle des processus plus détaillé que `root`. Les privilèges sont définis et appliqués dans le noyau. Les privilèges sont également appelés *privilèges de processus* ou *privilèges de noyau*. Pour une description complète des privilèges, reportez-vous à la page de manuel `privileges`(5).

profil de droits On parle aussi de profil. Ensemble de remplacements de sécurité pouvant être attribués à un rôle ou à 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 appelés profils supplémentaires.

profil de droits authentifié profil de droits où l'utilisateur ou le rôle attribué doit saisir un mot de passe avant d'exécuter une opération à partir du profil. Ce comportement est similaire au comportement `sudo`. La durée de temps pendant laquelle le mot de passe est valide est configurable.

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

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

RBAC Contrôle d'accès basé sur les rôles, fonction de gestion des droits des utilisateurs d'Oracle Solaris. Voir droits.

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

référence 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.

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

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

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

SEAM Nom de produit pour la version initiale de Kerberos sur les systèmes Solaris. Ce produit est basé sur la technologie Kerberos V5 développée au Massachusetts Institute of Technology. SEAM est maintenant appelé le service Kerberos. Il reste légèrement différent de la version MIT.

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

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

séparation des tâches Composante de la notion de moindre privilège. La séparation des tâches empêche un utilisateur d'exécuter ou d'approuver toutes les opérations qui terminent une transaction. Par exemple,

dans RBAC, vous pouvez séparer la création d'un utilisateur de connexion de l'affectation des remplacements de sécurité. Un rôle crée l'utilisateur. Un autre rôle peut affecter les attributs de sécurité, tels que des profils de droits, des rôles et des privilèges aux utilisateurs existants.

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

serveur d'application 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 vous vous connectez par `rlogin` à la machine `central.example.com` par exemple, cette machine est le serveur fournissant le service `rlogin`.

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

service de sécurité Voir service.

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

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

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

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

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 affectés à l'utilisation et que les mots de passe soient modifiés toutes les six semaines.

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

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

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

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

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

stratégie de sécurité Voir stratégie.

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

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

stratégie RBAC Voir stratégie de droits.

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

synthèse Voir synthèse de message.

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

TGS Service d'octroi de tickets. Partie du KDC responsable de l'émission des tickets.

TGT Ticket d'octroi de tickets. 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, référence, service, clé de session.

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

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

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

ticket renouvelable Etant donné que tout ticket dont la durée de vie est très longue peut présenter un risque pour la sécurité, les tickets peuvent être conçus pour être `renouvelables`. Un ticket renouvelable possède deux moments d'expiration : a) l'heure à laquelle l'instance courante du ticket expire et b) la durée de vie maximale de tout ticket. Si un client souhaite continuer à utiliser un ticket, il

peut le renouveler avant sa première expiration. Par exemple, un ticket peut être valide pendant une heure, et tous les tickets ont une durée de vie maximale de dix heures. Si le client détenant le ticket souhaite le conserver plus d'une heure, il doit le renouveler. Lorsqu'un ticket atteint sa durée de vie maximale, celui-ci expire automatiquement et ne peut pas être renouvelé.

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

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

utilisateur privilégié Droits un utilisateur disposant des droits d'utilisateur standard au-delà de la sur un système informatique. Voir également utilisateurs de confiance.

utilisateurs de confiance Utilisateurs qui, selon vous, peuvent réaliser les tâches d'administration à un certain niveau de confiance. En général, les administrateurs créent d'abord des identifiants de connexion pour les utilisateurs de confiance et affectent des droits d'administration qui correspondent au niveau de confiance des utilisateurs et leur capacité. Ces utilisateurs aident ensuite à configurer et entretenir le système. Egalement appelés *utilisateurs privilégiés*.

variante Historiquement, la *variante de sécurité* et la *variante d'authentification* désignaient la même chose, lorsqu'une variante indiquait un type d'authentification (AUTH_UNIX, AUTH_DES, AUTH_KERB). RPCSEC_GSS est également une variante de sécurité, même s'il permet d'assurer des services d'intégrité et de confidentialité, en plus de l'authentification.

variante de sécurité Voir variante.

VPN Réseau privé virtuel assurant une communication sécurisée en utilisant les mécanismes de chiffrement et de mise en tunnel pour connecter les utilisateurs via un réseau public.

Index

B

C

D

E

F

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z