

## **Administration d'Oracle® Solaris : services de sécurité**

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

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

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

#### U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

# Table des matières

---

<b>Préface .....</b>	<b>23</b>
<b>Partie I   Présentation de la sécurité .....</b>	<b>27</b>
<b>1   Services de sécurité (présentation) .....</b>	<b>29</b>
Sécurité du système .....	30
Services cryptographiques .....	31
Services d'authentification .....	32
Authentification avec chiffrement .....	33
Audit .....	33
Stratégie de sécurité .....	33
<b>Partie II   Sécurité du système, des fichiers et des périphériques .....</b>	<b>35</b>
<b>2   Gestion de la sécurité de la machine (présentation) .....</b>	<b>37</b>
Contrôle de l'accès à un système informatique .....	37
Maintenance de la sécurité physique .....	38
Gestion du contrôle de connexion .....	38
Contrôle de l'accès aux périphériques .....	43
Stratégie de périphériques (présentation) .....	44
Allocation des périphériques (présentation) .....	45
Contrôle de l'accès aux ressources de la machine .....	46
Limitation et surveillance du superutilisateur .....	46
Configuration du contrôle d'accès basé sur les rôles pour remplacer le superutilisateur ....	46
Prévention des mauvaises utilisations involontaires des ressources système .....	47
Restriction des fichiers exécutables setuid .....	48
Utilisation de la configuration Secure by Default .....	49

Utilisation des fonctions de gestion des ressources .....	49
Utilisation des zones Oracle Solaris .....	49
Surveillance de l'utilisation des ressources de la machine .....	50
Surveillance de l'intégrité des fichiers .....	50
Contrôle de l'accès aux fichiers .....	50
Protection des fichiers par chiffrement .....	51
Utilisation des listes de contrôle d'accès .....	51
Partage de fichiers entre des machines .....	51
Restriction de l'accès root aux fichiers partagés .....	52
Contrôle de l'accès réseau .....	52
Mécanismes de sécurité réseau .....	53
Authentification et autorisation pour l'accès à distance .....	53
Systèmes pare-feu .....	55
Chiffrement et systèmes pare-feu .....	56
Génération de rapports sur les problèmes de sécurité .....	57
 <b>3 Contrôle de l'accès aux systèmes (tâches) .....</b>	<b>59</b>
Contrôle de l'accès système (liste des tâches) .....	59
Sécurisation des connexions et des mots de passe (liste des tâches) .....	60
Sécurisation des connexions et des mots de passe (liste des tâches) .....	60
▼ Procédure de modification du mot de passe root .....	61
▼ Procédure d'affichage de l'état de connexion d'un utilisateur .....	61
▼ Procédure d'affichage des utilisateurs sans mots de passe .....	62
▼ Procédure de désactivation temporaire des connexions utilisateur .....	63
▼ Procédure de contrôle des tentatives de connexion ayant échoué .....	63
▼ Procédure de contrôle de toutes les tentatives de connexion ayant échoué .....	64
Modification de l'algorithme par défaut pour le chiffrement de mot de passe (tâches) .....	66
▼ Procédure de spécification d'un algorithme de chiffrement de mot de passe .....	66
▼ Procédure de spécification d'un nouvel algorithme de mot de passe pour un domaine NIS .....	67
▼ Procédure de spécification d'un nouvel algorithme de mot de passe pour un domaine LDAP .....	68
Contrôle et restriction du superutilisateur (tâches) .....	69
▼ Procédure de contrôle de l'utilisateur de la commande su .....	69
▼ Procédure de restriction et de contrôle des connexions superutilisateur .....	70
Contrôle de l'accès au matériel du système (tâches) .....	71

▼ Procédure de spécification d'un mot de passe obligatoire pour l'accès au matériel .....	71
▼ Procédure de désactivation de la séquence d'abandon d'un système .....	72
<b>4 Service d'analyse antivirus (tâches) .....</b>	<b>75</b>
A propos de l'analyse de virus .....	75
A propos du service Vscan .....	76
Utilisation du service Vscan (tâches) .....	77
▼ Procédure d'activation de l'analyse de virus sur un système de fichiers .....	77
▼ Procédure d'activation du service vscan .....	78
▼ Procédure d'ajout d'un moteur d'analyse .....	78
▼ Procédure d'affichage des propriétés vscan .....	79
▼ Procédure de modification des propriétés vscan .....	79
▼ Procédure d'exclusion de fichiers des analyses antivirus .....	80
<b>5 Contrôle de l'accès aux périphériques (tâches) .....</b>	<b>81</b>
Configuration des périphériques (liste des tâches) .....	81
Configuration de la stratégie de périphériques (tâches) .....	82
Configuration de la stratégie de périphériques (liste des tâches) .....	82
▼ Procédure d'affichage de la stratégie de périphériques .....	82
▼ Procédure de modification de la stratégie pour un périphérique existant .....	83
▼ Procédure d'audit des modifications apportées à la stratégie de périphériques .....	84
▼ Procédure de récupération d'informations IP MIB-II à partir d'un périphérique /dev/* .	84
Gestion de l'allocation de périphériques (tâches) .....	85
Gestion de l'allocation des périphériques (liste des tâches) .....	85
▼ Procédure d'activation de l'allocation de périphériques .....	86
▼ Procédure d'autorisation des utilisateurs à allouer un périphérique .....	87
▼ Procédure d'affichage d'informations d'allocation sur un périphérique .....	88
▼ Allocation forcée d'un périphérique .....	88
▼ Libération forcée d'un périphérique .....	89
▼ Procédure de modification des périphériques pouvant être alloués .....	89
▼ Procédure d'audit de l'allocation de périphériques .....	90
Allocation de périphériques (tâches) .....	91
▼ Procédure d'allocation des périphériques .....	91
▼ Procédure de montage d'un périphérique alloué .....	92
▼ Procédure de libération des périphériques .....	93

Protection de périphériques (référence) .....	94
Commandes de la stratégie de périphériques .....	95
Allocation de périphériques .....	95
<b>6 Utilisation de l'outil de génération de rapports d'audit de base (tâches) .....</b>	<b>103</b>
Outil de génération de rapports d'audit de base (présentation) .....	103
Fonctionnalités BART .....	104
Composants BART .....	104
Utilisation de BART (tâches) .....	106
Considérations de sécurité BART .....	107
Utilisation de BART (liste des tâches) .....	107
▼ Procédure de création d'un manifeste .....	108
▼ Procédure de personnalisation d'un manifeste .....	110
▼ Procédure de comparaison des manifestes pour le même système dans le temps .....	111
▼ Procédure de comparaison de manifestes de différents systèmes .....	113
▼ Procédure de personnalisation d'un rapport BART en spécifiant des attributs de fichiers .....	115
▼ Procédure de personnalisation d'un rapport BART en utilisant un fichier de règles .....	116
Manifestes BART, fichiers de règles et rapports (référence) .....	118
Format de fichier manifeste BART .....	118
Format de fichier de règles BART .....	119
Génération de rapports BART .....	120
<b>7 Contrôle de l'accès aux fichiers (tâches) .....</b>	<b>123</b>
Utilisation des autorisations UNIX pour protéger les fichiers .....	123
Commandes d'affichage et de sécurisation des fichiers .....	123
Propriété des fichiers et des répertoires .....	124
Autorisations des fichiers UNIX .....	125
Autorisations de fichiers spéciales (setuid, setgid et sticky bit) .....	125
Valeur umask par défaut .....	127
Modes d'autorisation de fichier .....	128
Utilisation des ACL pour protéger les fichiers UFS .....	130
Protection contre les problèmes de sécurité causés par les fichiers exécutables .....	131
Protection des fichiers (tâches) .....	132
Protection des fichiers avec des autorisations UNIX (liste des tâches) .....	132

▼ Procédure d'affichage des informations de fichier .....	133
▼ Procédure de modification du propriétaire d'un fichier .....	134
▼ Procédure de modification de la propriété de groupe d'un fichier .....	135
▼ Procédure de modification des autorisations de fichier en mode symbolique .....	136
▼ Procédure de modification des autorisations de fichier en mode absolu .....	137
▼ Procédure de modification des autorisations de fichier spéciales en mode absolu .....	138
Protection contre les programmes présentant des risques de sécurité (liste des tâches) ...	139
▼ Procédure de recherche de fichiers avec des autorisations de fichier spéciales .....	139
▼ Procédure de désactivation de l'utilisation de piles exécutables par les programmes .....	141
<b>Partie III Rôles, profils de droits et privilèges .....</b>	<b>143</b>
<b>8 Utilisation des rôles et des privilèges (présentation) .....</b>	<b>145</b>
Contrôle d'accès basé sur les rôles (présentation) .....	145
RBAC : la solution de substitution au modèle superutilisateur .....	145
Éléments et concepts de base RBAC .....	149
Escalade des privilèges .....	152
Autorisations RBAC .....	152
Autorisations et privilèges .....	153
Applications privilégiées et RBAC .....	153
Profils de droits RBAC .....	155
Rôles RBAC .....	155
Shells de profil et RBAC .....	156
Champ d'application du service de noms et RBAC .....	157
Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité ..	157
Considérations relatives à l'utilisation lors de l'affectation directe d'attributs de sécurité	158
Privilèges (présentation) .....	158
Protection des processus noyau par les privilèges .....	159
Descriptions des privilèges .....	160
Différences administratives sur un système disposant de privilèges .....	161
Privilèges et ressources du système .....	162
Mise en oeuvre des privilèges .....	162
Comment les processus obtiennent des privilèges .....	164
Affectation de privilèges .....	164
Privilèges et périphériques .....	166

Privilèges et débogage .....	167
<b>9 Utilisation du contrôle d'accès basé sur les rôles (tâches) .....</b>	<b>169</b>
Utilisation de RBAC (tâches) .....	169
Affichage et utilisation des valeurs par défaut RBAC (tâches) .....	170
Affichage et utilisation des valeurs par défaut RBAC (liste des tâches) .....	170
▼ Procédure d'affichage de tous les attributs de sécurité définis .....	170
▼ Procédure d'affichage des droits qui vous sont affectés .....	171
▼ Procédure d'endossement d'un rôle .....	174
▼ Procédure d'obtention des droits d'administration .....	175
Personnalisation RBAC pour votre site (tâches) .....	177
Configuration initiale RBAC (liste des tâches) .....	177
▼ Procédure de planification de votre implémentation RBAC .....	178
▼ Procédure de création d'un rôle .....	181
▼ Procédure d'attribution de rôle .....	183
▼ Procédure d'audit des rôles .....	184
▼ Procédure de création ou de modification d'un profil de droits .....	186
▼ Procédure d'ajout de propriétés RBAC aux anciennes applications .....	188
▼ Procédure de dépannage de RBAC et de l'affectation de privilèges .....	189
Gestion de RBAC (tâches) .....	192
Gestion de RBAC (liste des tâches) .....	192
▼ Procédure de modification du mot de passe d'un rôle .....	193
▼ Procédure de modification des attributs de sécurité d'un rôle .....	194
▼ Procédure de modification des propriétés RBAC d'un utilisateur .....	196
▼ Procédure de limitation d'un utilisateur aux applications de bureau .....	198
▼ Procédure de limitation d'un administrateur aux droits affectés de manière explicite .....	199
▼ Procédure d'octroi à un utilisateur de l'autorisation d'utiliser son propre mot de passe pour endosser un rôle .....	201
▼ Procédure de modification du rôle root en utilisateur .....	202
Utilisation des privilèges (tâches) .....	204
Détermination des privilèges (liste des tâches) .....	204
▼ Procédure de création d'une liste des privilèges sur le système .....	205
▼ Procédure de détermination des privilèges qui vous sont attribués directement .....	206
▼ Procédure de détermination des commandes privilégiées que vous pouvez exécuter .....	207
Gestion des privilèges (liste des tâches) .....	209



▼ Procédure de détermination de privilèges sur un processus .....	209
▼ Procédure de détermination des privilèges requis par un programme .....	211
▼ Procédure d'exécution d'un script shell avec des commandes privilégiées .....	213
<b>10 Attributs de sécurité dans Oracle Solaris (référence) .....</b>	<b>215</b>
Profils de droits .....	215
Affichage du contenu des profils de droits .....	217
Ordre de recherche pour les attributs de sécurité affectés .....	217
Autorisations .....	218
Conventions de nommage des autorisations .....	219
Exemple de granularité d'autorisation .....	219
Pouvoir de délégation dans les autorisations .....	219
Bases de données RBAC .....	220
Bases de données RBAC et services de noms .....	220
Base de données user_attr .....	220
Base de données auth_attr .....	221
Base de données prof_attr .....	222
Base de données exec_attr .....	222
Fichier policy.conf .....	222
Commandes RBAC .....	223
Commandes pour la gestion de RBAC .....	223
Commandes sélectionnées nécessitant des autorisations .....	224
Privilèges .....	225
Commandes d'administration pour la gestion des privilèges .....	225
Fichiers disposant d'informations sur les privilèges .....	226
Privilèges et audit .....	227
Prévention de l'escalade de privilèges .....	227
Anciennes applications et modèle de privilège .....	228
<b>Partie IV Services cryptographiques .....</b>	<b>229</b>
<b>11 Structure cryptographique (présentation) .....</b>	<b>231</b>
Introduction à la structure cryptographique .....	231
Terminologie utilisée dans la structure cryptographique .....	233

Champ d'application de la structure cryptographique .....	235
Commandes d'administration dans la structure cryptographique .....	235
Commandes au niveau de l'utilisateur dans la structure cryptographique .....	236
Signatures binaires pour les logiciels tiers .....	236
Plug-ins de la structure cryptographique .....	237
Services cryptographiques et zones .....	237
 <b>12 Structure cryptographique (tâches) .....</b>	<b>239</b>
Utilisation de la structure cryptographique (liste des tâches) .....	239
Protection des fichiers avec la structure cryptographique (tâches) .....	240
Protection de fichiers avec la structure cryptographique (liste des tâches) .....	240
▼ Procédure de génération d'une clé symétrique à l'aide de la commande <code>dd</code> .....	240
▼ Procédure de génération d'une clé symétrique à l'aide de la commande <code>pktool</code> .....	243
▼ Procédure de calcul d'une synthèse d'un fichier .....	247
▼ Procédure de calcul du code MAC d'un fichier .....	248
▼ Procédure de chiffrement et déchiffrement d'un fichier .....	250
Administration de la structure cryptographique (tâches) .....	254
Administration de la structure cryptographique (liste des tâches) .....	254
▼ Procédure d'établissement de la liste des fournisseurs disponibles .....	255
▼ Procédure d'ajout d'un fournisseur de logiciels .....	258
▼ Procédure d'interdiction de l'utilisation d'un mécanisme au niveau de l'utilisateur .....	260
▼ Procédure d'interdiction de l'utilisation d'un fournisseur de logiciels noyau .....	262
▼ Procédure d'établissement de la liste des fournisseurs de matériel .....	264
▼ Procédure de désactivation des mécanismes et fonctions d'un fournisseur de matériel ...	265
▼ Procédure d'actualisation ou de redémarrage de tous les services cryptographiques .....	267
 <b>13 Structure de gestion des clés .....</b>	<b>269</b>
Gestion des technologies à clé publique .....	269
Utilitaires de la structure de gestion des clés .....	270
Gestion de la stratégie KMF .....	271
Gestion de plug-in KMF .....	271
Gestion de keystore KMF .....	271
Utilisation de la structure de gestion des clés (tâches) .....	272
Utilisation de la structure de gestion des clés (liste des tâches) .....	272
▼ Procédure de création d'un certificat à l'aide de la commande <code>pktool gencert</code> .....	273

▼ Procédure d'importation d'un certificat dans votre keystore .....	274
▼ Procédure d'exportation d'un certificat et de la clé privée au format PKCS #12 .....	276
▼ Procédure de génération d'une phrase de passe à l'aide de la commande <code>pktool setpin</code> .....	277
▼ Procédure de génération d'une paire de clés à l'aide de la commande <code>pktool genkeypair</code> .....	278
▼ Procédure de signature d'une demande de certificat à l'aide de la commande <code>pktool signcsr</code> .....	282
▼ Procédure de gestion des plug-ins tiers dans KMF .....	283
<b>Partie V Services d'authentification et communication sécurisée .....</b>	<b>285</b>
<b>14 Authentification des services réseau (tâches) .....</b>	<b>287</b>
Présentation du RPC sécurisé .....	287
Services NFS et RPC sécurisé .....	287
Chiffrement DES avec NFS sécurisé .....	288
Authentification Kerberos .....	288
Authentification Diffie-Hellman et RPC sécurisé .....	288
Administration de l'authentification avec le RPC sécurisé (tâches) .....	292
Administration du RPC sécurisé (liste des tâches) .....	292
▼ Procédure de redémarrage du serveur de clé RPC sécurisé .....	293
▼ Procédure de configuration d'une clé Diffie-Hellman pour un hôte NIS .....	293
▼ Procédure de configuration d'une clé Diffie-Hellman pour un utilisateur NIS .....	294
▼ Procédure de partage de fichiers NFS avec l'authentification Diffie-Hellman .....	295
<b>15 Utilisation de PAM .....</b>	<b>297</b>
PAM (présentation) .....	297
Avantages de l'utilisation de PAM .....	297
Présentation de la structure PAM .....	298
Modifications apportées à la structure des modules PAM pour cette version .....	299
PAM (tâches) .....	299
PAM (liste des tâches) .....	300
Planification de la mise en oeuvre PAM .....	300
▼ Procédure d'ajout d'un module PAM .....	301
▼ Procédure d'interdiction de l'accès rhost à partir de systèmes distants avec PAM .....	302
▼ Procédure de journalisation de rapports d'erreur PAM .....	302

Configuration PAM (référence) .....	302
Syntaxe du fichier de configuration PAM .....	303
Fonctionnement de la superposition PAM .....	303
Exemple de superposition PAM .....	307
<b>16 Utilisation de SASL .....</b>	<b>309</b>
SASL (présentation) .....	309
SASL (référence) .....	310
Plug-ins SASL .....	310
Variable d'environnement SASL .....	310
Options SASL .....	311
<b>17 Utilisation de Secure Shell (tâches) .....</b>	<b>313</b>
Secure Shell (présentation) .....	313
Authentification Secure Shell .....	314
Secure Shell dans l'entreprise .....	315
Secure Shell et le projet OpenSSH .....	316
Secure Shell et prise en charge FIPS-140 .....	317
Secure Shell (liste des tâches) .....	317
Configuration de Secure Shell (tâches) .....	318
Configuration de Secure Shell (liste des tâches) .....	318
▼ Procédure de configuration de l'authentification basée sur l'hôte pour Secure Shell .....	318
▼ Procédure de configuration du transfert de port dans Secure Shell .....	321
▼ Procédure de création d'exceptions d'utilisateur et d'hôte SSH aux valeurs par défaut du système .....	321
Utilisation de Secure Shell (tâches) .....	322
Utilisation de Secure Shell (liste des tâches) .....	322
▼ Procédure de génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell .....	323
▼ Procédure de modification de la phrase de passe pour une clé privée Secure Shell .....	325
▼ Procédure de connexion à un hôte distant avec Secure Shell .....	325
▼ Procédure de réduction des invites de mot de passe dans Secure Shell .....	327
▼ Procédure d'utilisation du transfert de port dans Secure Shell .....	328
▼ Procédure de copie de fichiers avec Secure Shell .....	329
▼ Procédure de configuration de connexions par défaut à des hôtes en dehors du pare-feu .....	330

<b>18</b>	<b>Secure Shell (référence)</b>	333
	Session Secure Shell standard	333
	Caractéristiques des sessions dans Secure Shell	334
	Authentification et échange de clés dans Secure Shell	334
	Exécution des commandes et transmission de données dans Secure Shell	335
	Configuration des clients et des serveurs dans Secure Shell	336
	Configuration des clients dans Secure Shell	336
	Configuration du serveur dans Secure Shell	336
	Mots-clés dans Secure Shell	336
	Paramètres spécifiques à l'hôte dans Secure Shell	341
	Secure Shell et les variables d'environnement de connexion	341
	Mise à jour des hôtes connus dans Secure Shell	342
	Fichier Secure Shell	342
	Commandes Secure Shell	344
<b>Partie VI</b>	<b>Service Kerberos</b>	347
<b>19</b>	<b>Introduction au service Kerberos</b>	349
	Description du service Kerberos	349
	Fonctionnement du service Kerberos	350
	Authentification initiale : le TGT	351
	Authentifications Kerberos suivantes	353
	Applications distantes Kerberos	354
	Principaux Kerberos	355
	Domaines Kerberos	355
	Serveurs Kerberos	356
	Services de sécurité Kerberos	357
	Composants des différentes versions Kerberos	358
	Composants Kerberos	358
	A propos de Kerberos dans la version Oracle Solaris 11	360
<b>20</b>	<b>Planification du service Kerberos</b>	363
	Intérêt de la planification des déploiements de Kerberos	363
	Planification de domaines Kerberos	364

Noms de domaine .....	364
Nombre de domaines .....	364
Hiérarchie des domaines .....	365
Mappage de noms d'hôtes sur des domaines .....	365
Noms des clients et des principaux de service .....	366
Ports pour les services d'administration et le KDC .....	367
Nombre de KDC esclaves .....	367
Mappage d'informations d'identification GSS sur des informations d'identification UNIX ...	368
Migration automatique d'utilisateur vers un domaine Kerberos .....	368
Choix du système de propagation de base de données .....	369
Synchronisation de l'horloge dans un domaine .....	369
Options de configuration du client .....	369
Amélioration de la sécurité de connexion des clients .....	370
Options de configuration de KDC .....	371
Approbation de services pour la délégation .....	371
Types de chiffrement Kerberos .....	372
URL d'aide en ligne dans l'outil d'administration graphique de Kerberos .....	373
<b>21 Configuration du service Kerberos (tâches) .....</b>	<b>375</b>
Configuration du service Kerberos (liste des tâches) .....	375
Configuration de services Kerberos supplémentaires (liste des tâches) .....	376
Configuration des serveurs KDC .....	377
▼ Procédure de configuration automatique d'un KDC maître .....	378
▼ Procédure de configuration interactive d'un KDC maître .....	379
▼ Procédure de configuration manuelle d'un KDC maître .....	380
▼ Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP	384
▼ Procédure de configuration automatique d'un KDC esclave .....	391
▼ Procédure de configuration interactive d'un KDC esclave .....	392
▼ Procédure de configuration manuelle d'un KDC esclave .....	393
▼ Procédure d'actualisation des clés TGS sur un serveur maître .....	397
Configuration de l'authentification inter-domaine .....	397
▼ Procédure d'établissement de l'authentification inter-domaine hiérarchique .....	397
▼ Procédure d'établissement de l'authentification inter-domaine directe .....	399
Configuration des serveurs d'application réseau Kerberos .....	400
▼ Procédure de configuration d'un serveur d'application réseau Kerberos .....	400

▼ Procédure d'utilisation du service de sécurité générique avec Kerberos lors de l'exécution FTP .....	402
Configuration de serveurs NFS Kerberos .....	403
▼ Procédure de configuration des serveurs NFS Kerberos .....	404
▼ Procédure de création d'une table d'informations d'identification .....	405
▼ Procédure d'ajout d'une entrée unique à la table d'informations d'identification .....	406
▼ Procédure de mappage d'informations d'identification entre domaines .....	407
▼ Procédure de configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos .....	408
Configuration des clients Kerberos .....	410
Configuration des clients Kerberos (liste des tâches) .....	410
▼ Procédure de création d'un profil d'installation de client Kerberos .....	411
▼ Procédure de configuration automatique d'un client Kerberos .....	411
▼ Procédure de configuration interactive d'un client Kerberos .....	413
▼ Procédure de configuration d'un client Kerberos pour un serveur Active Directory .....	416
▼ Procédure de configuration manuelle d'un client Kerberos .....	417
▼ Procédure de désactivation de la vérification du ticket d'octroi de tickets .....	422
▼ Procédure d'accès à un système de fichiers NFS protégé par Kerberos en tant qu'utilisateur root .....	423
▼ Procédure de configuration de la migration automatique des utilisateurs dans un domaine Kerberos .....	424
▼ Procédure de configuration du verrouillage de compte .....	426
Synchronisation des horloges entre les KDC et les clients Kerberos .....	427
Echange d'un KDC maître et d'un KDC esclave .....	428
▼ Procédure de configuration d'un KDC échangeable .....	429
▼ Procédure d'échange d'un KDC maître et d'un KDC esclave .....	429
Administration de la base de données Kerberos .....	433
Sauvegarde et propagation de la base de données Kerberos .....	433
▼ Procédure de sauvegarde de la base de données Kerberos .....	435
▼ Procédure de restauration de la base de données Kerberos .....	436
▼ Procédure de conversion d'une base de données Kerberos après une mise à niveau du serveur .....	436
▼ Procédure de reconfiguration d'un KDC maître pour l'utilisation de la propagation incrémentielle .....	437
▼ Procédure de reconfiguration d'un KDC esclave pour l'utilisation de la propagation incrémentielle .....	439
▼ Procédure de configuration d'un KDC esclave pour l'utilisation de la propagation	

complète .....	440
▼ Procédure de vérification de la synchronisation des serveurs KDC .....	443
▼ Procédure de propagation manuelle de la base de données Kerberos aux KDC esclaves ..	445
Configuration d'une propagation parallèle .....	446
Étapes de configuration d'une propagation parallèle .....	446
Administration du fichier stash .....	447
▼ Procédure de suppression d'un fichier stash .....	448
▼ Procédure d'utilisation d'une nouvelle clé principale .....	448
Gestion d'un KDC sur un serveur d'annuaire LDAP .....	450
▼ Procédure d'association des attributs de principaux Kerberos dans un type de classe d'objet non Kerberos .....	450
▼ Procédure de suppression d'un domaine d'un serveur d'annuaire LDAP .....	451
Renforcement de la sécurité des serveurs Kerberos .....	452
▼ Procédure d'activation des applications utilisant Kerberos uniquement .....	452
▼ Procédure de restriction de l'accès aux serveurs KDC .....	453
▼ Procédure d'utilisation d'un fichier dictionnaire pour augmenter la sécurité de mot de passe .....	453
<b>22 Messages d'erreur et dépannage de Kerberos .....</b>	<b>455</b>
Messages d'erreur Kerberos .....	455
Messages d'erreur de l'outil SEAM .....	455
Messages d'erreur Kerberos courants (A-M) .....	456
Messages d'erreur Kerberos courants (N-Z) .....	466
Dépannage de Kerberos .....	470
▼ Identification des problèmes liés aux numéros de version de clé .....	470
Problèmes avec le format du fichier krb5.conf .....	471
Problèmes de propagation de la base de données Kerberos .....	471
Problèmes de montage d'un système de fichiers NFS utilisant Kerberos .....	472
Problèmes liés à l'authentification en tant qu'utilisateur root .....	473
Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX .....	473
Utilisation de DTrace avec le service Kerberos .....	473
<b>23 Administration des principaux et des stratégies Kerberos (tâches) .....</b>	<b>475</b>
Méthodes d'administration des principaux et des stratégies Kerberos .....	475



outil SEAM .....	476
Equivalents de ligne de commande de l'outil SEAM .....	477
Seul fichier modifié par l'outil SEAM .....	477
Fonctions d'impression et d'aide en ligne de l'outil SEAM .....	478
Utilisation de grandes listes dans l'outil SEAM .....	478
▼ Procédure de démarrage de l'outil SEAM .....	479
Gestion des principaux de Kerberos .....	480
Gestion des principaux de Kerberos (liste des tâches) .....	480
Automatisation de la création de principaux Kerberos .....	481
▼ Procédure d'affichage de la liste des principaux Kerberos .....	482
▼ Procédure d'affichage des attributs d'un principal Kerberos .....	484
▼ Procédure de création d'un principal Kerberos .....	486
▼ Procédure de duplication d'un principal Kerberos .....	489
▼ Procédure de modification d'un principal Kerberos .....	490
▼ Procédure de suppression d'un principal Kerberos .....	491
▼ Procédure de paramétrage des valeurs par défaut pour la création de principaux Kerberos .....	492
▼ Procédure de modification des privilèges d'administration Kerberos .....	493
Administration des stratégies Kerberos .....	494
Administration des stratégies Kerberos (liste des tâches) .....	494
▼ Procédure d'affichage de la liste des stratégies Kerberos .....	495
▼ Procédure d'affichage des attributs d'une stratégie Kerberos .....	497
▼ Procédure de création d'une stratégie Kerberos .....	499
▼ Procédure de duplication d'une stratégie Kerberos .....	501
▼ Procédure de modification d'une stratégie Kerberos .....	501
▼ Procédure de suppression d'une stratégie Kerberos .....	502
Référence de l'outil SEAM .....	503
Descriptions des panneaux de l'outil SEAM .....	503
Utilisation de l'outil SEAM avec privilèges d'administration Kerberos limités .....	506
Administration des fichiers keytab .....	508
Administration des fichiers keytab (liste des tâches) .....	509
▼ Procédure d'ajout d'un principal de service Kerberos à un fichier keytab .....	509
▼ Procédure de suppression d'un principal de service d'un fichier keytab .....	511
▼ Procédure d'affichage de la liste de clés (principaux) dans un fichier keytab .....	512
▼ Procédure de désactivation temporaire de l'authentification d'un service sur un hôte .....	512

<b>24</b>	<b>Utilisation des applications Kerberos (tâches)</b>	515
	Gestion des tickets Kerberos	515
	Avez-vous besoin de vous soucier des tickets ?	515
	Création d'un ticket Kerberos	516
	Affichage des tickets Kerberos	517
	Destruction des tickets Kerberos	518
	Gestion des mots de passe Kerberos	519
	Conseils sur le choix d'un mot de passe	519
	Modification de votre mot de passe	520
	Octroi de l'accès à votre compte	522
	Commandes utilisateur Kerberos	524
	Présentation des commandes utilisant Kerberos	524
	Transfert des tickets Kerberos	527
	Utilisation de commandes utilisant Kerberos (exemples)	529
<b>25</b>	<b>Service Kerberos (référence)</b>	531
	Fichiers Kerberos	531
	Commandes Kerberos	533
	Démons Kerberos	534
	Terminologie Kerberos	534
	Terminologie spécifique à Kerberos	534
	Terminologie spécifique à l'authentification	535
	Types de tickets	536
	Fonctionnement du système d'authentification Kerberos	540
	Interaction du service Kerberos avec le DNS et le service <code>nsswitch.conf</code>	541
	Obtention de l'accès à un service à l'aide de Kerberos	541
	Obtention d'informations d'identification pour le service d'octroi de tickets	541
	Obtention d'informations d'identification pour un serveur	542
	Obtention de l'accès à un service donné	543
	Utilisation des types de chiffrement Kerberos	544
	Utilisation de la table <code>gsscred</code>	546
	Différences notables entre Oracle Solaris Kerberos et MIT Kerberos	547

<b>Partie VII</b>	<b>Audit dans Oracle Solaris</b>	549
<b>26</b>	<b>Audit (présentation)</b>	551
	Description de l'audit	551
	Terminologie et concepts de l'audit	552
	Événements d'audit	554
	Classes d'audit et présélection	555
	Enregistrements d'audit et jetons d'audit	557
	Modules plug-in d'audit	557
	Journaux d'audit	558
	Stockage et gestion de la piste d'audit	560
	Garantie de la fiabilité de l'horodatage	561
	Gestion d'un référentiel distant	561
	Rapports entre l'audit et la sécurité	561
	Fonctionnement de l'audit	562
	Configuration de l'audit	563
	Audit sur un système à zones Oracle Solaris	564
	A propos du service d'audit dans cette version	565
<b>27</b>	<b>Planification de l'audit</b>	567
	Planification de l'audit (tâches)	567
	▼ Procédure de planification de l'audit par zone	568
	▼ Procédure de planification du stockage pour les enregistrements d'audit	569
	▼ Procédure de planification des personnes et objets à auditer	570
	Assimilation des concepts de stratégie d'audit	573
	Contrôle des coûts d'audit	576
	Coût de l'augmentation du temps de traitement des données d'audit	576
	Coût de l'analyse des données d'audit	577
	Coût du stockage des données d'audit	577
	Gestion efficace de l'audit	578
<b>28</b>	<b>Gestion de l'audit (tâches)</b>	581
	Gestion de l'audit (liste des tâches)	581
	Configuration du service d'audit (tâches)	582

Configuration du service d'audit (liste des tâches) .....	582
▼ Procédure d'affichage des paramètres par défaut du service d'audit .....	583
▼ Procédure de présélection des classes d'audit .....	585
▼ Procédure de configuration des caractéristiques d'audit d'un utilisateur .....	586
▼ Procédure de modification de la stratégie d'audit .....	590
▼ Procédure de modification des contrôles de file d'attente d'audit .....	592
▼ Procédure de configuration de l'alias de messagerie <code>audit_warn</code> .....	594
▼ Procédure d'ajout d'une classe d'audit .....	595
▼ Procédure de modification de l'appartenance à une classe d'un événement d'audit .....	596
Configuration des journaux d'audit (tâches) .....	597
Configuration des journaux d'audit (liste des tâches) .....	597
▼ Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit .....	598
▼ Procédure d'affectation de l'espace d'audit pour la piste d'audit .....	601
▼ Procédure d'envoi des fichiers d'audit à un référentiel distant .....	604
▼ Procédure de configuration des journaux d'audit <code>syslog</code> .....	605
Configuration du service d'audit dans les zones (tâches) .....	607
▼ Procédure de configuration identique de toutes les zones pour l'audit .....	607
▼ Procédure de configuration de l'audit par zone .....	609
Activation et désactivation du service d'audit (tâches) .....	611
▼ Procédure d'actualisation du service d'audit .....	611
▼ Procédure de désactivation du service d'audit .....	613
▼ Procédure d'activation du service d'audit .....	614
Gestion des enregistrements d'audit sur les systèmes locaux (tâches) .....	615
Gestion des enregistrements d'audit sur les systèmes locaux (liste des tâches) .....	615
▼ Procédure d'affichage des définitions d'enregistrement d'audit .....	615
▼ Procédure de fusion des fichiers d'audit de la piste d'audit .....	617
▼ Procédure de sélection des événements d'audit de la piste d'audit .....	619
▼ Procédure d'affichage du contenu des fichiers d'audit binaires .....	621
▼ Procédure de nettoyage d'un fichier d'audit <code>not_terminated</code> .....	623
▼ Procédure de contrôle du dépassement de la piste d'audit .....	624
Dépannage du service d'audit (tâches) .....	626
Dépannage du service d'audit (liste des tâches) .....	626
▼ Procédure de vérification de l'exécution de l'audit .....	627
▼ Procédure d'atténuation du volume des enregistrements d'audit produits .....	629
▼ Procédure d'audit de toutes les commandes par les utilisateurs .....	631
▼ Procédure de recherche des enregistrements d'audit concernant des modifications de	

fichiers spécifiques .....	633
▼ Procédure de mise à jour du masque de présélection des utilisateurs connectés .....	635
▼ Procédure de suppression de l'audit d'événements spécifiques .....	636
▼ Procédure de limitation de la taille des fichiers d'audit binaires .....	637
▼ Procédure de compression des fichiers d'audit sur un système de fichiers dédié .....	638
▼ Procédure d'audit des connexions à partir d'autres systèmes d'exploitation .....	639
▼ Procédure d'audit des transferts de fichiers FTP et SFTP .....	640
<b>29 Audit (référence) .....</b>	<b>643</b>
Service d'audit .....	643
Pages de manuel du service d'audit .....	645
Profils de droits pour l'administration de l'audit .....	646
Audit et zones Oracle Solaris .....	647
Classes d'audit .....	647
Syntaxe de classe d'audit .....	648
Plug-ins d'audit .....	649
Stratégie d'audit .....	649
Stratégies d'audit des événements asynchrones et synchrones .....	650
Caractéristiques de l'audit de processus .....	651
Piste d'audit .....	652
Conventions relatives aux noms de fichiers d'audit binaires .....	652
Structure d'enregistrement d'audit .....	653
Analyse d'enregistrement d'audit .....	653
Formats de jeton d'audit .....	654
Jeton acl .....	656
Jeton argument .....	656
Jeton attribute .....	656
Jeton cmd .....	657
Jeton exec_args .....	657
Jeton exec_env .....	657
Jeton file .....	658
Jeton fmri .....	658
Jeton group .....	658
Jeton header .....	658
Jeton ip address .....	659

Jeton ip port .....	659
Jeton ipc .....	659
Jeton IPC_perm .....	660
Jeton path .....	660
Jeton path_attr .....	661
Jeton privilege .....	661
Jeton process .....	661
Jeton return .....	661
Jeton sequence .....	662
Jeton socket .....	662
Jeton subject .....	662
Jeton text .....	663
Jeton trailer .....	663
Jeton use of authorization .....	663
Jeton use of privilege .....	664
Jeton user .....	664
Jeton xclient .....	664
Jeton zonename .....	664
 <b>Glossaire</b> .....	 665
 <b>Index</b> .....	 677

# Préface

---

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

---

**Remarque** – Cette version d'Oracle Solaris prend en charge des systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page [Oracle Solaris OS: Hardware Compatibility Lists](#). Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

---

## Utilisateurs de ce manuel

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

## Organisation des guides d'administration système

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

Titre du manuel	Sujets
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes SPARC</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement d'initialisation, initialisation à partir de ZFS, gestion de l'archive d'amorçage et dépannage de l'initialisation sur les plates-formes SPARC
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes x86</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement d'initialisation, initialisation à partir de ZFS, gestion de l'archive d'amorçage et dépannage de l'initialisation sur les plates-formes x86

Titre du manuel	Sujets
<i>Administration d'Oracle Solaris : Tâches courantes</i>	Utilisation des commandes Oracle Solaris, initialisation et arrêt d'un système, gestion des comptes et groupes d'utilisateurs, gestion des services, des pannes matérielles, des informations système, des ressources système et des performances système, gestion du logiciel, de l'impression, de la console et des terminaux, et résolution des problèmes logiciels et système
<i>Administration d'Oracle Solaris : Périphériques et systèmes de fichiers</i>	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
<i>Administration d'Oracle Solaris : Services IP</i>	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, IP Filter et IPQoS
<i>Oracle Solaris Administration: Naming and Directory Services</i>	Services d'annuaire et de nommage DNS, NIS et LDAP, y compris transition de NIS à LDAP
<i>Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau</i>	Configuration d'interface IP manuelle et automatique, y compris la configuration sans fil Wi-Fi ; administration des ponts, réseaux locaux virtuels (VLAN), agrégations, LLDP et IPMP ; gestion des ressources et cartes d'interface réseau virtuelles
<i>Administration d'Oracle Solaris : Services réseau</i>	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), messagerie, SLP et PPP
<i>Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources</i>	Fonctions de gestion des ressources, qui vous permettent de contrôler la façon dont les applications utilisent les ressources système disponibles ; technologie de partitionnement logiciel Oracle Solaris Zones, qui virtualise les services de système d'exploitation pour créer un environnement isolé pour les applications en cours d'exécution, et Oracle Solaris 10 Zones, qui héberge les environnements Oracle Solaris 10 exécutés sur le noyau Oracle Solaris 11.
<i>Administration d'Oracle Solaris : services de sécurité</i>	Audit, gestion de périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique, gestion des clés, privilèges, RBAC, SASL Secure Shell et analyse des virus
<i>Oracle Solaris Administration: SMB and Windows Interoperability</i>	Service SMB, qui vous permet de configurer un système Oracle Solaris pour mettre les partages SMB à disposition des clients SMB ; client SMB, qui vous permet d'accéder aux partages SMB ; services de mappage d'identités natif, qui vous permet de mapper les identités de groupe et d'utilisateur entre les systèmes Oracle Solaris et les systèmes Windows
<i>Administration d'Oracle Solaris : Systèmes de fichiers ZFS</i>	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger des fichiers ZFS et utilisation de ZFS sur un système Oracle Solaris avec des zones installées.



Titre du manuel	Sujets
<i>Configuration et administration d'Oracle Solaris Trusted Extensions</i>	Installation, configuration et administration système, spécifique à Trusted Extensions
<i>Directives de sécurité d'Oracle Solaris 11</i>	Sécurisation d'un système Oracle Solaris et scénarios d'utilisation de ses fonctions de sécurité, telles que les zones, ZFS et Trusted Extensions
<i>Transition d'Oracle Solaris 10 vers Oracle Solaris 11</i>	Fournit les informations d'administration système et des exemples de transition à partir d'Oracle Solaris 10 vers Oracle Solaris 11 dans les domaines suivants : gestion de l'installation, des périphériques, des disques et des systèmes de fichiers, gestion des logiciels, mise en réseau, gestion des systèmes, sécurité, virtualisation, fonctions du bureau, gestion des comptes utilisateur et environnements utilisateur, volumes émulés, dépannage et récupération de données

## Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> adapté aux utilisateurs malentendants.

## Conventions typographiques

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

TABLEAU P-1 Conventions typographiques

Type de caractères	Description	Exemple
AaBbCc123	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier <code>.login</code> .  Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers.  <code>nom_machine%</code> Vous avez reçu du courrier.
<b>AaBbCc123</b>	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	<code>nom_machine% su</code>  Mot de passe :
<i>aabbcc123</i>	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est <code>rm nom_fichier</code> .

TABLEAU P-1 Conventions typographiques (Suite)		
Type de caractères	Description	Exemple
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du <i>Guide de l'utilisateur</i> .  Un <i>cache</i> est une copie des éléments stockés localement.  <i>N'enregistrez pas</i> le fichier.  <b>Remarque</b> : en ligne, certains éléments mis en valeur s'affichent en gras.

## Invites de shell dans les exemples de commandes

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

TABLEAU P-2 Invites de shell	
Shell	Invite
Bash shell, korn shell et bourne shell	\$
Bash shell, korn shell et bourne shell pour superutilisateur	#
C shell	nom_machine%
C shell pour superutilisateur	nom_machine#

## PARTIE I

# Présentation de la sécurité

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



## Services de sécurité (présentation)

---

Pour préserver la sécurité du SE Oracle Solaris, le logiciel propose les fonctionnalités suivantes :

- “Sécurité du système” à la page 30 : possibilité d'empêcher les intrusions, de protéger les ressources de la machine et les périphériques contre les utilisations inappropriées et de protéger les fichiers contre les modifications malveillantes ou involontaires par des utilisateurs ou des intrus.
- “Services cryptographiques” à la page 31 : capacité de brouiller les données afin que seul l'expéditeur et le destinataire désigné puissent lire le contenu, et de gérer les fournisseurs cryptographiques et les objets de clé publique
- “Services d'authentification” à la page 32 : capacité d'identifier un utilisateur de manière sécurisée, ce qui nécessite le nom de l'utilisateur et une forme quelconque de preuve, en général un mot de passe
- “Authentification avec chiffrement” à la page 33 : capacité de s'assurer que les parties authentifiées peuvent communiquer sans interception, modification ou usurpation d'identité
- “Audit” à la page 33 : capacité d'identifier l'origine des modifications de sécurité apportées au système, y compris l'accès aux fichiers, les appels système associés à la sécurité, et les échecs d'authentification
- “Stratégie de sécurité” à la page 33 : conception et mise en oeuvre des directives de sécurité pour un système ou un réseau de systèmes

# Sécurité du système

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

- **Outils d'administration de connexion** : commandes de surveillance et de contrôle de la capacité d'un utilisateur à se connecter. Reportez-vous à la section [“Sécurisation des connexions et des mots de passe \(liste des tâches\)”](#) à la page 60.
- **Accès au matériel** : commandes de limitation de l'accès à la PROM et de restriction des utilisateurs autorisés à initialiser le système. Reportez-vous à la section [“Contrôle de l'accès au matériel du système \(tâches\)”](#) à la page 71.
- **Accès aux ressources** : outils et stratégies permettant d'optimiser l'utilisation appropriée des ressources de la machine tout en minimisant l'utilisation inappropriée de ces ressources. Reportez-vous à la section [“Contrôle de l'accès aux ressources de la machine”](#) à la page 46.  
Pour la gestion des ressources dans les zones Oracle Solaris, reportez-vous à la [Partie I, “Gestion des ressources Oracle Solaris”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.
- **Contrôle d'accès basé sur les rôles (RBAC)** : architecture permettant de créer des comptes utilisateur restreints spécifiques, qui sont autorisés à effectuer des tâches d'administration. Reportez-vous à la section [“Contrôle d'accès basé sur les rôles \(présentation\)”](#) à la page 145.
- **Privilèges** : droits discrets sur les processus pour effectuer des opérations. Ces droits sur les processus sont appliqués dans le noyau. Reportez-vous à la section [“Privilèges \(présentation\)”](#) à la page 158.
- **Gestion des périphériques** : la *stratégie* relative aux périphériques protège en outre les périphériques qui sont déjà protégés par des autorisations UNIX. L'*allocation* des périphériques contrôle l'accès aux périphériques, tels qu'un microphone ou une unité de CD-ROM. Lors de l'annulation de l'allocation, les scripts de nettoyage de périphérique peuvent ensuite effacer toutes les données du périphérique. Reportez-vous à la section [“Contrôle de l'accès aux périphériques”](#) à la page 43.
- **Outil de rapport d'audit de base (BART)** : instantané, appelé *manifeste*, des attributs des fichiers d'un système. En comparant les manifestes sur l'ensemble des systèmes ou sur un système dans le temps, les modifications apportées aux fichiers peuvent être surveillées pour réduire les risques de sécurité. Reportez-vous au [Chapitre 6, “Utilisation de l'outil de génération de rapports d'audit de base \(tâches\)”](#).
- **Autorisations de fichier** : attributs d'un fichier ou d'un répertoire. Les autorisations limitent les utilisateurs et les groupes qui sont autorisés à lire, écrire ou exécuter un fichier, ou effectuer une recherche dans un répertoire. Reportez-vous au [Chapitre 7, “Contrôle de l'accès aux fichiers \(tâches\)”](#).

- **Logiciel antivirus** : un service vsan vérifie les fichiers à la recherche de virus avant qu'une application utilise les fichiers. Un système de fichiers peut appeler ce service pour analyser des fichiers en temps réel à l'aide des définitions de virus les plus récentes avant que les fichiers soient accessibles par des clients du système de fichiers.

L'analyse en temps réel est effectuée par des applications tierces. Un fichier peut être analysé lorsqu'il est ouvert et une fois qu'il est fermé. Reportez-vous au [Chapitre 4, "Service d'analyse antivirus \(tâches\)"](#).

## Services cryptographiques

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

- **Structure cryptographique** : structure centrale des services cryptographiques pour les consommateurs au niveau du noyau et au niveau de l'utilisateur, qui est basée sur les normes suivantes : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). Les utilisations comprennent les mots de passe, IPsec et des applications tierces. La structure centralise les sources matérielles et logicielles pour le chiffrement. La bibliothèque PKCS 11 fournit une API pour les développeurs tiers pour la connexion de la cryptographie requise pour leurs applications. Reportez-vous au [Chapitre 11, "Structure cryptographique \(présentation\)"](#).
- **Mécanismes de chiffrement par application** :
  - Pour l'utilisation de DES dans le RPC sécurisé, reportez-vous à la section "[Présentation du RPC sécurisé](#)" à la page 287.
  - Pour l'utilisation de DES, 3DES, AES et ARCFOUR dans le service Kerberos, reportez-vous au [Chapitre 19, "Introduction au service Kerberos"](#).
  - Pour l'utilisation de RSA, DSA et de chiffrements tels que Blowfish dans Secure Shell, reportez-vous au [Chapitre 17, "Utilisation de Secure Shell \(tâches\)"](#).
  - Pour l'utilisation d'algorithmes de chiffrement dans les mots de passe, consultez la section "[Modification de l'algorithme par défaut pour le chiffrement de mot de passe \(tâches\)](#)" à la page 66.

- La structure de gestion des clés (KMF) constitue un utilitaire central permettant de gérer les objets de clé publique, y compris les stratégies, les clés et les certificats. KMF gère ces objets pour les technologies à clé publique OpenSSL, NSS et PKCS 11. Reportez-vous au [Chapitre 13](#), “Structure de gestion des clés”.

## Services d'authentification

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

- **RPC sécurisé** : mécanisme d'authentification qui utilise le [protocole Diffie-Hellman](#) pour protéger les montages NFS et un service de noms, tel que NIS. Reportez-vous à la section “Présentation du RPC sécurisé” à la page 287.
- **Module d'authentification enfichable (PAM)** : structure permettant à diverses technologies d'authentification d'être connectées à un service d'entrée système sans recompiler le service. Certains services d'entrée système comprennent login et ftp. Reportez-vous au [Chapitre 15](#), “Utilisation de PAM”.
- **SASL (Simple Authentication and Security Layer)** : structure qui fournit des services d'authentification et de sécurité aux protocoles réseau. Reportez-vous au [Chapitre 16](#), “Utilisation de SASL”.
- **Secure Shell** : protocole de connexion et de transmission à distance qui chiffre les communications sur un réseau non sécurisé. Reportez-vous au [Chapitre 17](#), “Utilisation de Secure Shell (tâches)”.
- **Service Kerberos** : architecture client-serveur qui fournit le chiffrement en même temps que l'authentification. Reportez-vous à la [Partie VI](#).



## Authentification avec chiffrement

L'authentification avec chiffrement est la base de la communication sécurisée.

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

- **Secure Shell** : protocole de protection des transmissions de données et des sessions réseau utilisateur interactives contre les écoutes, le détournement de session et les attaques Man-in-the-middle. L'authentification forte est fournie par l'intermédiaire de la cryptographie par clé publique. Les services X Window et d'autres services réseau peuvent être délivrés par tunnel de manière sécurisée sur les connexions Secure Shell pour ajouter un niveau de protection supplémentaire. Reportez-vous au [Chapitre 17, "Utilisation de Secure Shell \(tâches\)"](#).
- **Service Kerberos** : architecture client-serveur qui assure l'authentification avec chiffrement. Reportez-vous à la [Partie VI](#).
- **Architecture IPsec (Internet Protocol Security Architecture)** : architecture qui fournit une protection des datagrammes IP. Les protections comprennent la confidentialité, un niveau élevé d'intégrité des données, l'authentification des données et l'intégrité des séquences partielles. Reportez-vous à la [Partie III, "IPsec" du manuel Administration d'Oracle Solaris : Services IP](#).

## Audit

L'audit est un concept fondamental de la sécurité des systèmes et de la maintenance. L'audit est le processus d'analyse de l'historique des actions et des événements sur un système afin de déterminer ce qui s'est passé. L'historique est enregistré dans un journal répertoriant ce qui a été effectué, quand, par qui, et ce qui a été affecté. Reportez-vous à la [Partie VII](#).

## Stratégie de sécurité

L'expression "stratégie de sécurité", ou [stratégie](#), est utilisée dans l'ensemble de ce manuel pour faire référence aux directives relatives à la sécurité d'une entreprise. La stratégie de sécurité de votre site constitue un ensemble de règles qui définissent la sensibilité des informations traitées et les mesures prises pour protéger les informations contre tout accès non autorisé. Les technologies de sécurité telles que Secure Shell, l'authentification, RBAC, l'autorisation, les privilèges et le contrôle des ressources fournissent des mesures de protection des informations.

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

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

**TABEAU 1-1** Utilisation du mot " stratégie " dans Oracle Solaris

Terme "stratégie"	Pages de manuel sélectionnées	Informations complémentaires
stratégie d'audit	auditconfig(1M)	Chapitre 26, "Audit (présentation)"
stratégie dans la structure cryptographique	cryptoadm(1M)	Chapitre 11, "Structure cryptographique (présentation)"
stratégie de périphériques	getdevpolicy(1M)	"Contrôle de l'accès aux périphériques" à la page 43
stratégie Kerberos	krb5.conf(4)	Chapitre 23, "Administration des principaux et des stratégies Kerberos (tâches)"
stratégies de réseau	ipfilter(5), ipadm(1M), ike.config(4), ipsecconf(1M), routeadm(1M)	Partie III, "IPsec" du manuel <i>Administration d'Oracle Solaris : Services IP</i>
stratégie de mot de passe	passwd(1), crypt.conf(4), policy.conf(4)	"Gestion du contrôle de connexion" à la page 38
stratégie pour technologies à clé publique	kmfcfg(1)	Chapitre 13, "Structure de gestion des clés"
stratégie RBAC	rbac(5), policy.conf(4)	"Fichier policy.conf" à la page 222

## PARTIE II

# Sécurité du système, des fichiers et des périphériques

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

- Chapitre 2, “Gestion de la sécurité de la machine (présentation)”
- Chapitre 3, “Contrôle de l'accès aux systèmes (tâches)”
- Chapitre 4, “Service d'analyse antivirus (tâches)”
- Chapitre 5, “Contrôle de l'accès aux périphériques (tâches)”
- Chapitre 6, “Utilisation de l'outil de génération de rapports d'audit de base (tâches)”
- Chapitre 7, “Contrôle de l'accès aux fichiers (tâches)”



## Gestion de la sécurité de la machine (présentation)

---

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

Vous trouverez ci-dessous une liste des informations générales contenues dans ce chapitre.

- “Contrôle de l'accès à un système informatique” à la page 37
- “Contrôle de l'accès aux périphériques” à la page 43
- “Contrôle de l'accès aux ressources de la machine” à la page 46
- “Contrôle de l'accès aux fichiers” à la page 50
- “Contrôle de l'accès réseau” à la page 52
- “Génération de rapports sur les problèmes de sécurité” à la page 57

### Contrôle de l'accès à un système informatique

Dans une entreprise, tous les ordinateurs connectés à un serveur peuvent être considérés comme un grand système multiforme. Vous êtes responsable de la sécurité de ce vaste système. Vous devez défendre le réseau contre les tentatives d'accès par des intrus. Vous devez également garantir l'intégrité des données sur les ordinateurs à l'intérieur du réseau.

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

Vous pouvez contrôler et surveiller l'accès au système en effectuant les opérations suivantes :

- “Maintenance de la sécurité physique” à la page 38
- “Gestion du contrôle de connexion” à la page 38
- “Contrôle de l'accès aux périphériques” à la page 43
- “Contrôle de l'accès aux ressources de la machine” à la page 46

- [“Contrôle de l'accès aux fichiers” à la page 50](#)
- [“Contrôle de l'accès réseau” à la page 52](#)
- [“Génération de rapports sur les problèmes de sécurité” à la page 57](#)

## Maintenance de la sécurité physique

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

Vous pouvez protéger un système SPARC contre tout accès non autorisé aux paramètres du matériel. Utilisez la commande `eeprom` pour exiger un mot de passe pour accéder à la PROM. Pour plus d'informations, reportez-vous à la section [“Procédure de spécification d'un mot de passe obligatoire pour l'accès au matériel” à la page 71](#). Pour protéger le matériel x86, consultez la documentation du fournisseur.

## Gestion du contrôle de connexion

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

Lorsqu'un utilisateur se connecte à un système, la commande `login` vérifie le service de noms adéquat ou la base de données de service d'annuaire adéquate en fonction des informations présentes dans le service de commutation de noms, `svc:/system/name-service/switch`. Les bases de données suivantes peuvent avoir une incidence sur la connexion :

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

Pour une description du service de noms, reportez-vous à la page de manuel [`nscd\(1M\)`](#). Pour plus d'informations sur les services de noms et les services d'annuaire, reportez-vous à la section [Oracle Solaris Administration: Naming and Directory Services](#).

La commande `login` vérifie le nom d'utilisateur et le mot de passe indiqués par l'utilisateur. Si le nom d'utilisateur ne figure pas dans la base de données des mots de passe, la commande `login` refuse l'accès au système. Si le mot de passe ne correspond pas au nom d'utilisateur spécifié, la

commande `login` refuse l'accès au système. Lorsque l'utilisateur fournit un nom d'utilisateur valide et son mot de passe correspondant, le système accorde à l'utilisateur l'accès au système.

Des modules PAM peuvent simplifier la connexion aux applications après une connexion réussie au système. Pour plus d'informations, reportez-vous au [Chapitre 15, "Utilisation de PAM"](#).

Des mécanismes d'authentification et d'autorisation sophistiqués sont disponibles sur les systèmes Oracle Solaris. Pour une description des mécanismes d'authentification et d'autorisation au niveau du réseau, reportez-vous à la section "[Authentification et autorisation pour l'accès à distance](#)" à la page 53.

## Gestion des informations de mot de passe

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

Les mots de passe sont initialement créés lorsque vous configurez un compte utilisateur. Pour assurer la sécurité des comptes utilisateur, vous pouvez configurer le vieillissement du mot de passe afin d'obliger les utilisateurs à en changer régulièrement. Vous pouvez également désactiver un compte utilisateur en verrouillant le mot de passe. Pour des informations plus détaillées sur la gestion des mots de passe, reportez-vous au [Chapitre 2, "Gestion des comptes utilisateur et des groupes \(présentation\)"](#) du manuel *Administration d'Oracle Solaris : Tâches courantes* et à la page de manuel `passwd(1)`.

## Mots de passe locaux

Si votre réseau utilise des fichiers locaux pour authentifier des utilisateurs, les informations du mot de passe sont conservées dans les fichiers `/etc/passwd` et `/etc/shadow` du système. Le nom de l'utilisateur et d'autres informations sont conservées dans le fichier `/etc/passwd`. Le mot de passe chiffré lui-même est conservé dans un autre fichier *shadow* appelé `/etc/shadow`. Cette mesure de sécurité empêche les utilisateurs d'accéder aux mots de passe chiffrés. Alors que le fichier `/etc/passwd` est accessible à toute personne pouvant se connecter à un système, seul le superutilisateur peut lire le fichier `/etc/shadow`. Vous pouvez utiliser la commande `passwd` pour modifier un mot de passe utilisateur sur un système local.

## Mots de passe NIS

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

## Mots de passe LDAP

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

La stratégie de mot de passe est appliquée sur le Oracle Directory Server Enterprise Edition. Plus précisément, le module `pam_ldap` du client suit les contrôles de stratégie de mot de passe mis en oeuvre sur le Oracle Directory Server Enterprise Edition. Pour plus d'informations, reportez-vous à la section “LDAP Naming Services Security Model” du manuel *Oracle Solaris Administration: Naming and Directory Services*.

## Chiffrement du mot de passe

Le chiffrement du mot de passe fort constitue une première barrière contre les attaques. Le logiciel Oracle Solaris fournit six algorithmes de chiffrement de mot de passe. Les algorithmes [Blowfish](#), [MD5](#) et [SHA](#) assurent un chiffrement de mot de passe plus robuste que l'algorithme UNIX.

## Identificateurs d'algorithmes de mot de passe

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

TABLEAU 2-1 Algorithmes de chiffrement de mot de passe

Identificateur	Description	Page de manuel de l'algorithme
1	Algorithme MD5 compatible avec des algorithmes MD5 sur des systèmes BSD et Linux.	<a href="#">crypt_bsmd5(5)</a>
2a	Algorithme Blowfish compatible avec l'algorithme Blowfish sur les systèmes BSD.	<a href="#">crypt_bsdbf(5)</a>
md5	Algorithme Sun MD5 considéré comme plus fort que la version BSD et Linux de MD5.	<a href="#">crypt_sunmd5(5)</a>
5	Algorithme SHA256. SHA est l'acronyme de Secure Hash Algorithm (algorithme de hachage sécurisé). Cet algorithme est un membre de la famille SHA-2. SHA256 prend en charge des mots de passe à 255 caractères.	<a href="#">crypt_sha256(5)</a>
6	Algorithme SHA512.	<a href="#">crypt_sha512(5)</a>
__unix__	Algorithme de chiffrement UNIX conventionnel.	<a href="#">crypt_unix(5)</a>



## Configuration d'algorithmes dans le fichier policy.conf

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

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

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

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

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

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

Identificateur = Algorithme de mot de passe		
Mot de passe initial	Mot de passe modifié	Explication
1 = crypt_bsdmd5	Utilise le même algorithme	L'identificateur 1 est également la valeur de <code>CRYPT_DEFAULT</code> . Le mot de passe de l'utilisateur continue d'être chiffré avec l'algorithme <code>crypt_bsdmd5</code> .
2a = crypt_bsdbf	Utilise le même algorithme	L'identificateur 2a est dans la liste <code>CRYPT_ALGORITHMS_ALLOW</code> . Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme <code>crypt_bsdbf</code> .
md5 = crypt_md5	Utilise le même algorithme	L'identificateur m5a est dans la liste <code>CRYPT_ALGORITHMS_ALLOW</code> . Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme <code>crypt_md5</code> .

Identificateur = Algorithme de mot de passe		
Mot de passe initial	Mot de passe modifié	Explication
5 = crypt_sha256	Utilise le même algorithme	L'identificateur 5 est dans la liste CRYPT_ALGORITHMS_ALLOW. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme crypt_sha256.
6 = crypt_sha512	Utilise le même algorithme	L'identificateur 6 est dans la liste CRYPT_ALGORITHMS_ALLOW. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme crypt_sha512.
__unix__ = crypt_unix	Utilise l'algorithme crypt_bsmd5	L'identificateur __unix__ n'est pas dans la liste CRYPT_ALGORITHMS_ALLOW. Par conséquent, l'algorithme crypt_unix ne peut pas être utilisé. Par conséquent, le nouveau mot de passe est chiffré avec l'algorithme CRYPT_DEFAULT.

Pour plus d'informations sur la configuration des sélections d'algorithme, reportez-vous à la page de manuel [policy.conf\(4\)](#) Pour spécifier le mot de passe, les algorithmes de chiffrement des mots de passe, consultez “[Modification de l'algorithme par défaut pour le chiffrement de mot de passe \(tâches\)](#)” à la page 66.

### Comptes système spéciaux

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



**Attention** – Ne modifiez jamais la définition du mot de passe d'un compte système. Les comptes système dans Oracle Solaris sont fournis dans un état sûr et sécurisé.

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

TABLEAU 2-2 Comptes de connexion système et leurs utilisations

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

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

Compte de connexion	UID	Utilisation
sys	3	Est propriétaire de nombreux fichiers système.
adm	4	Est propriétaire de certains fichiers administratifs.
lp	71	Est propriétaire des fichiers de données d'objet et des fichiers de données mis en spool pour l'imprimante.
uucp	5	Est propriétaire des fichiers de données d'objet et des fichiers de données mis en spool pour UUCP, le programme de copie UNIX-to-UNIX.
nuucp	9	Est utilisé par les systèmes distants pour se connecter au système et démarrer des transferts de fichiers.

## Connexions distantes

Les connexions distantes constituent une cible tentante pour les intrus. Oracle Solaris fournit plusieurs commandes pour surveiller, limiter et désactiver les connexions distantes. Pour plus d'informations sur les procédures, reportez-vous à la section “[Sécurisation des connexions et des mots de passe \(liste des tâches\)](#)” à la page 60.

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

# Contrôle de l'accès aux périphériques

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

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

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

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

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

- **Définir la stratégie de périphériques** : dans Oracle Solaris, vous pouvez exiger que le processus accédant à un périphérique particulier s'exécute avec un ensemble de privilèges. Les processus ne disposant pas de ces privilèges ne peuvent pas utiliser le périphérique. Au moment de l'initialisation, le logiciel Oracle Solaris configure la stratégie de périphériques. Les pilotes tiers peuvent être configurés avec la stratégie de périphériques au cours de l'installation. Après l'installation, vous pouvez, en tant qu'administrateur, ajouter une stratégie de périphériques à un périphérique.
- **Rendre des périphériques allouables** : lorsque vous activez l'allocation des périphériques, vous pouvez limiter l'utilisation d'un périphérique à un utilisateur à la fois. Vous pouvez également requérir que l'utilisateur remplisse certaines exigences en matière de sécurité. Par exemple, vous pouvez exiger que l'utilisateur soit autorisé à utiliser le périphérique.
- **Empêcher l'utilisation de périphériques** : vous pouvez empêcher l'utilisation d'un périphérique, tel qu'un microphone, quel que soit l'utilisateur sur un système informatique. Un ordinateur kiosque peut être un candidat approprié pour rendre certains périphériques indisponibles pour l'utilisation.
- **Confiner un périphérique dans une zone particulière** : vous pouvez affecter l'utilisation d'un périphérique à une zone non globale. Pour plus d'informations, reportez-vous à la section [“Utilisation de périphériques dans les zones non globales”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*. Pour une analyse plus générale des périphériques et des zones, reportez-vous à la section [“Périphériques configurés dans des zones”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

## Stratégie de périphériques (présentation)

Le mécanisme de la stratégie de périphériques vous permet d'indiquer que des processus permettant d'ouvrir un périphérique nécessitent certains privilèges. Les périphériques protégés par une stratégie de périphériques ne sont accessibles que par les processus s'exécutant avec les privilèges spécifiés par la stratégie correspondante. Oracle Solaris fournit une stratégie de périphériques par défaut. Par exemple, des interfaces réseau telles que `bge0` exigent que les processus accédant à l'interface s'exécutent avec le privilège `net_rawaccess`. L'exigence est appliquée dans le noyau. Pour plus d'informations sur les privilèges, reportez-vous à la section [“Privilèges \(présentation\)”](#) à la page 158.

Dans les versions antérieures, les noeuds de périphérique étaient protégés uniquement par les autorisations du fichier. Par exemple, les périphériques appartenant au groupe sys ne pouvaient être ouverts que par les membres du groupe sys. Aujourd'hui, les autorisations de fichier ne prédisent pas qui peut ouvrir un périphérique. Au lieu de cela, les périphériques sont protégés par des autorisations de fichier *et* par une stratégie de périphériques. Par exemple, le fichier /dev/lp a 666 autorisations. Cependant, le périphérique peut uniquement être ouvert par un processus disposant des privilèges appropriés.

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

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

- [“Configuration de la stratégie de périphériques \(liste des tâches\)” à la page 82](#)
- [“Commandes de la stratégie de périphériques” à la page 95](#)
- [“Privilèges et périphériques” à la page 166](#)

## Allocation des périphériques (présentation)

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

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

L'allocation des périphériques peut limiter l'utilisation d'un périphérique aux utilisateurs autorisés. L'allocation des périphériques peut également empêcher tout accès à un périphérique. Un utilisateur qui alloue un périphérique bénéficie d'un usage exclusif jusqu'à ce que l'utilisateur libère le périphérique. Lorsqu'un périphérique est libéré, des scripts de nettoyage de périphériques effacent toutes les données résiduelles. Vous pouvez écrire un script de nettoyage de périphériques pour supprimer des informations sur des périphériques ne disposant pas de script. Pour un exemple, reportez-vous à la section [“Ecriture de nouveaux scripts de nettoyage de périphériques” à la page 102](#).

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

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

- [“Gestion de l'allocation des périphériques \(liste des tâches\)” à la page 85](#)
- [“Allocation de périphériques” à la page 95](#)

- [“Commandes d'allocation de périphériques” à la page 97](#)

## Contrôle de l'accès aux ressources de la machine

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

### Limitation et surveillance du superutilisateur

Votre système nécessite un mot de passe root pour l'accès superutilisateur. Dans la configuration par défaut, l'utilisateur ne peut pas se connecter à distance à un système en tant que root. Lors d'une connexion à distance, un utilisateur doit se connecter avec son nom d'utilisateur, puis utiliser la commande `su` pour se connecter en tant que root. Vous pouvez surveiller les personnes utilisant la commande `su`, en particulier les utilisateurs qui essaient d'obtenir un accès superutilisateur. Pour plus d'informations sur les procédures permettant de surveiller le superutilisateur et de limiter l'accès au superutilisateur, reportez-vous à la rubrique [“Contrôle et restriction du superutilisateur \(tâches\)” à la page 69](#).

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

Fonction d'Oracle Solaris, le contrôle d'accès basé sur les rôles (RBAC) est conçu pour distribuer les capacités du superutilisateur à des rôles d'administration. Le superutilisateur, utilisateur root, a accès à toutes les ressources du système. Avec RBAC, vous pouvez remplacer root par un ensemble de rôles disposant de pouvoirs discrets. Par exemple, vous pouvez configurer un rôle pour gérer la création des comptes utilisateur, et un autre rôle pour gérer les modifications d'un fichier du système. Lorsque vous avez établi un rôle pour gérer une fonction ou un ensemble de fonctions, vous pouvez supprimer ces fonctions des capacités de l'utilisateur root.

Chaque rôle exige qu'un utilisateur connu se connecte avec son nom d'utilisateur et son mot de passe. Une fois connecté, l'utilisateur endosse le rôle avec un mot de passe spécifique. Par conséquent, toute personne connaissant le mot de passe root a une capacité limitée d'endommager votre système. Pour plus d'informations sur le contrôle RBAC, reportez-vous à la section [“Contrôle d'accès basé sur les rôles \(présentation\)” à la page 145](#).

## Prévention des mauvaises utilisations involontaires des ressources système

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

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

### Définition de la variable PATH

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

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

### Affectation d'un shell restreint à des utilisateurs

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

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

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

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

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

## Restriction de l'accès aux données dans les fichiers

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

Vous voulez peut-être permettre à certains utilisateurs de lire des fichiers et autoriser d'autres utilisateurs à modifier ou supprimer des fichiers. Il se peut que vous disposiez de données dont vous souhaitez qu'elles ne soient vues par personne d'autre. [Chapitre 7, “Contrôle de l'accès aux fichiers \(tâches\)”](#) explique comment définir les autorisations de fichier.

## Restriction des fichiers exécutables setuid

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

A l'exception des exécutables fournis par Oracle avec le bit `setuid` défini sur `root`, vous devez interdire l'utilisation des programmes `setuid`. Si vous ne pouvez pas interdire l'utilisation des programmes `setuid`, vous devez restreindre leur utilisation. Une administration sécurisée requiert quelques programmes `setuid`.



Pour plus d'informations, consultez [“Protection contre les problèmes de sécurité causés par les fichiers exécutables” à la page 131](#). Pour plus d'informations sur les procédures, reportez-vous à la section [“Protection contre les programmes présentant des risques de sécurité \(liste des tâches\)” à la page 139](#).

## Utilisation de la configuration Secure by Default

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

## Utilisation des fonctions de gestion des ressources

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

Avec les fonctions de gestion des ressources d'Oracle Solaris, vous pouvez désigner des ressources pour des projets particuliers. Vous pouvez également régler de façon dynamique les ressources disponibles. Pour plus d'informations, reportez-vous à la [Partie I, “Gestion des ressources Oracle Solaris” du manuel \*Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources\*](#).

## Utilisation des zones Oracle Solaris

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

Les zones Oracle Solaris sont idéales pour les environnements qui regroupent plusieurs applications sur un serveur unique. Pour plus d'informations, reportez-vous à la [Partie II, “Oracle Solaris Zones” du manuel \*Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources\*](#).

## Surveillance de l'utilisation des ressources de la machine

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

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

Grâce à ce type d'informations, vous pouvez utiliser les outils disponibles pour auditer l'utilisation du système et surveiller les activités des utilisateurs individuels. La surveillance est très utile lorsqu'une violation de sécurité est suspectée. Pour plus d'informations sur le service d'audit, reportez-vous au [Chapitre 26, “Audit \(présentation\)”](#).

## Surveillance de l'intégrité des fichiers

En tant qu'administrateur système, vous devez vous assurer que les fichiers installés sur les systèmes que vous administrez n'ont pas subi de modifications inattendues. Dans les installations de grande taille, un outil de comparaison et de génération de rapports sur la pile de logiciels sur chacun de vos systèmes vous permet d'effectuer le suivi de vos systèmes. L'outil de génération de rapports d'audit de base (BART) permet de valider de manière exhaustive les systèmes en effectuant des vérifications d'un ou plusieurs systèmes dans le temps au niveau des fichiers. Les modifications apportées à un *manifeste* BART sur l'ensemble des systèmes ou pour un système au fil du temps peuvent valider l'intégrité de vos systèmes. BART assure la création et la comparaison de manifestes et fournit des règles pour les rapports d'écriture de script. Pour plus d'informations, reportez-vous au [Chapitre 6, “Utilisation de l'outil de génération de rapports d'audit de base \(tâches\)”](#).

## Contrôle de l'accès aux fichiers

Oracle Solaris est un environnement multiutilisateur. Dans un environnement multiutilisateur, tous les utilisateurs connectés à un système peuvent lire des fichiers appartenant à d'autres utilisateurs. Les utilisateurs disposant des autorisations de fichiers appropriées peuvent également utiliser des fichiers appartenant à d'autres utilisateurs. Pour plus d'informations, reportez-vous au [Chapitre 7, “Contrôle de l'accès aux fichiers \(tâches\)”](#). Pour obtenir des instructions détaillées sur la définition des autorisations de fichiers appropriées, reportez-vous à la section [“Protection des fichiers \(tâches\)”](#) à la page 132.

## Protection des fichiers par chiffrement

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

La structure cryptographique fournit les commandes `digest`, `mac` et `encrypt` pour protéger les fichiers. Pour plus d'informations, reportez-vous au [Chapitre 11, "Structure cryptographique \(présentation\)"](#).

## Utilisation des listes de contrôle d'accès

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

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

- Autorisations de fichier de propriétaire
- Autorisations de fichier pour le groupe du propriétaire
- Autorisations de fichier pour d'autres utilisateurs n'appartenant pas au groupe du propriétaire
- Autorisations de fichier pour des utilisateurs spécifiques
- Autorisations de fichier pour des groupes spécifiques
- Autorisations par défaut pour chacune des catégories précédentes

Pour plus d'informations sur l'utilisation des ACL, reportez-vous à la section "[Utilisation des ACL pour protéger les fichiers UFS](#)" à la page 130. Pour protéger les fichiers ZFS avec des ACL (listes de contrôle d'accès), reportez-vous au [Chapitre 8, "Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS"](#) du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

## Partage de fichiers entre des machines

Un serveur de fichiers réseau peut contrôler les fichiers disponibles pour le partage. Un serveur de fichiers réseau peut également déterminer quels clients ont accès aux fichiers et quel type

d'accès est autorisé pour ces clients. En général, le serveur de fichiers peut accorder un accès en lecture-écriture ou un accès en lecture seule à tous les clients ou à des clients spécifiques. Le contrôle d'accès est spécifié lorsque des ressources sont mises à disposition à l'aide de la commande `share`.

Lorsque vous créez un partage NFS d'un système de fichiers ZFS, le système de fichiers est partagé définitivement jusqu'à ce que vous supprimiez le partage. SMF gère automatiquement le partage lorsque le système est redémarré. Pour plus d'informations, reportez-vous au [Chapitre 3, “Différences entre les systèmes de fichiers Oracle Solaris ZFS et classiques”](#) du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

## Restriction de l'accès root aux fichiers partagés

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

Un serveur NFS peut accorder l'accès root à un système de fichiers partagé en fonction de l'hôte. Pour accorder ces privilèges, utilisez l'option `root=hostname` avec la commande `share`. Vous devez utiliser cette option avec précaution. Pour une description des options de sécurité avec NFS, reportez-vous au [Chapitre 6, “Accès aux systèmes de fichiers réseau \(référence\)”](#) du manuel *Administration d'Oracle Solaris : Services réseau*.

## Contrôle de l'accès réseau

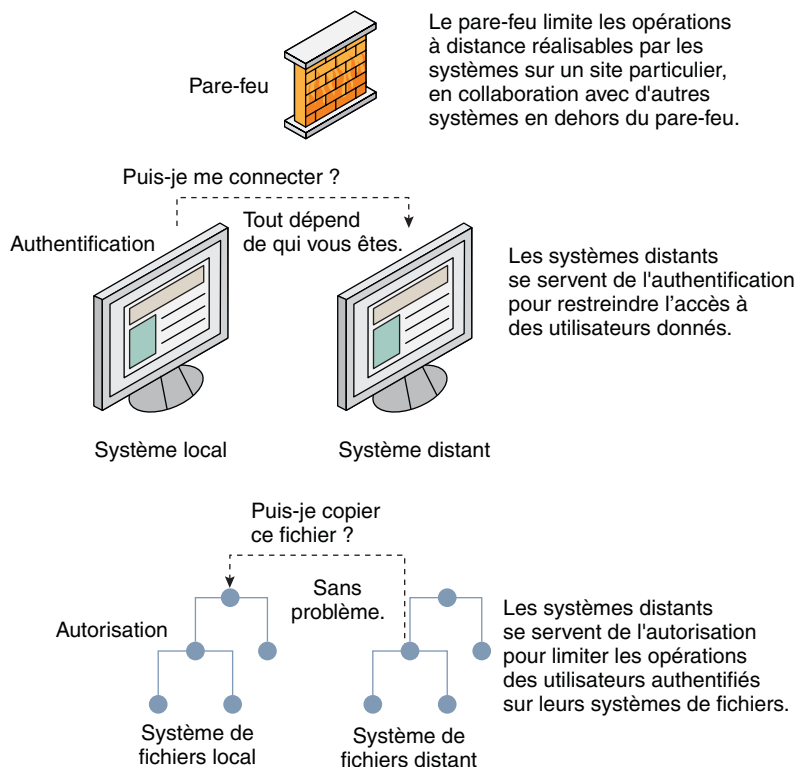
Les ordinateurs font souvent partie d'un *réseau* d'ordinateurs. Un réseau permet aux ordinateurs connectés d'échanger des informations. Les ordinateurs en réseau peuvent accéder aux données et à des ressources sur d'autres ordinateurs du réseau. Les réseaux d'ordinateurs créent un environnement informatique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

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

## Mécanismes de sécurité réseau

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

FIGURE 2-1 Restrictions de sécurité sur les opérations à distance



## Authentification et autorisation pour l'accès à distance

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

TABLEAU 2-3 Services d'authentification pour l'accès à distance

Service	Description	Voir
IPsec	IPsec propose une authentification par certificat basée sur les hôtes et le chiffrement du trafic réseau.	<a href="#">Chapitre 14, “Architecture IPsec (présentation)” du manuel <i>Administration d'Oracle Solaris : Services IP</i></a>
Kerberos	Kerberos utilise le chiffrement pour authentifier et autoriser un utilisateur se connectant au système.	Pour obtenir un exemple, reportez-vous à la section “ <a href="#">Fonctionnement du service Kerberos</a> ” à la page 350.
LDAP	Le service d'annuaire LDAP peut fournir à la fois l'authentification et l'autorisation au niveau du réseau.	<a href="#">Oracle Solaris Administration: Naming and Directory Services</a>
Commandes de connexion à distance	Les commandes de connexion à distance permettent aux utilisateurs de se connecter à un système distant via le réseau et d'utiliser ses ressources. <code>rlogin</code> , <code>rcp</code> et <code>ftp</code> sont des exemples de commandes de connexion à distance. Si vous êtes un “hôte de confiance”, l'authentification est automatique. Sinon, vous êtes invité à vous authentifier.	<a href="#">Chapitre 29, “Accès aux systèmes distants (tâches)” du manuel <i>Administration d'Oracle Solaris : Services réseau</i></a>
SASL	La couche SASL (Simple Authentication and Security Layer) est une structure fournissant des services d'authentification et de sécurité facultatifs aux protocoles réseau. Des plug-ins vous permettent de choisir un protocole d'authentification approprié.	<a href="#">“SASL (présentation)” à la page 309</a>
RPC sécurisé	Le RPC sécurisé améliore la sécurité des environnements réseau en authentifiant des utilisateurs adressant des demandes sur des machines distantes. Vous pouvez utiliser un système d'authentification UNIX, DES ou Kerberos pour le RPC sécurisé.	<a href="#">“Présentation du RPC sécurisé” à la page 287</a>
	Le RPC sécurisé peut également être utilisé pour assurer une sécurité supplémentaire dans un environnement NFS. Un environnement NFS avec RPC sécurisé est appelé NFS sécurisé. Il utilise l'authentification Diffie-Hellman pour les clés publiques.	<a href="#">“Services NFS et RPC sécurisé” à la page 287</a>
Secure Shell	Secure Shell chiffre le trafic réseau sur un réseau non sécurisé. Secure Shell assure l'authentification par l'emploi de mots de passe, de clés publiques ou des deux. Secure Shell utilise l'authentification RSA et DSA pour les clés publiques.	<a href="#">“Secure Shell (présentation)” à la page 313</a>

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

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

```
"Weak Authentication  
NFS request from unprivileged port"
```

## Systèmes pare-feu

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

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

Un pare-feu peut également être utile entre certains réseaux internes. Par exemple, vous pouvez configurer un pare-feu ou un ordinateur passerelle sécurisé pour restreindre le transfert de paquets. La passerelle peut interdire l'échange de paquets entre deux réseaux, à moins que l'ordinateur passerelle ne soit l'adresse source ou l'adresse de destination du paquet. Un pare-feu doit également être configuré pour transférer des paquets pour des protocoles particuliers uniquement. Par exemple, vous pouvez autoriser des paquets pour le transfert de courrier, mais pas pour la commande `telnet` ou `rlogin`.

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



---

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

---

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

IPsec et la fonction IP Filter d'Oracle Solaris peuvent fournir une protection par pare-feu. Pour plus d'informations sur la protection du trafic réseau, reportez-vous à la [Partie III, "IPsec"](#) du manuel *Administration d'Oracle Solaris : Services IP*.

## Chiffrement et systèmes pare-feu

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

L'éclatement de paquets consiste à capturer les paquets avant qu'ils n'atteignent leur destination. L'intrus injecte ensuite des données arbitraires dans le contenu, puis les renvoie à leur course initiale. Sur un réseau local, l'éclatement de paquets est impossible car ceux-ci atteignent tous les systèmes, y compris le serveur, en même temps. En revanche, la procédure est possible sur une passerelle. Vous devez donc vous assurer que toutes les passerelles du réseau sont protégées.

Les attaques les plus dangereuses affectent l'intégrité des données. De telles attaques impliquent la modification du contenu des paquets ou l'emprunt d'identité d'un utilisateur. Les attaques impliquant l'écoute électronique ne compromettent pas l'intégrité des données. Un système d'écoute électronique enregistre des conversations pour une rediffusion ultérieure. Un tel système n'emprunte pas l'identité d'un utilisateur. Bien que les attaques de ce type n'affectent pas l'intégrité des données, elles portent atteinte à leur confidentialité. Vous avez la possibilité de protéger la confidentialité des informations sensibles en chiffrant les données qui transitent sur le réseau.

- Pour chiffrer des opérations à distance via un réseau non sécurisé, reportez-vous au [Chapitre 17, "Utilisation de Secure Shell \(tâches\)"](#).
- Pour chiffrer et authentifier des données sur un réseau, reportez-vous au [Chapitre 19, "Introduction au service Kerberos"](#).
- Pour chiffrer des datagrammes IP, reportez-vous au [Chapitre 14, "Architecture IPsec \(présentation\)"](#) du manuel *Administration d'Oracle Solaris : Services IP*.



## Génération de rapports sur les problèmes de sécurité

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



## Contrôle de l'accès aux systèmes (tâches)

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

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

- “Contrôle de l'accès système (liste des tâches)” à la page 59
- “Sécurisation des connexions et des mots de passe (liste des tâches)” à la page 60
- “Modification de l'algorithme par défaut pour le chiffrement de mot de passe (tâches)” à la page 66
- “Contrôle et restriction du superutilisateur (tâches)” à la page 69
- “Contrôle de l'accès au matériel du système (tâches)” à la page 71

Pour des informations générales sur la sécurité du système, reportez-vous à la section [Chapitre 2, “Gestion de la sécurité de la machine \(présentation\)”](#).

### Contrôle de l'accès système (liste des tâches)

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

Tâche	Description	Voir
Contrôle, autorisation et refus d'une connexion utilisateur.	Contrôle les activités de connexion inhabituelles. Empêche temporairement les connexions.	“Sécurisation des connexions et des mots de passe (liste des tâches)” à la page 60
Garantie du chiffrement de mot de passe fort.	Indique les algorithmes permettant de chiffrer les mots de passe utilisateur. Installe des algorithmes supplémentaires.	“Modification de l'algorithme par défaut pour le chiffrement de mot de passe (tâches)” à la page 66
Contrôle et restriction des activités superutilisateur.	Contrôle régulièrement l'activité superutilisateur. Empêche la connexion à distance par un utilisateur root.	“Contrôle et restriction du superutilisateur (tâches)” à la page 69

Tâche	Description	Voir
Déni d'accès aux paramètres du matériel.	Maintient les utilisateurs standard hors de la PROM.	<a href="#">“Contrôle de l'accès au matériel du système (tâches)” à la page 71</a>

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

Vous pouvez limiter les connexions à distance, exiger que les utilisateurs aient des mots de passe et que le compte root ait un mot de passe complexe. Vous pouvez également contrôler les tentatives d'accès ayant échoué et désactiver temporairement les connexions.

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

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

Tâche	Description	Voir
Modification du mot de passe root.	Veille à ce que le compte root se conforme aux exigences de mot de passe.	<a href="#">“Procédure de modification du mot de passe root” à la page 61</a>
Affichage de l'état de connexion d'un utilisateur.	Répertorie des informations complètes sur le compte de connexion d'un utilisateur, telles que le nom complet et le vieillissement du mot de passe.	<a href="#">“Procédure d'affichage de l'état de connexion d'un utilisateur” à la page 61</a>
Recherche d'utilisateurs qui n'ont pas de mot de passe.	Recherche uniquement les utilisateurs dont les comptes n'ont pas besoin d'un mot de passe.	<a href="#">“Procédure d'affichage des utilisateurs sans mots de passe” à la page 62</a>
Désactivation temporaire des connexions.	Refuse les connexions utilisateur à une machine pendant la fermeture du système ou la maintenance de routine.	<a href="#">“Procédure de désactivation temporaire des connexions utilisateur” à la page 63</a>
Enregistrement des tentatives de connexion ayant échoué.	Crée un journal des utilisateurs qui n'ont pas réussi à fournir le bon mot de passe après cinq tentatives.	<a href="#">“Procédure de contrôle des tentatives de connexion ayant échoué” à la page 63</a>
Enregistrement de toutes les tentatives de connexion ayant échoué.	Crée un journal des échecs de tentative de connexion.	<a href="#">“Procédure de contrôle de toutes les tentatives de connexion ayant échoué” à la page 64</a>

## ▼ Procédure de modification du mot de passe root

Lorsque vous modifiez le mot de passe root, vous devez respecter les exigences relatives au mot de passe qui s'appliquent à tous les utilisateurs du système.

### Avant de commencer

Vous devez être dans le rôle root.

#### ● Modifiez votre mot de passe.

```
# passwd root
New Password:
Re-enter new Password:
passwd: password successfully changed for root
```

Un message s'affiche à l'écran si votre mot de passe n'est pas conforme aux exigences. Les messages sont informatifs. Après trois tentatives, vous devez exécuter la commande à nouveau pour modifier le mot de passe.

```
passwd: Password too short - must be at least 6 characters.
passwd: The password must contain at least 2 alphabetic character(s).
passwd: The password must contain at least 1 numeric or special character(s).
```

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

### Avant de commencer

Vous devez être dans le rôle root.

#### ● Affichez l'état de connexion d'un utilisateur à l'aide de la commande `logins`.

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

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

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

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

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

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

```
# logins -x -l jdoe
jdoe      500      staff      10      Jaylee Jaye Doe
           /home/jdoe
           /bin/bash
           PS 010103 10 7 -1
```

jdoe Identifie le nom de connexion de l'utilisateur.

500 Identifie l'ID utilisateur (UID).

staff Identifie le groupe principal de l'utilisateur.

10 Identifie l'ID de groupe (GID).

Jaylee Jaye Doe Identifie le commentaire.

/home/jdoe Identifie le répertoire personnel de l'utilisateur.

/bin/bash Identifie le shell de connexion.

PS 010170 10 7 -1

Spécifie les informations de vieillissement du mot de passe :

- Date à laquelle le mot de passe a été modifié pour la dernière fois
- Nombre de jours qui sont requis entre les modifications
- Nombre de jours avant qu'une modification ne soit requise
- Période d'avertissement

## ▼ Procédure d'affichage des utilisateurs sans mots de passe

### Avant de commencer

Vous devez être dans le rôle root.

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

```
# logins -p
```

L'option `-p` affiche une liste des utilisateurs sans mot de passe. La commande `logins` utilise la base de données `passwd` à partir du système local sauf si un service de noms distribué est spécifié dans le fichier `nsswitch.conf`.

### Exemple 3–2 Affichage des utilisateurs sans mot de passe

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

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

## ▼ Procédure de désactivation temporaire des connexions utilisateur

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

### Avant de commencer

Vous devez être dans le rôle root.

- 1 Créez le fichier `/etc/nlogin` dans un éditeur de texte.

```
# vi /etc/nlogin
```

- 2 Incluez un message sur la disponibilité du système.

- 3 Fermez et enregistrez le fichier.

### Exemple 3–3 Désactivation des connexions utilisateur

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

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

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

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

Vous pouvez également mettre le système au niveau d'exécution 0, en mode monutilisateur, pour désactiver les connexions. Pour plus d'informations sur la mise du système en mode monutilisateur, reportez-vous au [Chapitre 3, “Arrêt d'un système \(tâches\)”](#) du manuel *Initialisation et arrêt d'Oracle Solaris sur les plates-formes x86*.

## ▼ Procédure de contrôle des tentatives de connexion ayant échoué

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

### Avant de commencer

Vous devez être dans le rôle root.

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

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

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

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

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

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

**4 Vérifiez que le journal fonctionne.**

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

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

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

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

## ▼ Procédure de contrôle de toutes les tentatives de connexion ayant échoué

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

**Avant de commencer**

Vous devez être dans le rôle `root`.

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

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

```
# grep SYSLOG /etc/default/login
# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
SYSLOG=YES
```



```
# The SYSLOG_FAILED_LOGINS variable is used to determine how many failed
#SYSLOG_FAILED_LOGINS=5
SYSLOG_FAILED_LOGINS=0
#
```

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

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

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

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

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

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

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

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

Envoyer les échecs au fichier `authlog`.

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

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

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

**b. Actualisez le service `system-log`.**

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

**4 Vérifiez que le journal fonctionne.**

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

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

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

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

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

### Exemple 3-5 Fermeture de la connexion après trois échecs de connexion

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

## Modification de l'algorithme par défaut pour le chiffrement de mot de passe (tâches)

Par défaut, les mots de passe utilisateur sont chiffrés avec l'algorithme `crypt_sha256`. Vous pouvez utiliser un autre algorithme de chiffrement en modifiant l'algorithme de chiffrement de mot de passe par défaut.

### ▼ Procédure de spécification d'un algorithme de chiffrement de mot de passe

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

#### Avant de commencer

Vous devez être dans le rôle root.

#### ● Spécifiez l'identificateur de l'algorithme de chiffrement choisi.

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

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

```
# cat /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#
# Use the version of MD5 (5) that works with Linux and BSD systems.
# Passwords previously encrypted with SHA256 (1) will be encrypted
# with MD5 when users change their passwords.
#
#
#CRYPT_DEFAULT=5
CRYPT_DEFAULT=1
```

Dans cet exemple, la configuration des algorithmes assure que l'algorithme sha256 n'est pas utilisé pour chiffrer un mot de passe. Les utilisateurs dont les mots de passe ont été chiffrés avec le module sha256 obtiennent un mot de passe chiffré par crypt\_bsdmd5 lorsqu'ils changent leurs mots de passe.

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

### Exemple 3–6 Contrainte des algorithmes de chiffrement de mot de passe dans un environnement hétérogène

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

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

## ▼ Procédure de spécification d'un nouvel algorithme de mot de passe pour un domaine NIS

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

#### Avant de commencer

Vous devez être dans le rôle root.

- 1 **Spécifiez l'algorithme de chiffrement de mot de passe dans le fichier `/etc/security/policy.conf` du client NIS.**
- 2 **Copiez le fichier `/etc/security/policy.conf` modifié sur chaque système client dans le domaine NIS.**

- 3 Pour éviter toute confusion, copiez le fichier `/etc/security/policy.conf` modifié sur le serveur root NIS et les serveurs esclaves.

## ▼ Procédure de spécification d'un nouvel algorithme de mot de passe pour un domaine LDAP

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

### Avant de commencer

Vous devez être dans le rôle root.

- 1 Spécifiez un algorithme de chiffrement de mot de passe dans le fichier `/etc/security/policy.conf` du client LDAP.
- 2 Copiez le fichier `policy.conf` modifié pour chaque système client dans le domaine LDAP.
- 3 Assurez-vous que le fichier `/etc/pam.conf` du client n'utilise pas un module `pam_ldap`.

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

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

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

---

**Remarque** – Pour tirer parti des commandes de stratégie de mot de passe sur le serveur LDAP, utilisez l'option `server_policy` avec les entrées `pam_authok_store` dans le fichier `pam.conf`. Les mots de passe sont alors chiffrés sur le serveur en utilisant le mécanisme cryptographique de Oracle Directory Server Enterprise Edition. Pour plus d'informations sur cette procédure, reportez-vous au [Chapitre 11, “Setting Up Oracle Directory Server Enterprise Edition With LDAP Clients \(Tasks\)”](#) du manuel *Oracle Solaris Administration: Naming and Directory Services*.

---

## Contrôle et restriction du superutilisateur (tâches)

Une alternative à l'utilisation du compte de superutilisateur est de définir le contrôle de l'accès basé sur le rôle (RBAC). Pour des informations générales sur le contrôle RBAC, reportez-vous à la section “[Contrôle d'accès basé sur les rôles \(présentation\)](#)” à la page 145. Pour configurer RBAC, reportez-vous au [Chapitre 9](#), “[Utilisation du contrôle d'accès basé sur les rôles \(tâches\)](#)”.

### ▼ Procédure de contrôle de l'utilisateur de la commande su

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

#### Avant de commencer

Vous devez être dans le rôle `root`.

#### ● Contrôle du contenu du fichier `/var/adm/su.log` de façon régulière.

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

Les entrées affichent les informations suivantes :

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

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

```
SULOG=/var/adm/su.log
```

#### Erreurs fréquentes

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

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

## ▼ Procédure de restriction et de contrôle des connexions superutilisateur

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

### Avant de commencer

Vous devez être dans le rôle `root`.

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

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

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

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

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

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

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

#### 3 Surveillez les tentatives de devenir **root**.

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

##### a. Ouvrez une console de terminal sur le bureau.

##### b. Dans une autre fenêtre, utilisez la commande `su` pour devenir superutilisateur.

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

Un message est imprimé sur la console de terminal.

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

**Exemple 3-7 Journalisation des tentatives d'accès superutilisateur**

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

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

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

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

**Erreurs fréquentes**

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

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

## Contrôle de l'accès au matériel du système (tâches)

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

Pour protéger le BIOS, consultez la documentation du fournisseur.

### ▼ Procédure de spécification d'un mot de passe obligatoire pour l'accès au matériel

**Avant de commencer**

Le profil de droits Device Security (sécurité des périphériques), Maintenance and Repair (maintenance et réparation) ou System Administrator (administrateur système) doit vous être affecté.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

**2 Dans une fenêtre de terminal, saisissez le mode de sécurité de la PROM.**

```
# eeprom security-mode=command
```

Changing PROM password:

New password:       <Type password>

Retype new password:   <Retype password>

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

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

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

```
# eeprom security-password=       Press Return
```

Changing PROM password:

New password:       <Type password>

Retype new password:   <Retype password>

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



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

---

## ▼ **Procédure de désactivation de la séquence d'abandon d'un système**

---

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

---

**Avant de commencer**

Vous devez être dans le rôle `root`.



**1 Modifiez la valeur de KEYBOARD\_ABORT en la définissant sur disable.**

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

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

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

```
# kbd -i
```



## Service d'analyse antivirus (tâches)

---

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

- “A propos de l'analyse de virus” à la page 75
- “A propos du service Vscan” à la page 76
- “Utilisation du service Vscan (tâches)” à la page 77

### A propos de l'analyse de virus

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

Le service vscan peut être configuré pour utiliser plusieurs moteurs d'analyse. Il est recommandé que le service vscan utilise un minimum de deux moteurs d'analyse. Les demandes pour les analyses de virus sont réparties entre tous les moteurs d'analyse disponibles. Le [Tableau 4-1](#) présente les moteurs d'analyse pris en charge lorsqu'ils sont configurés avec leur patch le plus récent.

TABLEAU 4-1 Logiciel de moteur d'analyse antivirus

Logiciel antivirus	Prise en charge d'ICAP
Symantec Antivirus Scan Engine 4.3	Pris en charge
Symantec Antivirus Scan Engine 5.1	Pris en charge

**TABLEAU 4-1** Logiciel de moteur d'analyse antivirus (Suite)

Logiciel antivirus	Prise en charge d'ICAP
Computer Associates eTrust AntiVirus 7.1	Non pris en charge <sup>1</sup>
Computer Associates Integrated Threat Management 8.1	
Trend Micro Interscan Web Security Suite (IWSS) 2.5	Pris en charge
McAfee Secure Internet Gateway 4.5	Pris en charge

<sup>1</sup> Nécessite l'installation de Sun StorageTek 5000 NAS ICAP Server for Computer Associates Antivirus Scan Engine. Vous pouvez obtenir le package au [centre de téléchargement Sun](http://www.oracle.com/technetwork/indexes/downloads/index.html) : (<http://www.oracle.com/technetwork/indexes/downloads/index.html>).

# A propos du service Vscan

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

La section suivante décrit le processus d'analyse de virus :

1. Lorsqu'un utilisateur ouvre un fichier à partir du client, le service vscan détermine si le fichier doit être analysé, suivant si le fichier a été précédemment analysé avec les signatures de virus actuelles et si le fichier a été modifié depuis sa dernière analyse.
  - Si le fichier doit être analysé, il est transféré vers le [moteur d'analyse](#). Si une connexion à un moteur d'analyse échoue, le fichier est envoyé à un autre moteur d'analyse. Si aucun moteur d'analyse n'est disponible, l'analyse de virus scan échoue et l'accès au fichier peut être refusé.
  - Si le fichier n'a pas besoin d'être analysé, le client est autorisé à accéder au fichier.
2. Le moteur d'analyse analyse le fichier à l'aide des définitions de virus actuelles.
  - Si un virus est détecté, le fichier est marqué comme étant mis en quarantaine. Un fichier mis en quarantaine ne peut pas être lu, exécuté ou renommé, mais il peut être supprimé. Le journal système enregistre le nom du fichier mis en quarantaine et le nom du virus et, si l'audit a été activé, un enregistrement d'audit avec les mêmes informations est créé.
  - Si le fichier n'est pas infecté, il est marqué avec un timbre d'analyse et le client est autorisé y à accéder.

## Utilisation du service Vscan (tâches)

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

- Au moins un moteur d'analyse est installé et configuré.
- Les fichiers sont stockés dans un système de fichiers qui prend en charge l'analyse de virus.
- L'analyse de virus est activée sur le système de fichiers.
- Le service vscan est activé.
- Le service vscan est configuré pour analyser les fichiers du type de fichier spécifié.

Le tableau suivant indique les tâches que vous pouvez effectuer pour configurer le service vscan.

Tâche	Description	Voir
Installation d'un <a href="#">moteur d'analyse</a> .	Installe et configure un ou plusieurs produits tiers pris en charge répertoriés dans le <a href="#">Tableau 4-1</a> .	Consultez la documentation fournie avec le produit.
Activation du système de fichiers afin d'autoriser les analyses de virus.	Active les analyses de virus sur un système de fichiers ZFS. Par défaut, les analyses sont désactivées.	<a href="#">“Procédure d'activation de l'analyse de virus sur un système de fichiers” à la page 77</a>
Activation du service vscan.	Démarre le service d'analyse.	<a href="#">“Procédure d'activation du service vscan” à la page 78</a>
Ajout d'un moteur d'analyse au service vscan.	Inclut des moteurs d'analyse spécifiques dans le service vscan.	<a href="#">“Procédure d'ajout d'un moteur d'analyse” à la page 78</a>
Configuration du service vscan.	Affiche et modifie les propriétés vscan.	<a href="#">“Procédure d'affichage des propriétés vscan” à la page 79</a> <a href="#">“Procédure de modification des propriétés vscan” à la page 79</a>
Configuration du service vscan pour des types de fichier spécifiques.	Indique les types de fichier à inclure et exclure dans une analyse.	<a href="#">“Procédure d'exclusion de fichiers des analyses antivirus” à la page 80</a>

### ▼ Procédure d'activation de l'analyse de virus sur un système de fichiers

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

**Avant de commencer**

Le profil de droits ZFS System Management (gestion de système ZFS) ou ZFS Storage Management (gestion de stockage ZFS) doit vous être attribué. Le système de fichiers ZFS permet à certaines tâches d'administration d'être déléguées à des utilisateurs spécifiques. Pour plus d'informations sur l'administration déléguée, reportez-vous au [Chapitre 9](#), “Administration déléguée de ZFS dans Oracle Solaris” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.
- 2 **Activez l'analyse de virus sur un système de fichiers ZFS, par exemple, pool/volumes/vol1.**  
`# zfs set vscan=on path/pool/volumes/vol1`

## ▼ Procédure d'activation du service vscan

**Avant de commencer**

Le profil de droits VSCAN doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.
- 2 **Utilisez la commande `svcadm(1M)` pour activer l'analyse de virus.**  
`# svcadm enable vscan`

## ▼ Procédure d'ajout d'un moteur d'analyse

**Avant de commencer**

Le profil de droits VSCAN doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.
- 2 **Pour ajouter un moteur d'analyse au service vscan avec les propriétés par défaut, tapez :**  
`#vscanadm add-engine engine_ID`  
Reportez-vous à la page de manuel relative à la commande `vscanadm(1M)` pour obtenir une description de la commande.

## ▼ Procédure d'affichage des propriétés vscan

### Avant de commencer

Le profil de droits VSCAN doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175.](#)

#### 2 Affichez les propriétés du service vscan, de tous les moteurs d'analyse ou d'un moteur d'analyse spécifique.

##### ■ Pour afficher les propriétés d'un moteur d'analyse spécifique, tapez :

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

##### ■ Pour visualiser les propriétés de tous les moteurs d'analyse, tapez :

```
# vscanadm get-engine
```

##### ■ Pour afficher l'une des propriétés du service vscan, tapez :

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

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

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

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

## ▼ Procédure de modification des propriétés vscan

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

### Avant de commencer

Le profil de droits VSCAN doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175.](#)

#### 2 Affichez les propriétés actuelles en utilisant la commande `vscanadm show`.

- 3 Définissez la taille maximale d'analyses anti-virus sur 128 Mo par exemple.

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

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

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

Reportez-vous à la page de manuel relative à la commande `vscanadm(1M)` pour obtenir une description de la commande.

## ▼ Procédure d'exclusion de fichiers des analyses antivirus

Lorsque vous activez une protection antivirus, vous pouvez indiquer que tous les fichiers de types spécifiques doivent être exclus de l'analyse antivirus. Dans la mesure où le service `vscan` affecte les performances du système, vous pouvez conserver les ressources système en ciblant des types de fichiers spécifiques pour les analyses de virus.

### Avant de commencer

Le profil de droits `VSCAN` doit vous avoir été attribué.

- 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

- 2 Affichez la liste de tous les types de fichiers inclus dans la recherche de virus.

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

- 3 Spécifiez les types de fichiers devant faire l'objet d'une analyse de virus :

- Excluez un type de fichier spécifique, par exemple le type JPEG, de l'analyse de virus.

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

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

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

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



## Contrôle de l'accès aux périphériques (tâches)

---

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

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

- “Configuration des périphériques (liste des tâches)” à la page 81
- “Configuration de la stratégie de périphériques (tâches)” à la page 82
- “Gestion de l'allocation de périphériques (tâches)” à la page 85
- “Allocation de périphériques (tâches)” à la page 91
- “Protection de périphériques (référence)” à la page 94

Pour des informations générales sur la protection des périphériques, reportez-vous à la section “Contrôle de l'accès aux périphériques” à la page 43.

### Configuration des périphériques (liste des tâches)

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

Tâche	Voir
Gestion de la stratégie de périphériques.	“Configuration de la stratégie de périphériques (liste des tâches)” à la page 82
Gestion de l'allocation de périphériques.	“Gestion de l'allocation des périphériques (liste des tâches)” à la page 85
Utilisation de l'allocation de périphériques.	“Allocation de périphériques (tâches)” à la page 91

# Configuration de la stratégie de périphériques (tâches)

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

## Configuration de la stratégie de périphériques (liste des tâches)

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

Tâche	Description	Voir
Affichage de la stratégie pour les périphériques de votre système.	Dresse la liste des périphériques et des stratégies correspondantes.	<a href="#">“Procédure d’affichage de la stratégie de périphériques” à la page 82</a>
Demande de privilège pour l'utilisation de périphériques.	Utilise des privilèges pour protéger un périphérique.	<a href="#">“Procédure de modification de la stratégie pour un périphérique existant” à la page 83</a>
Suppression des exigences concernant les privilèges pour un périphérique.	Supprime ou réduit les privilèges requis pour accéder à un périphérique	<a href="#">Exemple 5–3</a>
Audit des modifications apportées à la stratégie de périphériques.	Enregistre les modifications apportées à la stratégie de périphériques dans la piste d'audit.	<a href="#">“Procédure d’audit des modifications apportées à la stratégie de périphériques” à la page 84</a>
Accès à /dev/arp.	Récupère des informations d'Oracle Solaris IP MIB-II.	<a href="#">“Procédure de récupération d’informations IP MIB-II à partir d’un périphérique /dev/*” à la page 84</a>

### ▼ Procédure d’affichage de la stratégie de périphériques

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

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

**Exemple 5–1** Affichage de la stratégie pour un périphérique spécifique

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

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

## ▼ Procédure de modification de la stratégie pour un périphérique existant

### Avant de commencer

Le profil de droits Device Security (sécurité des périphériques) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Ajoutez une stratégie à un périphérique.

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

-a                      Spécifie une *policy* pour un *device-driver*.

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

*device-driver*        Pilote du périphérique.

Pour plus d'informations, reportez-vous à la page de manuel [update\\_drv\(1M\)](#).

### Exemple 5–2 Ajout d'une stratégie à un périphérique existant

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

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

**Exemple 5-3** Suppression d'une stratégie d'un périphérique

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

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

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

Par défaut, la classe d'audit as inclut l'événement d'audit AUE\_MODDEVPLCY.

### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.
- 2 **Présélectionnez la classe d'audit incluant l'événement d'audit AUE\_MODDEVPLCY.**

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

Pour des instructions détaillées, reportez-vous à la section [“Procédure de présélection des classes d'audit”](#) à la page 585.

## ▼ Procédure de récupération d'informations IP MIB-II à partir d'un périphérique /dev/\*

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

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

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
```

```
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
/dev/arp
read_priv_set=none
write_priv_set=none
```

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

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

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

# Gestion de l'allocation de périphériques (tâches)

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

## Gestion de l'allocation des périphériques (liste des tâches)

La liste des tâches suivante présente les procédures permettant d'activer et de configurer l'allocation de périphériques. L'allocation de périphériques n'est pas activée par défaut. Une fois l'allocation de périphériques activée, reportez-vous à la section [“Allocation de périphériques \(tâches\)” à la page 91](#) pour obtenir les instructions relatives à l'allocation des périphériques.

Tâche	Description	Voir
Procédure pour rendre un périphérique allouable.	Permet d'allouer un périphérique à un utilisateur à la fois.	<a href="#">“Procédure d'activation de l'allocation de périphériques” à la page 86</a>
Désactivation de l'allocation de périphériques.	Supprime des restrictions d'allocation de tous les périphériques.	
Octroi de l'autorisation d'allouer un périphérique à des utilisateurs.	Attribue des autorisations d'allocation de périphériques aux utilisateurs.	<a href="#">“Procédure d'autorisation des utilisateurs à allouer un périphérique” à la page 87</a>
Affichage des périphériques allouables sur votre système.	Dresse la liste des périphériques allouables et de leur état.	<a href="#">“Procédure d'affichage d'informations d'allocation sur un périphérique” à la page 88</a>

Tâche	Description	Voir
Allocation forcée d'un périphérique.	Alloue un périphérique à un utilisateur ayant un besoin immédiat.	<a href="#">“Allocation forcée d'un périphérique” à la page 88</a>
Libération forcée d'un périphérique.	Libère un périphérique actuellement alloué à un utilisateur.	<a href="#">“Libération forcée d'un périphérique” à la page 89</a>
Modification des propriétés d'allocation d'un périphérique.	Modifie les conditions requises pour allouer un périphérique.	<a href="#">“Procédure de modification des périphériques pouvant être alloués” à la page 89</a>
Création d'un script de nettoyage de périphériques.	Purge les données d'un périphérique physique.	<a href="#">“Ecriture de nouveaux scripts de nettoyage de périphériques” à la page 102</a>
Audit de l'allocation de périphériques.	Enregistre l'allocation de périphériques dans la piste d'audit.	<a href="#">“Procédure d'audit de l'allocation de périphériques” à la page 90</a>

## ▼ Procédure d'activation de l'allocation de périphériques

**Avant de commencer**

Le profil de droits Device Security (sécurité des périphériques) doit vous avoir été attribué.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

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

```
# svcadm enable svc:/system/device/allocate
# svcs -x allocate
svc:/system/device/allocate:default (device allocation)
State: online since September 10, 2011 01:10:11 PM PDT
See: allocate(1)
See: deallocate(1)
See: list_devices(1)
See: device_allocate(1M)
See: mkdevalloc(1M)
See: mkdevmaps(1M)
See: dminfo(1M)
See: device_maps(4)
See: /var/svc/log/system-device-allocate:default.log
Impact: None.
```

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

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

## ▼ Procédure d'autorisation des utilisateurs à allouer un périphérique

### Avant de commencer

Le profil de droits User Security (sécurité des utilisateurs) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

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

Généralement, vous créez un profil de droits qui inclut l'autorisation `solaris.device.allocate`. Suivez les instructions fournies à la section [“Procédure de création ou de modification d'un profil de droits” à la page 186](#). Donnez au profil de droits les propriétés appropriées, telles que les suivantes :

- Nom du profil de droits : `Device Allocation`
- Autorisations accordées : `solaris.device.allocate`
- Commandes avec attributs de sécurité : dans la base de données `exec_attr`, `mount` avec le privilège `sys_mount` et `umount` avec le privilège `sys_mount`

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

Suivez les instructions fournies à la section [“Procédure de création d'un rôle” à la page 181](#). Utilisez les propriétés de rôle suivantes, données à titre d'exemple :

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

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

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

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

Pour consulter des exemples d'allocation de média amovible, reportez-vous à la section [“Procédure d'allocation des périphériques” à la page 91](#).

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

### Avant de commencer

Vous avez terminé “[Procédure d'activation de l'allocation de périphériques](#)” à la page 86.

Le profil de droits Device Security (sécurité des périphériques) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

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

```
# list_devices device-name
```

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

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

### Erreurs fréquentes

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

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

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

## ▼ Allocation forcée d'un périphérique

L'allocation forcée est utilisée lorsque quelqu'un a oublié de libérer un périphérique.

L'allocation forcée peut également être utilisée lorsqu'un utilisateur a un besoin immédiat d'un périphérique.

### Avant de commencer

L'autorisation `solaris.device.revoke` doit vous avoir été attribuée.

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

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



## 2 Forcez l'allocation du périphérique à l'utilisateur nécessitant le périphérique.

Dans cet exemple, le lecteur de bande est alloué de force à l'utilisateur j doe.

```
$ allocate -U jdoe
```

## ▼ Libération forcée d'un périphérique

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

### Avant de commencer

L'autorisation `solaris.device.revoke` doit vous avoir été attribuée.

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

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

## 2 Forcez la libération du périphérique.

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

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

## ▼ Procédure de modification des périphériques pouvant être alloués

### Avant de commencer

L'allocation de périphériques doit être activée pour cette procédure s'exécute correctement. Pour activer l'allocation de périphériques, reportez-vous à la section [“Procédure d'activation de l'allocation de périphériques”](#) à la page 86. Vous devez être connecté en tant que superutilisateur.

## ● Spécifiez si l'autorisation est requise ou indiquez l'autorisation `solaris.device.allocate`.

Modifiez le cinquième champ dans l'entrée de périphérique du fichier `device__allocate`.

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

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

### Exemple 5-4 Attribution de l'autorisation d'allouer un périphérique à n'importe quel utilisateur

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

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

### Exemple 5-5 Interdiction d'utilisation de certains périphériques

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

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

### Exemple 5-6 Interdiction d'utilisation de tous les périphériques

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

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

## ▼ Procédure d'audit de l'allocation de périphériques

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

#### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Présélectionnez la classe d'audit `ot`.

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

Pour des instructions détaillées, reportez-vous à la section [“Procédure de présélection des classes d'audit”](#) à la page 585.

# Allocation de périphériques (tâches)

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

## ▼ Procédure d'allocation des périphériques

### Avant de commencer

L'allocation de périphériques doit être activée, comme décrit à la section [“Procédure d'activation de l'allocation de périphériques”](#) à la page 86. Si une autorisation est requise, l'utilisateur doit disposer de l'autorisation.

#### 1 Allouez le périphérique.

Spécifiez le périphérique en indiquant son nom.

```
% allocate device-name
```

#### 2 Vérifiez que le périphérique est alloué.

Exécutez la même commande.

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

### Exemple 5-7 Allocation d'un microphone

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

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

### Exemple 5-8 Allocation d'une imprimante

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

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

Pour obtenir un exemple de libération forcée, reportez-vous à la section [“Libération forcée d'un périphérique”](#) à la page 89.

### Exemple 5-9 Allocation d'un lecteur de bande

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

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

### Erreurs fréquentes

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

## ▼ Procédure de montage d'un périphérique alloué

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

### Avant de commencer

Vous avez alloué le périphérique. Vous recevez les privilèges qui sont nécessaires pour monter le périphérique. Pour accorder les privilèges requis, reportez-vous à la [“Procédure d'autorisation des utilisateurs à allouer un périphérique”](#) à la page 87.

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

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

#### 2 Créez et protégez un point de montage dans le répertoire personnel du rôle.

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

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

#### 3 Répertoriez les périphériques allouables.

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

#### 4 Allouez le périphérique.

Spécifiez le périphérique en indiquant son nom.

```
$ allocate device-name
```

#### 5 Montez le périphérique.

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

où

-o ro Indique que le périphérique doit être monté en lecture seule. Utilisez  
-o rw pour indiquer que vous devez être en mesure d'écrire sur le  
périphérique.

<code>-F filesystem-type</code>	Indique le format du système de fichiers du périphérique. En règle générale, un CD-ROM est formaté avec un système de fichiers HSFS. Une disquette est généralement formatée avec un système de fichiers PCFS.
<code>device-path</code>	Indique le chemin d'accès au périphérique. La sortie de la commande <code>list_devices -l</code> inclut le <code>device-path</code> .
<code>mount-point</code>	Indique le point de montage que vous avez créé à l' <a href="#">Étape 2</a> .

### Exemple 5–10 Allocation d'une unité de CD-ROM

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

```
% roles
devicealloc
% su - devicealloc
Password: <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
List of the contents of CD-ROM
```

#### Erreurs fréquentes

Si la commande `mount` ne peut pas monter le périphérique, un message d'erreur s'affiche :  
`mount: insufficient privileges. Vérifiez les points suivants :`

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

Contactez votre administrateur si vous ne pouvez toujours pas monter le périphérique alloué.

## ▼ Procédure de libération des périphériques

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

**Avant de commencer**

Vous devez avoir alloué le périphérique.

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

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

**2 Libérez le périphérique.**

```
$ deallocate device-name
```

**Exemple 5–11 Libération d'un microphone**

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

```
% whoami
jdoe
% deallocate audio0
```

**Exemple 5–12 Libération d'une unité de CD-ROM**

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

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

## Protection de périphériques (référence)

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

## Commandes de la stratégie de périphériques

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

Le tableau suivant répertorie les commandes de gestion des périphériques.

TABLEAU 5-1 Commandes de gestion des périphériques

Page de manuel pour les commandes	Objectif
<code>devfsadm(1M)</code>	<p>Administre des périphériques et des pilotes de périphériques sur un système en cours d'exécution. Charge également la stratégie de périphériques.</p> <p>La commande <code>devfsadm</code> permet de nettoyer des liens <code>/dev</code> lâches vers des disques, des bandes, des ports, des périphériques audio et des pseudopériphériques. Des périphériques d'un pilote nommé peuvent également être reconfigurés.</p>
<code>getdevpolicy(1M)</code>	<p>Affiche la stratégie associée à un ou plusieurs périphériques. Cette commande peut être exécutée par n'importe quel utilisateur.</p>
<code>add_drv(1M)</code>	<p>Ajoute un nouveau pilote de périphérique à un système en cours d'exécution. Contient des options pour ajouter une stratégie au nouveau périphérique. En règle générale, cette commande est appelée dans un script lorsqu'un pilote de périphérique est en cours d'installation.</p>
<code>update_drv(1M)</code>	<p>Met à jour les attributs d'un pilote de périphérique existant. Contient des options pour mettre à jour la stratégie de périphériques pour le périphérique. En règle générale, cette commande est appelée dans un script lorsqu'un pilote de périphérique est en cours d'installation.</p>
<code>rem_drv(1M)</code>	<p>Supprime un périphérique ou un pilote de périphérique.</p>

## Allocation de périphériques

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

## Composants de l'allocation de périphériques

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

- Le service `svc:/system/device/allocate`. Pour plus d'informations, reportez-vous à la page de manuel [smf\(5\)](#) et aux pages de manuel concernant les commandes d'allocation de périphériques.
- Les commandes `allocate`, `deallocate`, `dminfo` et `list_devices`. Pour plus d'informations, reportez-vous à la section “[Commandes d'allocation de périphériques](#)” à la page 97.
- Les profils de droits Device Management (gestion des périphériques) et Device Security (sécurité des périphériques). Pour plus d'informations, reportez-vous à la section “[Profils de droits Device Allocation \(allocation de périphériques\)](#)” à la page 96.
- Les scripts de nettoyage de périphériques pour chaque périphérique allouable.

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

- Le fichier `/etc/security/device_allocate`. Pour plus d'informations, reportez-vous à la page de manuel [device\\_allocate\(4\)](#).
- Le fichier `/etc/security/device_maps`. Pour plus d'informations, reportez-vous à la page de manuel [device\\_maps\(4\)](#).
- Un fichier de verrouillage, dans le répertoire `/etc/security/dev`, pour chaque périphérique allouable.
- Les attributs modifiés du fichier de verrouillage qui sont associés à chaque périphérique allouable.

---

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

---

## Service d'allocation de périphériques

Le service `svc:/system/device/allocate` contrôle l'allocation de périphériques. Ce service est désactivé par défaut. Pour activer le service, exécutez la commande `svcadm enable svc:/system/device/allocate`.

## Profils de droits Device Allocation (allocation de périphériques)

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

Ces profils de droits comprennent les autorisations suivantes :

- `solaris.device.allocate` : nécessaire pour allouer un périphérique
- `solaris.device.cdrw` : nécessaire pour lire et écrire un CD-ROM



- `solaris.device.config` : nécessaire pour configurer les attributs d'un périphérique
- `solaris.device.grant` : nécessaire pour déléguer à un autre utilisateur les autorisations des périphériques qui vous sont affectées
- `solaris.device.mount.alloptions.fixed` : nécessaire pour spécifier des options de montage lors du montage d'un périphérique fixe
- `solaris.device.mount.alloptions.removable` : nécessaire pour spécifier des options de montage lors du montage d'un périphérique amovible
- `solaris.device.mount.fixed` : nécessaire pour monter un périphérique fixe
- `solaris.device.mount.removable` : nécessaire pour monter un périphérique amovible
- `solaris.device.revoke` : nécessaire pour révoquer ou récupérer un périphérique

## Commandes d'allocation de périphériques

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

TABLEAU 5-2 Commandes d'allocation de périphériques

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

## Autorisations pour les commandes d'allocation

Par défaut, les utilisateurs doivent avoir l'autorisation `solaris.device.allocate` pour réserver un périphérique allouable. Pour créer un profil de droits afin d'inclure l'autorisation

`solaris.device.allocate`, reportez-vous à la section [“Procédure d'autorisation des utilisateurs à allouer un périphérique” à la page 87](#).

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

Pour plus d'informations, reportez-vous à la section [“Commandes sélectionnées nécessitant des autorisations” à la page 224](#).

## Etat d'erreur d'allocation

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

La commande `deallocate` avec l'option `-F` force la libération. Vous pouvez également utiliser `allocate -U` pour affecter le périphérique à un utilisateur. Une fois le périphérique alloué, vous pouvez analyser les messages d'erreur qui s'affichent. Après la correction des problèmes liés au périphérique, vous pouvez forcer la libération.

## Fichier `device_maps`

Des cartes de périphériques sont créées lorsque vous paramétrez l'allocation de périphériques. Le fichier `/etc/security/device_maps` inclut les noms de périphérique, types de périphérique, fichiers spécifiques au périphérique qui sont associés à chaque périphérique allouable.

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

Chaque périphérique est représenté par une entrée d'une ligne au format suivant :

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

### EXEMPLE 5-13 Exemple d'entrée `device_maps`

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

**EXEMPLE 5-13** Exemple d'entrée `device_maps` (Suite)

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

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

- device-name* Spécifie le nom du périphérique. Pour obtenir une liste des noms de périphériques courants, reportez-vous à la section [“Procédure d'affichage d'informations d'allocation sur un périphérique” à la page 88](#).
- device-type* Spécifie le type de périphérique générique. Le nom générique est le nom de la classe de périphériques, comme `st`, `fd`, `rmdisk` ou `audio`. Le champ *device-type* regroupe logiquement les périphériques liés.
- device-list* Répertoire les fichiers spécifiques à un périphérique qui sont associés au périphérique physique. *device-list* doit contenir tous les fichiers spécifiques qui permettent d'accéder à un périphérique en particulier. Si la liste est incomplète, un utilisateur malveillant peut toujours obtenir ou modifier des informations privées. Les entrées valides pour le champ *device-list* reflètent les fichiers de périphériques qui sont situés dans le répertoire `/dev`.

## Fichier `device_allocate`

Vous pouvez modifier le fichier `/etc/security/device_allocate` pour rendre des périphériques allouables non allouables ou pour ajouter de nouveaux périphériques. Un exemple de fichier `device_allocate` est indiqué ci-après.

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

Une entrée dans le fichier `device_allocate` ne signifie pas que le périphérique est allouable, sauf si l'entrée stipule spécifiquement que le périphérique est allouable. Dans l'exemple de fichier `device_allocate`, notez l'astérisque (\*) dans le cinquième champ de l'entrée de périphérique `audio`. Un astérisque dans le cinquième champ indique au système que le périphérique n'est pas allouable. Par conséquent, le périphérique ne peut pas être utilisé. D'autres valeurs ou aucune valeur dans ce champ indiquent que le périphérique peut être utilisé.

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

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

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

<i>device-name</i>	Spécifie le nom du périphérique. Pour obtenir une liste des noms de périphériques courants, reportez-vous à la section <a href="#">“Procédure d'affichage d'informations d'allocation sur un périphérique” à la page 88</a> .
<i>device-type</i>	Spécifie le type de périphérique générique. Le nom générique est le nom de la classe de périphériques, tel que <code>st</code> , <code>fd</code> et <code>sr</code> . Le champ <i>device-type</i> regroupe logiquement les périphériques liés. Lorsque vous rendez un périphérique allouable, récupérez le nom du périphérique du champ <i>device-type</i> dans le fichier <code>device_maps</code> .
<i>reserved</i>	Sun se réserve les deux champs qui sont marqués <code>reserved</code> pour une utilisation ultérieure.
<i>auths</i>	Indique si le périphérique est allouable. Un astérisque (*) dans ce champ indique que le périphérique n'est pas allouable. Une chaîne d'autorisation ou un champ vide indique que le périphérique est allouable. Par exemple, la chaîne <code>solaris.device.allocate</code> dans le champ <i>auths</i> indique que l'autorisation <code>solaris.device.allocate</code> est requise pour allouer le périphérique. Un signe arobase (@) dans ce fichier indique que le périphérique est allouable par n'importe quel utilisateur.
<i>device-exec</i>	Fournit le nom de chemin d'un script à invoquer pour une manipulation spéciale, telle que le nettoyage et la protection contre la réutilisation des objets durant le processus d'allocation. Le script <i>device-exec</i> est exécuté chaque fois qu'une commande <code>deallocate</code> est effectuée sur le périphérique.

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

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

Vous pouvez décider d'accepter les périphériques par défaut et leurs caractéristiques définies. Après l'installation d'un nouveau périphérique, vous pouvez modifier les entrées. Tout périphérique devant être alloué avant l'utilisation doit être défini dans les fichiers `device_allocate` et `device_maps` pour le système de ce périphérique. Actuellement, les lecteurs de bande de cartouche, unités de disquette, unités de CD-ROM, périphériques de

médias amovibles et puces audio sont considérés comme allouables. Ces types de périphériques disposent de scripts de nettoyage de périphériques.

---

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

---

## Scripts de nettoyage de périphériques

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

### Script de nettoyage de périphériques pour bandes

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

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

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

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

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

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

- **scriptfd\_clean** : script de nettoyage de périphériques pour disquettes.
- **script sr\_clean** : script de nettoyage de périphériques pour unités de CD-ROM.

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

## Script de nettoyage de périphériques audio

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

## Ecriture de nouveaux scripts de nettoyage de périphériques

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

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

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

- I Requis uniquement lors de l'initialisation du système. Toutes les sorties doivent aller à la console du système. L'échec ou l'incapacité à éjecter de force le média doivent mettre le périphérique dans l'état d'erreur d'allocation.
- i Similaire à l'option `-I`, à l'exception du fait que la sortie est supprimée.
- f Pour le nettoyage forcé. L'option est interactive et suppose que l'utilisateur est disponible pour répondre aux invites. Un script exécuté avec cette option doit tenter de terminer le nettoyage si une partie du nettoyage échoue.
- S Pour le nettoyage standard. L'option est interactive et suppose que l'utilisateur est disponible pour répondre aux invites.

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

---

Ce chapitre décrit la création d'un manifeste des fichiers sur un système et son utilisation pour vérifier l'intégrité du système. L'outil de génération de rapports d'audit de base (BART) permet de valider de manière exhaustive les systèmes en effectuant des vérifications d'un système dans le temps au niveau des fichiers.

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

- [“Outil de génération de rapports d'audit de base \(présentation\)” à la page 103](#)
- [“Utilisation de BART \(tâches\)” à la page 106](#)
- [“Manifestes BART, fichiers de règles et rapports \(référence\)” à la page 118](#)

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

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

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

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

## Fonctionnalités BART

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

Les utilisations et avantages supplémentaires de BART sont les suivants :

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

## Composants BART

BART comporte deux composants principaux et un composant facultatif :

- Manifeste BART
- Rapport BART
- Fichier de règles BART

### Manifeste BART

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



---

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

---

Pour plus d'informations sur les manifestes BART, reportez-vous à la section “[Format de fichier manifeste BART](#)” à la page 118.

## Rapport BART

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

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

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

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

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

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

Pour plus d'informations sur les rapports BART, reportez-vous à la section “[Génération de rapports BART](#)” à la page 120.

## Fichier de règles BART

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

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

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

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

---

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

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

---

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

Pour plus d'informations sur le fichier de règles BART, reportez-vous à la section “[Format de fichier de règles BART](#)” à la page 119 et à la page de manuel `bart_rules(4)`.

## Utilisation de BART (tâches)

Vous pouvez exécuter la commande `bart` en tant qu'utilisateur standard, superutilisateur ou utilisateur ayant endossé un rôle. Si vous exécutez la commande `bart` en tant qu'utilisateur standard, vous pouvez uniquement classifier et surveiller des fichiers pour lesquels vous disposez d'une autorisation d'accès, tels que des fichiers dans votre répertoire personnel. L'avantage de vous connecter en tant que superutilisateur lorsque vous exécutez la commande `bart` est que les manifestes que vous créez contiennent des informations sur les fichiers cachés et privés que vous souhaitez peut-être surveiller. Si vous avez besoin de classifier des informations sur des fichiers disposant d'autorisations restreintes, par exemple, le fichier `/etc/passwd` ou `/etc/shadow`, exécutez la commande `bart` en tant que superutilisateur. Pour

plus d'informations sur l'utilisation du contrôle d'accès basé sur le rôle, reportez-vous à la section "[Contrôle d'accès basé sur les rôles \(présentation\)](#)" à la page 145.

## Considérations de sécurité BART

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

---

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

---

## Utilisation de BART (liste des tâches)

Tâche	Description	Voir
Création d'un manifeste BART.	Génère une liste d'informations sur chaque fichier installé sur un système.	"Procédure de création d'un manifeste" à la page 108
Création d'un manifeste BART personnalisé.	Génère une liste d'informations sur des fichiers spécifiques installés sur un système.	"Procédure de personnalisation d'un manifeste" à la page 110
Comparaison de manifestes BART.	Génère un rapport qui compare les modifications apportées à un système dans le temps.  Ou génère un rapport qui compare un ou plusieurs systèmes pour contrôler le système.	"Procédure de comparaison des manifestes pour le même système dans le temps" à la page 111  "Procédure de comparaison de manifestes de différents systèmes" à la page 113
(Facultatif) Personnalisation d'un rapport BART.	Génère un rapport BART personnalisé de l'une des manières suivantes : <ul style="list-style-type: none"> <li>■ En spécifiant des attributs.</li> <li>■ En utilisant un fichier de règles</li> </ul>	"Procédure de personnalisation d'un rapport BART en spécifiant des attributs de fichiers" à la page 115  "Procédure de personnalisation d'un rapport BART en utilisant un fichier de règles" à la page 116

## ▼ Procédure de création d'un manifeste

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

### Avant de commencer

Pour créer un manifeste système, vous devez posséder le rôle root.

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

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

- R Spécifie le répertoire root pour le manifeste. Tous les chemins d'accès spécifiés par les règles sont interprétés par rapport à ce répertoire. Tous les chemins d'accès signalés dans le manifeste sont relatifs à ce répertoire.
- I Accepte une liste de fichiers individuels à classer, soit sur la ligne de commande soit à lire dans l'entrée standard.
- r Nom du fichier de règles pour ce manifeste. Notez que –, lorsqu'il est utilisé avec l'option -r, lit le fichier de règles dans l'entrée standard.
- n Désactive les signatures de contenu de tous les fichiers standard dans la liste de fichiers. Cette option peut être utilisée pour améliorer les performances. Ou bien vous pouvez l'utiliser s'il est prévu que le contenu de la liste de fichiers change, comme dans le cas des fichiers journaux du système.

#### 2 Examinez le contenu du manifeste.

#### 3 Enregistrez le manifeste pour une utilisation ultérieure.

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

### Exemple 6–1 Création d'un manifeste répertoriant des informations sur chaque fichier d'un système

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

Par exemple :

```
# bart create
! Version 1.1
! HASH SHA256
! Wednesday, September 07, 2011 (22:22:27)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 1024 40755 user::rwx,group::r-x,mask:r-x,other:r-x
3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090 0 0
.
.
.
/zone D 512 40755 user::rwx group::r-x,mask:r-x,other:r-x 3f81e892
154de3e7bdfd0d57a074c9fae0896a9e2e04bebfe5e872d273b063319e57f334 0 0
.
.
.
```

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

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

## ▼ Procédure de personnalisation d'un manifeste

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

- En spécifiant une sous-arborescence

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

- En spécifiant un nom de fichier

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

- En utilisant un fichier de règles

Vous utilisez un fichier de règles pour créer des manifestes personnalisés qui répertorient des informations sur des fichiers spécifiques et des sous-arborescences spécifiques sur un système donné. Vous pouvez également utiliser un fichier de règles pour contrôler des attributs de fichiers spécifiques. L'utilisation d'un fichier de règles pour créer et comparer des manifestes vous donne la possibilité de spécifier des attributs multiples pour plusieurs fichiers ou sous-arborescences. En revanche, à partir de la ligne de commande, vous ne pouvez indiquer qu'une définition d'attribut globale qui s'applique à tous les fichiers pour chaque manifeste que vous créez ou chaque rapport que vous générez.

### Avant de commencer

Vous devez être dans le rôle `root`.

- 1 Déterminez les fichiers que vous souhaitez classifier et surveiller.
- 2 Après l'installation du logiciel Oracle Solaris, créez un manifeste personnalisé à l'aide de l'une des options suivantes :

- En spécifiant une sous-arborescence :

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

- En spécifiant un ou des noms de fichiers :

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

Par exemple :

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

- En utilisant un fichier de règles :

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

- 3 Examinez le contenu du manifeste.
- 4 Enregistrez le manifeste pour une utilisation ultérieure.

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

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

### Avant de commencer

Pour créer et comparer des manifestes qui incluent des objets publics, vous devez posséder le rôle root.

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

```
# bart create -R /etc > control-manifest
```
- 2 Créez un manifeste de test préparé exactement de la même façon que le manifeste de contrôle chaque fois que vous voulez surveiller les modifications apportées au système.  

```
# bart create -R /etc > test-manifest
```
- 3 Comparez le manifeste de contrôle à celui de test.  

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

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

## 4 Recherchez les singularités dans le rapport BART

### Exemple 6-2 Comparaison des manifestes pour le même système dans le temps

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

- Créez un manifeste de contrôle.

```
# bart create -R /etc > system1.control.090711
! Version 1.1
! HASH SHA256
! Wednesday, September 07, 2011 (11:11:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/.cpr_config F 2236 100644 owner@:read_data/write_data/append_data/read_xattr/wr
ite_xattr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchr
onize:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:all
ow,everyone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4e271c59 0 0 3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
/.login F 1429 100644 owner@:read_data/write_data/append_data/read_xattr/write_x
attr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize
:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow,ev
eryone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4bf9d6d7 0 3 ff6251a473a53de68ce8b4036d0f569838cff107caf1dd9fd04701c48f09242e
.
.
.
```

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

```
# bart create -R /etc > system1.test.101011
Version 1.1
! HASH SHA256
! Monday, October 10, 2011 (10:10:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/.cpr_config F 2236 100644 owner@:read_data/write_data/append_data/read_xattr/wr
ite_xattr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchr
onize:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:all
ow,everyone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4e271c59 0 0 3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
```



- - 
  - 
  - Comparez le manifeste de contrôle à celui de test.
- ```
# bart compare system1.control.090711 system1.test.101011
/security/audit_class
mtime 4f272f59
```

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

## ▼ Procédure de comparaison de manifestes de différents systèmes

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

### Avant de commencer

Pour comparer les manifestes système, vous devez posséder le rôle `root`.

#### 1 Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle.

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

#### 2 Enregistrez le manifeste de contrôle.

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

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

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

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

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

Par exemple :

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

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

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

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

- 7 Recherchez les singularités dans le rapport BART

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

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

### Exemple 6-3 Comparaison de manifestes de différents systèmes avec le manifeste d'un système de contrôle

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

- Créez un manifeste de contrôle.

```
# bart create -R /usr/bin > control-manifest.090711
! Version 1.1
! HASH SHA256
! Wednesday, September 07, 2011 (11:11:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/2to3 F 105 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4bf9d261 0
2 154de3e7bdfd0d57a074c9fae0896a9e2e04bebf5e872d273b063319e57f334
/7z F 509220 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4dad48a 0
2 3ecd418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
...
```

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

```
# bart create -R /usr/bin > system2-manifest.101011
! Version 1.1
! HASH SHA256
! Monday, October 10, 2011 (10:10:22)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/2to3 F 105 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4bf9d261 0
2 154de3e7bdfd0d57a074c9fae0896a9e2e04bebf5e872d273b063319e57f334
...
```

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

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

- Comparez le manifeste de contrôle à celui de test.

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

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

## ▼ Procédure de personnalisation d'un rapport BART en spécifiant des attributs de fichiers

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

**Avant de commencer**

Vous devez être dans le rôle root.

- 1 **Déterminez les attributs de fichier que vous voulez surveiller.**
- 2 **Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle.**
- 3 **Créez un manifeste de test lorsque vous voulez surveiller les modifications.**  
Préparez le manifeste de test exactement de la même façon que le manifeste de contrôle.
- 4 **Comparez les manifestes.**  
Par exemple :  

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

  
Notez qu'une virgule sépare chaque attribut que vous indiquez dans la syntaxe de la ligne de commande.
- 5 **Recherchez les singularités dans le rapport BART**

## ▼ Procédure de personnalisation d'un rapport BART en utilisant un fichier de règles

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

**Avant de commencer**

Vous devez être dans le rôle root.

- 1 **Déterminez les fichiers et attributs de fichier que vous voulez surveiller.**
- 2 **Utilisez un éditeur de texte pour créer un fichier de règles avec les directives appropriées.**
- 3 **Après l'installation du logiciel Oracle Solaris, créez un manifeste de contrôle à l'aide du fichier de règles que vous avez créé.**  

```
# bart create -r rules-file > control-manifest
```
- 4 **Créez un manifeste de test préparé exactement de la même façon que le manifeste de contrôle.**  

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

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

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

**6 Recherchez les singularités dans le rapport BART****Exemple 6-4 Personnalisation d'un rapport BART en utilisant un fichier de règles**

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

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

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

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

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

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

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

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

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

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

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

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

# Manifestes BART, fichiers de règles et rapports (référence)

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

## Format de fichier manifeste BART

Chaque entrée de fichier manifeste constitue une seule ligne, selon le type de fichier. Chaque entrée commence par *fname*, qui est le nom du fichier. Pour éviter les problèmes d'analyse provoqués par des caractères spéciaux incorporés dans les noms de fichiers, les noms de fichier sont codés. Pour plus d'informations, reportez-vous à la section [“Format de fichier de règles BART” à la page 119](#).

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

|                 |                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>type</i>     | Type de fichier avec les valeurs possibles suivantes : <ul style="list-style-type: none"> <li>▪ B pour un noeud de périphérique en mode bloc</li> <li>▪ C pour un noeud de périphérique en mode caractère</li> <li>▪ D pour un répertoire</li> <li>▪ F pour un fichier</li> <li>▪ L pour un lien symbolique</li> <li>▪ P pour un tuyau</li> <li>▪ S pour un socket</li> </ul> |
| <i>size</i>     | Taille de fichier en octets.                                                                                                                                                                                                                                                                                                                                                  |
| <i>mode</i>     | Nombre octal représentant les autorisations du fichier.                                                                                                                                                                                                                                                                                                                       |
| <i>acl</i>      | Attributs ACL du fichier. Pour un fichier avec des attributs ACL, contient la sortie de <code>acltotext()</code> .                                                                                                                                                                                                                                                            |
| <i>uid</i>      | ID utilisateur numérique du propriétaire de cette entrée.                                                                                                                                                                                                                                                                                                                     |
| <i>gid</i>      | L'ID de groupe numérique du propriétaire de cette entrée.                                                                                                                                                                                                                                                                                                                     |
| <i>dirmtime</i> | Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les répertoires.                                                                                                                                                                                                                                                               |
| <i>lnmtime</i>  | Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les liens.                                                                                                                                                                                                                                                                     |
| <i>mtime</i>    | Heure de la dernière modification, en secondes, depuis 00:00:00 UTC, le 1er janvier 1970, pour les fichiers.                                                                                                                                                                                                                                                                  |
| <i>contents</i> | Valeur de somme de contrôle du fichier. Cet attribut n'est défini que pour des fichiers standard. Si vous désactivez la vérification du contexte ou si les sommes de contrôle ne peuvent pas être calculées, la valeur de ce champ est –.                                                                                                                                     |
| <i>dest</i>     | Destination d'un lien symbolique.                                                                                                                                                                                                                                                                                                                                             |

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

Pour plus d'informations sur les manifestes BART, reportez-vous à la page de manuel [bart\\_manifest\(4\)](#).

## Format de fichier de règles BART

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

Les fichiers d'entrée ont trois types de directives :

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

### EXEMPLE 6-5 Format de fichier de règles

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

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

---

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

---

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

## Attributs du fichier de règles

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

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

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

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

## Syntaxe de citation

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

Pour plus d'informations sur le fichier de règles BART ou la syntaxe de citation, reportez-vous à la page de manuel [bart\\_rules\(4\)](#).

## Génération de rapports BART

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

```
CHECK all
IGNORE    dirmtime
```

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



## Sortie BART

Les valeurs de sortie renvoyées sont les suivantes :

- 0 Succès
- 1 Erreur non fatale lors du traitement de fichiers, telle que des problèmes d'autorisation
- >1 Erreur fatale, telle qu'une option de ligne de commande non valide

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

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

Par exemple :

```
filename attribute control:xxxx test:yyyy
```

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

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

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

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

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

Par exemple :

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

*filename* Identique à l'attribut *filename* dans le format par défaut

*Attribut control-val test-val* Description des attributs de fichier qui diffèrent entre les manifestes de contrôle et de test pour chaque fichier.

Pour obtenir une liste des attributs pris en charge par la commande `bart`, reportez-vous à la section “[Attributs du fichier de règles](#)” à la page 119.

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

## Contrôle de l'accès aux fichiers (tâches)

---

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

---

**Remarque** – Pour protéger les fichiers ZFS avec des ACL (listes de contrôle d'accès), reportez-vous au [Chapitre 8, “Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS”](#) du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

---

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

- “Utilisation des autorisations UNIX pour protéger les fichiers” à la page 123
- “Protection contre les problèmes de sécurité causés par les fichiers exécutables” à la page 131
- “Protection des fichiers avec des autorisations UNIX (liste des tâches)” à la page 132
- “Protection contre les programmes présentant des risques de sécurité (liste des tâches)” à la page 139

## Utilisation des autorisations UNIX pour protéger les fichiers

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

## Commandes d'affichage et de sécurisation des fichiers

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

TABLEAU 7-1 Commandes de sécurisation des fichiers et répertoires

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

## Propriété des fichiers et des répertoires

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

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

Le propriétaire du fichier peut généralement affecter ou modifier les autorisations de fichier. En outre, le compte root peut modifier la propriété d'un fichier. Pour remplacer la stratégie du système, reportez-vous à l'[Exemple 7-2](#).

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

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

## Autorisations des fichiers UNIX

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

TABLEAU 7-2 Autorisations des fichiers et répertoires

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

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

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

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

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

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

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

Il est recommandé de surveiller votre système pour toute utilisation non autorisée des autorisations `setuid` et `setgid` pour obtenir les capacités de superutilisateur. Une autorisation suspecte accorde la propriété d'un programme d'administration à un utilisateur plutôt qu'à root ou bin. Pour rechercher et afficher la liste de tous les fichiers qui utilisent ces autorisations spéciales, reportez-vous à la section [“Procédure de recherche de fichiers avec des autorisations de fichier spéciales” à la page 139](#).

## Autorisation `setuid`

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

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

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

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

---

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

---

## Autorisation `setgid`

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

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

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

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

Vous devez surveiller votre système pour toute utilisation non autorisée des autorisations `setgid` pour obtenir des capacités de superutilisateur. Des autorisations suspectes accordent l'accès de groupe à un tel programme à un groupe inhabituel plutôt qu'à `root` ou `bin`. Pour rechercher et afficher la liste de tous les fichiers qui utilisent ces autorisations, reportez-vous à la section [“Procédure de recherche de fichiers avec des autorisations de fichier spéciales”](#) à la page 139.

## Sticky Bit

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

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

Veillez à définir le sticky bit manuellement lorsque vous définissez un répertoire public directory dans un système de fichiers TMPFS. Pour plus d'instructions, reportez-vous à l'[Exemple 7-5](#).

## Valeur umask par défaut

Lorsque vous créez un fichier ou un répertoire, vous devez le créer avec un jeu d'autorisations par défaut. Les valeurs par défaut du système sont ouvertes. Un fichier texte dispose de 666 autorisations, et accorde des autorisations de lecture et d'écriture à tout le monde. Un répertoire et un fichier exécutable disposent de 777 autorisations, et accordent des autorisations de lecture, d'écriture et d'exécution à tout le monde. En règle générale, les utilisateurs remplacent les valeurs par défaut du système dans leurs fichiers d'initialisation du shell, tels que `.bashrc` et `.kshrc.user`. L'administrateur peut également définir des valeurs par défaut dans le fichier `/etc/profile`.

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

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

TABLEAU 7-3 Paramètres umask pour différents niveaux de sécurité

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

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

## Modes d'autorisation de fichier

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

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

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

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

TABLEAU 7-4 Définition des autorisations de fichiers en mode absolu

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



TABLEAU 7-4 Définition des autorisations de fichiers en mode absolu (Suite)

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

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

TABLEAU 7-5 Définition des autorisations de fichiers en mode symbolique

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

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

*who* Spécifie pour qui les autorisations doivent être modifiées.

*operator* Indique l'opération à effectuer.

*permissions*      Spécifie les autorisations à modifier.

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

TABLEAU 7-6 Définition des autorisations de fichiers spéciales en mode absolu

| Valeur octale | Autorisations de fichiers spéciales |
|---------------|-------------------------------------|
| 1             | Sticky bit                          |
| 2             | <code>setgid</code>                 |
| 4             | <code>setuid</code>                 |

## Utilisation des ACL pour protéger les fichiers UFS

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

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

**Remarque** – Pour les ACL dans le système de fichiers ZFS et les ACL sur les fichiers NFSv4, reportez-vous au [Chapitre 8, “Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS”](#) du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

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

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

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

|                   |                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>entry-type</i> | Type d'entrée d'ACL sur laquelle définir les autorisations de fichiers. Par exemple, <i>entry-type</i> peut être <i>user</i> (le propriétaire d'un fichier) ou <i>mask</i> (le masque ACL).                                              |
| <i>uid</i>        | Nom d'utilisateur ou ID d'utilisateur (UID).                                                                                                                                                                                             |
| <i>gid</i>        | Nom du groupe ou ID de groupe (GID).                                                                                                                                                                                                     |
| <i>perms</i>      | Représente les autorisations définies sur <i>entry-type</i> . <i>perms</i> peut être indiqué par les caractères symboliques <i>rwX</i> ou un nombre octal. Il s'agit des mêmes nombres que ceux utilisés avec la commande <i>chmod</i> . |

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

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



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

Pour plus d'informations sur les ACL sur les systèmes de fichiers UFS, reportez-vous au *System Administration Guide: Security Services* pour la version 10 d'Oracle Solaris.

## Protection contre les problèmes de sécurité causés par les fichiers exécutables

Programmes pour lire et écrire des données sur la pile. D'une manière générale, ils s'exécutent à partir de portions de mémoire en lecture seule qui sont spécifiquement désignées pour ce code. Certaines attaques provoquant des tampons sur la pile jusqu'au débordement tentent d'insérer un nouveau code sur la pile et forcent le programme à l'exécuter. Ces attaques peuvent être mises en échec en supprimant les autorisations d'exécution de la Suppression de droits d'exécution la mémoire de la pile. C'est-à-dire que la plupart de ces programmes peuvent fonctionner correctement sans utiliser les piles exécutables.

Les processus 64 bits ont toujours des piles non exécutables. La variable *noexec\_user\_stack* vous permet de spécifier si les piles des processus 32 bits sont exécutables. Pour se conformer à l'interface SPARC ABI 32 bits, la valeur par défaut est zéro, ce qui indique que la pile est exécutable.

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

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

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

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

Vous pouvez utiliser la fonction `mprotect()` si vous souhaitez que les programmes marquent explicitement leur pile comme exécutable. Pour plus d'informations, reportez-vous à la page de manuel [mprotect\(2\)](#). Vous pouvez également compiler votre programme avec `-M/usr/lib/ld/map.noexec` pour rendre la pile non exécutable indépendamment du paramètre à l'échelle du système.

## Protection des fichiers (tâches)

Les procédures d'installation suivantes permettent de protéger les fichiers avec des autorisations UNIX, localiser des fichiers présentant des risques liés à la sécurité et de protéger le système contre toute compromission par ces fichiers.

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

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

| Tâche                                              | Voir                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affichage des informations de fichier.             | <a href="#">“Procédure d’affichage des informations de fichier” à la page 133</a>                                                                                                                                                                                                                                                     |
| Modification des propriétaires de fichier locaux.  | <a href="#">“Procédure de modification du propriétaire d’un fichier” à la page 134</a><br><a href="#">“Procédure de modification de la propriété de groupe d’un fichier” à la page 135</a>                                                                                                                                            |
| Modification des autorisations de fichiers locaux. | <a href="#">“Procédure de modification des autorisations de fichier en mode symbolique” à la page 136</a><br><a href="#">“Procédure de modification des autorisations de fichier en mode absolu” à la page 137</a><br><a href="#">“Procédure de modification des autorisations de fichier spéciales en mode absolu” à la page 138</a> |

## ▼ Procédure d’affichage des informations de fichier

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

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

```
% ls -la
```

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

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

### Exemple 7–1 Affichage des informations de fichier

Dans l’exemple suivant, une liste partielle des fichiers placés dans le répertoire `/sbin` s’affiche.

```
% cd /sbin
% ls -la
total 4960
drwxr-xr-x  2 root    sys          64 Dec  8 11:57 ./
drwxr-xr-x 39 root    root         41 Dec  8 15:20 ../
-r-xr-xr-x  1 root    bin        21492 Dec  1 20:55 autopush*
-r-xr-xr-x  1 root    bin       33680 Oct  1 11:36 beadm*
-r-xr-xr-x  1 root    bin     184360 Dec  1 20:55 bootadm*
lrwxrwxrwx  1 root    root         21 Jun  7 2010 bpgetfile -> ...
-r-xr-xr-x  1 root    bin       86048 Dec  1 20:55 cryptoadm*
-r-xr-xr-x  1 root    bin       12828 Dec  1 20:55 devprop*
-r-xr-xr-x  1 root    bin     130132 Dec  1 20:55 dhcpagent*
-r-xr-xr-x  1 root    bin       13076 Dec  1 20:55 dhcpcinfo*

.
.
.
```

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

- Type de fichier : par exemple, d. Pour obtenir la liste des types de fichiers, reportez-vous à la section [“Propriété des fichiers et des répertoires”](#) à la page 124.
- Autorisations : par exemple, r-xr-xr-x. Pour obtenir une description, reportez-vous à la section [“Propriété des fichiers et des répertoires”](#) à la page 124.
- Nombre de liens fixes : par exemple, 2.
- Propriétaire du fichier : par exemple, root.
- Groupe du fichier : par exemple, bin.
- Taille du fichier, en octets : par exemple, 21308.
- Date à laquelle le fichier a été créé ou modifié pour la dernière fois : par exemple, Dec 9 15:55.
- Nom du fichier : par exemple, dhcpinfo.

## ▼ Procédure de modification du propriétaire d'un fichier

### Avant de commencer

Si vous n'êtes pas le propriétaire du fichier ou du répertoire, le profil de droits Object Access Management (gestion de l'accès aux objets) doit vous être affecté. Pour modifier un fichier qui est un [objet public](#), vous devez être connecté en tant que superutilisateur.

#### 1 Affichez les autorisations d'un fichier.

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

#### 2 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 3 Modifiez le propriétaire du fichier.

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

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

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

Les systèmes de fichiers montés sur NFS ont des restrictions supplémentaires en ce qui concerne la modification de la propriété et des groupes. Pour plus d'informations, reportez-vous à la section [Chapitre 6, “Accès aux systèmes de fichiers réseau \(référence\)”](#) du manuel *Administration d'Oracle Solaris : Services réseau*.

**Exemple 7–2** Modification par les utilisateurs de la propriété de leurs propres fichiers

**Considération de sécurité :** vous devez avoir une bonne raison de modifier la valeur de la variable `rstchown` à zéro. Le paramètre par défaut empêche les utilisateurs de répertorier leurs fichiers comme appartenant à d'autres utilisateurs afin de contourner les quotas d'espace.

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

```
set rstchown = 0
```

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

## ▼ Procédure de modification de la propriété de groupe d'un fichier

### Avant de commencer

Si vous n'êtes pas le propriétaire du fichier ou du répertoire, le profil de droits Object Access Management (gestion de l'accès aux objets) doit vous être affecté. Pour modifier un fichier qui est un [objet public](#), vous devez être connecté en tant que superutilisateur.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

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

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

Pour plus d'informations sur la définition des groupes, reportez-vous au [Chapitre 2, “Gestion des comptes utilisateur et des groupes \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

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

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

Reportez-vous également à l'[Exemple 7–2](#).

## ▼ Procédure de modification des autorisations de fichier en mode symbolique

Dans la procédure ci-dessous, un utilisateur modifie les autorisations d'un fichier qui lui appartient.

### 1 Modifiez les autorisations en mode symbolique.

```
% chmod who operator permissions filename
```

*who*                      Spécifie pour qui les autorisations doivent être modifiées.

*operator*                Indique l'opération à effectuer.

*permissions*            Spécifie les autorisations à modifier. Pour obtenir la liste des symboles valides, reportez-vous au [Tableau 7-5](#).

*filename*                Spécifie le fichier ou répertoire.

### 2 Vérifiez que les autorisations du fichier ont changé.

```
% ls -l filename
```

---

**Remarque** – Si vous n'êtes pas le propriétaire du fichier ou du répertoire, le profil de droits Object Access Management (gestion de l'accès aux objets) doit vous être affecté. Pour modifier un fichier qui est un [objet public](#), vous devez être connecté en tant que superutilisateur.

---

### Exemple 7-3 Modification des autorisations en mode symbolique

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

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

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

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

Dans l'exemple suivant, les autorisations de lecture, d'écriture et d'exécution pour le groupe sont affectés à un fichier local.

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



## ▼ Procédure de modification des autorisations de fichier en mode absolu

Dans la procédure ci-dessous, un utilisateur modifie les autorisations d'un fichier qui lui appartient.

### 1 Modifiez les autorisations en mode absolu.

```
% chmod nnn filename
```

*nnn* Spécifie les valeurs octales qui représentent les autorisations du propriétaire du fichier, du groupe de fichiers et autres, dans cet ordre. Pour obtenir la liste des valeurs octales, reportez-vous au [Tableau 7-4](#).

*filename* Spécifie le fichier ou répertoire.

---

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

---

### 2 Vérifiez que les autorisations du fichier ont changé.

```
% ls -l filename
```

---

**Remarque** – Si vous n'êtes pas le propriétaire du fichier ou du répertoire, le profil de droits Object Access Management (gestion de l'accès aux objets) doit vous être affecté. Pour modifier un fichier qui est un [objet public](#), vous devez être connecté en tant que superutilisateur.

---

### Exemple 7-4 Modification des autorisations en mode absolu

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

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

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

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

## ▼ Procédure de modification des autorisations de fichier spéciales en mode absolu

### Avant de commencer

Si vous n'êtes pas le propriétaire du fichier ou du répertoire, le profil de droits Object Access Management (gestion de l'accès aux objets) doit vous être affecté. Pour modifier un fichier qui est un **objet public**, vous devez être connecté en tant que superutilisateur.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

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

`% chmod nnnn filename`

*nnnn* Spécifie les valeurs octales qui modifient les autorisations du fichier ou du répertoire. La valeur octale le plus à gauche définit les autorisations spéciales du fichier. Pour obtenir la liste de valeurs octales valides pour les autorisations spéciales, reportez-vous au [Tableau 7-6](#).

*filename* Spécifie le fichier ou répertoire.

---

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

---

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

`% ls -l filename`

### Exemple 7-5 Définition des autorisations de fichiers spéciales en mode absolu

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

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

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

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

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

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

## Protection contre les programmes présentant des risques de sécurité (liste des tâches)

La liste des tâches suivante présente les procédures permettant trouver les exécutables à risque dans le système, et qui empêchent les programmes d'exploiter une pile exécutable.

| Tâche                                                             | Description                                                                                                                | Voir                                                                                                                |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Recherche de fichiers avec des autorisations spéciales.           | Localise les fichiers avec l'ensemble de bits <code>setuid</code> , mais non détenus par l'utilisateur <code>root</code> . | <a href="#">“Procédure de recherche de fichiers avec des autorisations de fichier spéciales” à la page 139</a>      |
| Empêchement du débordement de pile exécutable.                    | Empêche les programmes d'exploiter une pile exécutable.                                                                    | <a href="#">“Procédure de désactivation de l'utilisation de piles exécutables par les programmes” à la page 141</a> |
| Empêchement de la journalisation des messages de pile exécutable. | Désactive la journalisation des messages de pile exécutable.                                                               | <a href="#">Exemple 7-7</a>                                                                                         |

### ▼ Procédure de recherche de fichiers avec des autorisations de fichier spéciales

Cette procédure permet de repérer toute utilisation potentiellement interdite des autorisations `setuid` et `setgid` sur les programmes. Un fichier exécutable suspect accorde la propriété à un utilisateur plutôt qu'à `root` ou `bin`.

**Avant de commencer**

Vous devez être dans le rôle root.

**1 Recherchez les fichiers avec des autorisations setuid en utilisant la commande find.**

```
# find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/filename
```

*find directory* Vérifie tous les chemins montés en commençant par le *répertoire* spécifié, qui peut être root (/), sys, bin, ou mail.

-user root Affiche les fichiers appartenant uniquement à root.

-perm -4000 Affiche les fichiers uniquement avec les autorisations définies sur 4000.

-exec ls -ldb Affiche le résultat de la commande find au format ls -ldb.

/tmp/*filename* Il s'agit du fichier qui contient les résultats de la commande find.

**2 Affichez les résultats dans /tmp/*filename*.**

```
# more /tmp/filename
```

Pour plus d'informations d'ordre général sur les autorisations setuid, reportez-vous à la section [“Autorisation setuid” à la page 126](#).

**Exemple 7–6 Recherche de fichiers avec des autorisations setuid**

La sortie de l'exemple suivant indique qu'un utilisateur d'un groupe appelé rar a effectué une copie personnelle de /usr/bin/sh et a défini les autorisations setuid sur root. Par conséquent, le programme /usr/rar/bin/sh s'exécute avec les autorisations root.

Ce résultat a été enregistré pour référence ultérieure en déplaçant le répertoire /var/tmp/ckprm dans une archive.

```
# find / -user root -perm -4000 -exec ls -ldb {} \; > /var/tmp/ckprm
# cat /var/tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
# mv /var/tmp/ckprm /export/sysreports/ckprm
```

## ▼ Procédure de désactivation de l'utilisation de piles exécutables par les programmes

Pour obtenir une description des risques de sécurité liés aux piles exécutables 32 bits, reportez-vous à la section “[Protection contre les problèmes de sécurité causés par les fichiers exécutables](#)” à la page 131.

### Avant de commencer

Vous devez être dans le rôle root.

#### 1 Modifiez le fichier `/etc/system`, puis ajoutez la ligne suivante :

```
set noexec_user_stack=1
```

#### 2 Réinitialisez le système.

```
# reboot
```

### Exemple 7-7 Désactivation de la journalisation des messages de pile exécutable

Dans cet exemple, la journalisation des messages de pile exécutable est désactivée et le système est ensuite redémarré.

```
# cat /etc/system
set noexec_user_stack=1
set noexec_user_stack_log=0
# reboot
```

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

- [http://blogs.oracle.com/gbrunett/entry/solaris\\_non\\_executable\\_stack\\_overview](http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_overview)
- [http://blogs.oracle.com/gbrunett/entry/solaris\\_non\\_executable\\_stack\\_continued](http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_continued)
- [http://blogs.oracle.com/gbrunett/entry/solaris\\_non\\_executable\\_stack\\_concluded](http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_concluded)



## PARTIE III

# Rôles, profils de droits et privilèges

Cette section couvre le contrôle d'accès basé sur les rôles (RBAC) et la gestion des droits de processus. Les composants RBAC incluent les rôles, les profils de droits et les autorisations. La gestion des droits de processus est mise en oeuvre par le biais des privilèges. Les privilèges, aux côtés des composants RBAC, permettent d'offrir une alternative d'administration mieux sécurisée que l'administration d'un système par un superutilisateur.

- Chapitre 8, “Utilisation des rôles et des privilèges (présentation)”
- Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles (tâches)”
- Chapitre 10, “Attributs de sécurité dans Oracle Solaris (référence)”





## Utilisation des rôles et des privilèges (présentation)

---

La fonction de contrôle d'accès basé sur les rôles (RBAC) d'Oracle Solaris et la fonction de privilèges d'Oracle Solaris fournissent une alternative plus sécurisée au superutilisateur. Ce chapitre contient des informations de présentation sur le RBAC et les privilèges.

Vous trouverez ci-dessous une liste des informations générales contenues dans ce chapitre.

- “Contrôle d'accès basé sur les rôles (présentation)” à la page 145
- “Privilèges (présentation)” à la page 158

### Contrôle d'accès basé sur les rôles (présentation)

La fonction de sécurité RBAC permet de contrôler l'accès des utilisateurs aux tâches qui incombent normalement au rôle root. En appliquant les attributs de sécurité aux processus et aux utilisateurs, RBAC peut répartir les capacités superutilisateur entre plusieurs administrateurs. La gestion des droits des processus est mise en oeuvre par le biais des *privilèges*. La gestion des droits des utilisateurs est mise en oeuvre par le biais de RBAC.

- Pour une description de la gestion des droits des processus, reportez-vous à la section “Privilèges (présentation)” à la page 158.
- Pour plus d'informations sur les tâches RBAC, reportez-vous au [Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles \(tâches\)”](#).
- Pour des informations de référence, reportez-vous au [Chapitre 10, “Attributs de sécurité dans Oracle Solaris \(référence\)”](#).

### RBAC : la solution de substitution au modèle superutilisateur

Dans les systèmes UNIX classiques, l'utilisateur root, également appelé superutilisateur, dispose de tous les pouvoirs. Les programmes exécutés comme root ou setuid ont tous les

pouvoirs. L'utilisateur root peut lire les fichiers et y écrire des données, exécuter tous les programmes et envoyer des signaux d'interruption aux processus. Concrètement, un superutilisateur peut changer le pare-feu d'un site, modifier la piste d'audit, consulter des informations confidentielles et arrêter l'ensemble du réseau. Un programme setuid piraté peut avoir la mainmise sur le système.

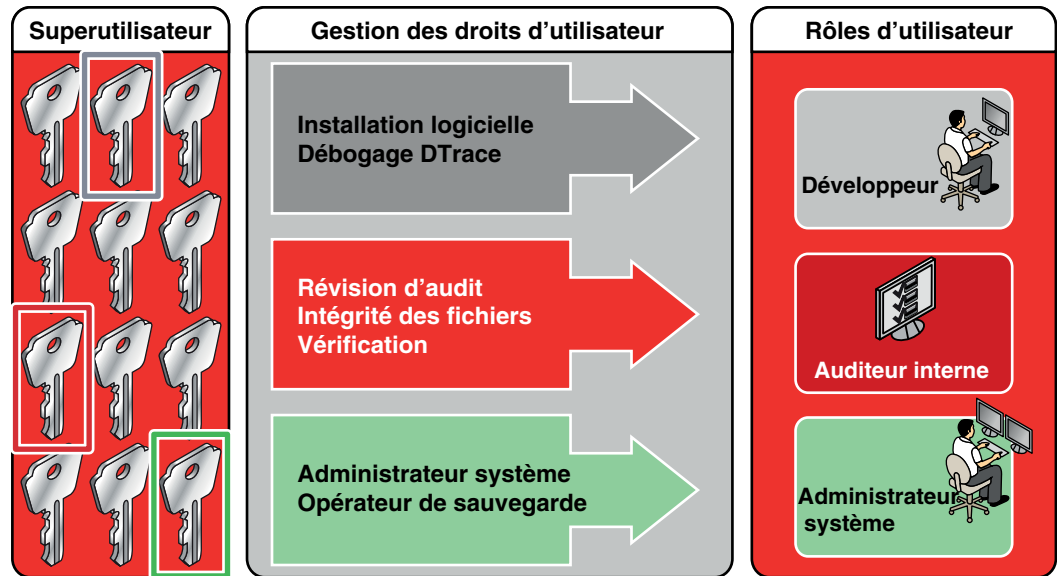
RBAC constitue la solution de substitution plus sécurisée au modèle du tout ou rien des superutilisateurs. Avec RBAC, vous pouvez appliquer des stratégies de sécurité à un niveau plus détaillé. RBAC met en oeuvre le principe de sécurité du *moindre privilège*. En d'autres termes, un utilisateur dispose des privilèges exacts en termes de quantité nécessaires à l'exécution d'un travail. Les utilisateurs standard ont suffisamment de privilèges pour utiliser leurs applications, vérifier l'état de leurs tâches, imprimer des fichiers, créer des fichiers, et ainsi de suite. Les capacités qui dépassent celles de l'utilisateur standard sont regroupées dans des profils de droits. Les utilisateurs devant effectuer des tâches pour lesquelles il est nécessaire de disposer de capacités de superutilisateur endossent un rôle incluant le profil de droits approprié.

RBAC regroupe les capacités de superutilisateur en *profils de droits*. Ces profils de droits sont affectés à des comptes utilisateur spéciaux, appelés *rôles*. Un utilisateur peut alors endosser un rôle pour effectuer une tâche qui requiert certaines capacités du superutilisateur. Des profils de droits prédéfinis sont fournis avec le logiciel Oracle Solaris. Vous créez les rôles et affectez les profils.

Les profils de droits peuvent fournir des capacités étendues. Par exemple, le profil de droits System Administrator (administrateur système) permet à un compte d'effectuer des tâches qui ne sont pas liées à la sécurité, telles que la gestion de l'imprimante et les tâches cron. Les profils de droits peuvent également être définis avec précision. Par exemple, le profil de droits Cron Management (gestion Cron) gère les tâches at et cron. Lorsque vous créez des rôles, des capacités restreintes et/ou étendues peuvent leur être attribuées.

La figure suivante montre comment RBAC permet de distribuer des droits aux parties de confiance.

FIGURE 8-1 Répartition des droits RBAC



Dans le modèle RBAC, le superutilisateur crée un ou plusieurs rôles. Les rôles sont basés sur des profils de droits. Le superutilisateur attribue ensuite les rôles aux utilisateurs autorisés à effectuer les tâches que ce rôle implique. Les utilisateurs se connectent avec leur nom d'utilisateur. Une fois connectés, les utilisateurs endossent les rôles qui autorisent l'utilisation des commandes d'administration et des outils d'interface graphique d'accès limité.

La flexibilité qui caractérise la configuration des rôles permet de définir une vaste gamme de stratégies de sécurité. Bien que Oracle Solaris soit livré avec quelques rôles, différents rôles peuvent être configurés facilement. Vous pouvez baser la plupart des rôles sur des profils de droits du même nom :

- **root** : rôle puissant, équivalent à l'utilisateur root. Cependant, le rôle root ne permet pas de se connecter. Un utilisateur standard doit se connecter, puis prendre le rôle root qui lui est affecté. Ce rôle est configuré par défaut.
- **Administrateur système** : rôle moins puissant impliquant des tâches d'administration, mais pas de sécurité. Ce rôle peut gérer des systèmes de fichiers, la messagerie électronique et l'installation de logiciels. Cependant, ce rôle ne permet pas de définir des mots de passe.
- **Opérateur** : rôle d'administrateur débutant, permettant d'effectuer des opérations telles que la gestion d'imprimantes et de sauvegardes.

**Remarque** – Le profil de droits Media Backup (sauvegarde des médias) donne accès au système de fichiers racine entier. Par conséquent, bien que les profils de droits Media Backup et Operator (opérateur) soient conçus pour les administrateurs débutants, les utilisateurs auxquels vous les affectez doivent être dignes de confiance.

Vous pouvez aussi être amené à configurer un ou plusieurs rôles de sécurité. Trois profils de droits et leurs profils supplémentaires prennent en charge la sécurité. Il s'agit des profils suivants : Information Security (sécurité des informations), User Security (sécurité des utilisateurs) et Zone Security (sécurité de la zone). Sécurité du réseau est un profil supplémentaire inclus dans le profil de droits Information Security (sécurité des informations).

Il n'est pas nécessaire de mettre en oeuvre ces rôles. Les rôles sont fonction des besoins de sécurité d'une organisation. Une stratégie consiste à configurer les rôles pour les administrateurs ayant un objectif précis dans des domaines tels que la sécurité, la mise en réseau ou l'administration d'un pare-feu. Une autre stratégie consiste à créer un seul rôle d'administrateur puissant conjointement avec un rôle d'utilisateur avancé. Le rôle d'utilisateur avancé est affecté aux utilisateurs autorisés à réparer des parties de leur propre système.

Le modèle superutilisateur et le modèle RBAC peuvent coexister. Le tableau suivant résume les différents degrés (du superutilisateur à l'utilisateur standard limité) possibles dans le modèle RBAC. Le tableau comprend les actions d'administration pouvant faire l'objet d'un suivi dans les deux modèles. Pour obtenir un récapitulatif de l'effet de chaque privilège sur un système, reportez-vous au [Tableau 8–2](#).

**TABEAU 8–1** Modèle de superutilisateur par rapport au modèle RBAC avec privilèges

| Capacités d'un utilisateur sur un système                                                                                          | Modèle superutilisateur                     | Modèle RBAC                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------|
| Peut devenir superutilisateur avec la capacité correspondante complète                                                             | Peut                                        | Peut                                                                              |
| Peut se connecter en tant qu'utilisateur disposant des capacités utilisateur complètes                                             | Peut                                        | Peut                                                                              |
| Peut devenir superutilisateur avec des capacités limitées                                                                          | Ne peut pas                                 | Peut                                                                              |
| Peut se connecter en tant qu'utilisateur et disposer des capacités de superutilisateur, sporadiquement                             | Peut, avec les programmes setuid uniquement | Peut, avec les programmes setuid et RBAC                                          |
| Peut se connecter en tant qu'utilisateur disposant des capacités d'administration, mais sans la capacité superutilisateur complète | Ne peut pas                                 | Peut, avec RBAC et avec les privilèges et les autorisations attribués directement |

**TABEAU 8-1** Modèle de superutilisateur par rapport au modèle RBAC avec privilèges (Suite)

| Capacités d'un utilisateur sur un système                                                           | Modèle superutilisateur             | Modèle RBAC                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Peut se connecter en tant qu'utilisateur disposant de moins de capacités qu'un utilisateur standard | Ne peut pas                         | Peut, avec RBAC et avec les privilèges supprimés                                                                                                          |
| Peut suivre les actions superutilisateur                                                            | Peut, par l'audit de la commande su | Peut, par l'audit des appels à <code>pfexec()</code><br><br>En outre, le nom de l'utilisateur qui a endossé le rôle root se trouve dans la piste d'audit. |

## Éléments et concepts de base RBAC

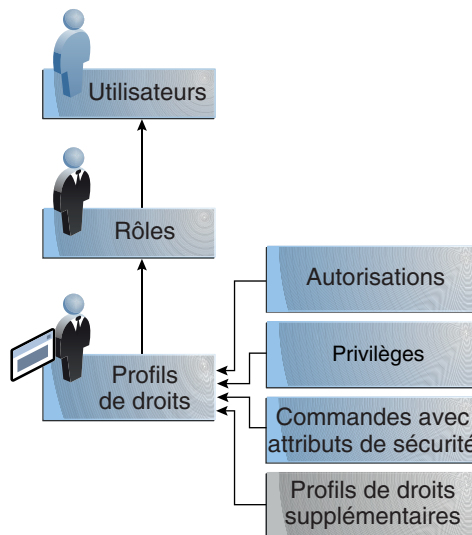
Le modèle RBAC dans Oracle Solaris introduit les éléments suivants :

- **Autorisation** : autorisation permettant à un utilisateur ou rôle de réaliser une classe d'actions nécessitant des droits supplémentaires. Par exemple, la stratégie de sécurité lors de l'installation attribue aux utilisateurs standard l'autorisation `solaris.device.cdrw`. Cette autorisation offre aux utilisateurs les droits de lecture et d'écriture au niveau du périphérique de CD-ROM. Pour obtenir la liste des autorisations, reportez-vous au fichier `/etc/security/auth_attr`.
- **Privilège** : droit discret accordé à une commande, un utilisateur, un rôle ou un système. Les privilèges permettent la réussite d'un processus. Par exemple, le privilège `proc_exec` permet à un processus d'appeler `execve()`. Les utilisateurs standard disposent des privilèges de base. Pour connaître vos privilèges de base, exécutez la commande `ppriv -vl basic`.
- **Attribut de sécurité** : attribut autorisant un processus à effectuer une opération. Dans un environnement UNIX standard, un attribut de sécurité permet à un processus d'effectuer une opération qui serait autrement interdite aux utilisateurs standard. Par exemple, les programmes `setuid` et `setgid` ont des attributs de sécurité. Dans le modèle RBAC, les autorisations et les privilèges sont des attributs de sécurité qui s'ajoutent aux programmes `setuid` et `setgid`. Ces attributs peuvent être affectés à un utilisateur. Par exemple, un utilisateur avec l'autorisation `solaris.device.allocate` peut allouer un périphérique pour une utilisation exclusive. Les privilèges peuvent être placés sur un processus. Par exemple, un processus avec le privilège `file_flag_set` peut définir des attributs de fichier immuable, `no-unlink` ou `append-only`.
- **Application privilégiée** : application ou commande pouvant ignorer les contrôles système en recherchant les *attributs de sécurité*. Dans un environnement UNIX standard et dans le modèle RBAC, les programmes qui utilisent `setuid` et `setgid` sont des applications privilégiées. Dans le modèle RBAC, les programmes ayant besoin de privilèges ou d'autorisations pour s'exécuter correctement sont également des applications privilégiées. Pour plus d'informations, reportez-vous à la section “Applications privilégiées et RBAC” à la page 153.

- **Profil de droits** : ensemble d'attributs de sécurité pouvant être affecté à un rôle ou un utilisateur. Un profil de droits peut inclure des autorisations, des privilèges affectés directement, des commandes avec des attributs de sécurité et d'autres profils de droits. Les profils au sein d'un autre profil sont appelés des profils de droits supplémentaires. Les profils de droits offrent un moyen pratique de regrouper les attributs de sécurité.
- **Rôle** : identité spéciale permettant d'exécuter des applications privilégiées. L'identité spéciale peut être endossée par les utilisateurs assignés uniquement. Dans un système exécuté par des rôles, y compris le rôle root, le superutilisateur n'est pas nécessaire. Les capacités de superutilisateur sont distribuées aux différents rôles. Par exemple, dans un système à deux rôles, les tâches de sécurité sont traitées par un rôle de sécurité. Le deuxième rôle traite des tâches d'administration système qui ne sont pas liées à la sécurité. Les rôles peuvent être définis de manière plus précise. Par exemple, un système peut inclure des rôles d'administration distincts pour la gestion de la structure cryptographique, des imprimantes, du temps système, des systèmes de fichiers et de l'audit.

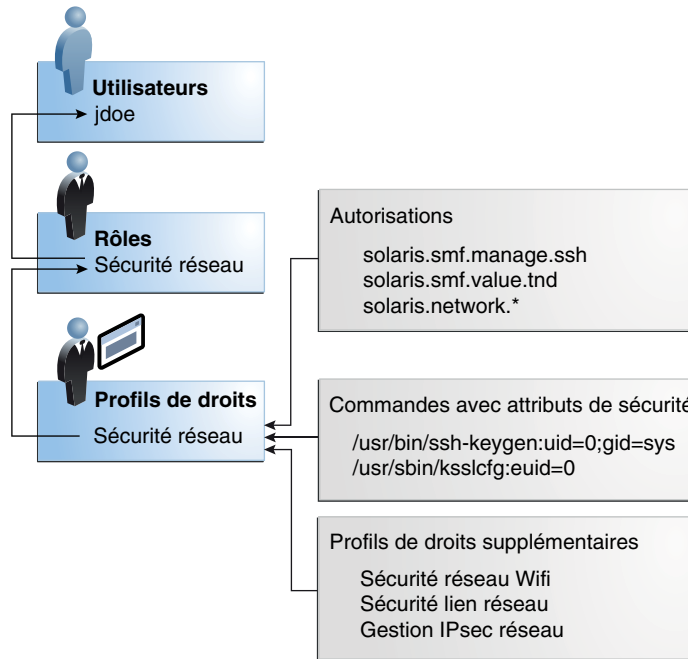
La figure suivante illustre la collaboration entre les éléments RBAC.

FIGURE 8-2 Relations entre les éléments RBAC



La figure suivante utilise le rôle Sécurité réseau et le profil de droits Network Security (sécurité réseau) pour illustrer les relations RBAC.

FIGURE 8-3 Exemple de relations entre éléments RBAC



Le rôle sécurité du réseau permet de gérer les liaisons réseau, IPsec et wifi. Ce rôle est assigné à l'utilisateur `jdoe`. Pour endosser le rôle, `jdoe` change de rôle, puis indique le mot de passe correspondant. L'administrateur peut personnaliser le rôle pour qu'il accepte le mot de passe utilisateur plutôt que le mot de passe du rôle.

Dans la Figure 8-3, le profil de droits Network Security (sécurité réseau) est affecté au rôle Sécurité réseau. Le profil de droits Network Security (sécurité réseau) contient des profils supplémentaires qui sont évalués dans l'ordre Network Wifi Security (sécurité wifi réseau), Network Link Security (sécurité liaison réseau) et Network IPsec Management (gestion IPsec réseau). Ces profils supplémentaires remplissent les tâches principales du rôle.

Le profil de droits Network Security (sécurité réseau) comporte trois autorisations attribuées directement, aucun privilège affecté directement et deux commandes avec des attributs de sécurité. Les profils de droits supplémentaires ont des autorisations attribuées directement et deux d'entre eux ont des commandes avec des attributs de sécurité. Dans le rôle Sécurité réseau, `jdoe` possède toutes les autorisations attribuées dans ces profils et peut exécuter toutes les commandes avec les attributs de sécurité dans ces profils. `jdoe` peut administrer la sécurité du réseau.

## Escalade des privilèges

Oracle Solaris offre aux administrateurs une grande flexibilité pour configurer la sécurité. Selon la configuration de l'installation, le logiciel n'autorise pas l'[escalade des privilèges](#). L'escalade des privilèges se produit lorsqu'un utilisateur ou un processus obtient plus de droits d'administration qu'il n'était prévu de lui accorder. Dans ce sens, privilège signifie n'importe quel attribut de sécurité.

Le logiciel Oracle Solaris comprend les attributs de sécurité affectés au rôle root uniquement. Si d'autres systèmes de sécurité sont en place, l'administrateur peut affecter les attributs conçus pour le rôle root à d'autres comptes, mais il doit procéder avec prudence.

Le profil de droits et le jeu d'autorisations suivants peuvent escalader les privilèges d'un compte non root.

- **Profil de droits Media Restore (restauration des médias)** : ce profil existe, mais il ne fait partie d'aucun autre profil de droits. Dans la mesure où Media Restore permet d'accéder à l'ensemble du système de fichiers racine, son utilisation est une escalade possible de privilège. Des fichiers délibérément modifiés ou des médias de substitution peuvent être restaurés. Par défaut, le rôle root inclut ce profil de droits.
- **solaris.\*.assign authorizations** : ces autorisations existent, mais ne sont affectées à aucun profil de droits ou compte. Un compte avec une autorisation `solaris.*.assign` peut affecter des attributs de sécurité à d'autres auxquels le compte lui-même n'est pas affecté. Par exemple, un rôle avec l'autorisation `solaris.profile.assign` peut affecter des profils de droits à d'autres comptes auxquels le rôle lui-même n'est pas affecté. Par défaut, seul le rôle root dispose des autorisations `solaris.*.assign`.

La meilleure pratique consiste à affecter les autorisations `solaris.*.delegate` et non les autorisations `solaris.*.assign`. Une autorisation `solaris.*.delegate` permet au délégué de n'attribuer à d'autres comptes que les attributs de sécurité qu'il possède. Par exemple, un rôle avec l'autorisation `solaris.profile.delegate` peut affecter à d'autres utilisateurs et rôles des profils de droits qui lui sont affectés.

Pour connaître les escalades ayant une incidence sur l'attribut de sécurité, reportez-vous à la section "[Prévention de l'escalade de privilèges](#)" à la page 227.

## Autorisations RBAC

Une *autorisation* est un droit discret pouvant être accordé à un rôle ou à un utilisateur. Les autorisations permettent d'appliquer des stratégies au niveau de l'application utilisateur.

Tandis que les autorisations peuvent être attribuées directement à un rôle ou à un utilisateur, il est recommandé d'inclure les autorisations dans un profil de droits. Le profil de droits est alors ajouté à un rôle et le rôle est assigné à un utilisateur. Pour en voir un exemple, reportez-vous à la [Figure 8-3](#).



Les autorisations comportant les mots `delegate` ou `assign` permettent à l'utilisateur ou au rôle d'affecter des attributs de sécurité à d'autres.

Pour empêcher l'escalade des privilèges, il est recommandé de ne pas affecter d'autorisation `assign` à un compte.

- Une autorisation `delegate` permet au délégant de n'attribuer à d'autres utilisateurs que les attributs de sécurité qu'il possède. Par exemple, un rôle avec l'autorisation `solaris.profile.delegate` peut affecter à d'autres utilisateurs des profils de droits qui lui sont affectés.
- Une autorisation `assign` permet à l'assignataire d'affecter à d'autres utilisateurs des attributs de sécurité que le compte ne possède pas. Par exemple, un rôle avec l'autorisation `solaris.profile.assign` peut affecter à d'autres utilisateurs n'importe quel profil de droits.

Les autorisations `solaris.*.assign` sont fournies, mais ne sont pas incluses dans tous les profils. Par défaut, seul le rôle `root` possède les autorisations `solaris.*.assign`.

Les applications compatibles avec RBAC peuvent vérifier les autorisations de l'utilisateur avant de lui autoriser l'accès au niveau de l'application ou des opérations spécifiques au sein de l'application. Cette vérification remplace la vérification conventionnelle dans les applications UNIX pour `UID=0`. Pour plus d'informations sur les autorisations, reportez-vous aux sections suivantes :

- [“Autorisations” à la page 218](#)
- [“Base de données `auth\_attr`” à la page 221](#)
- [“Commandes sélectionnées nécessitant des autorisations” à la page 224](#)

## Autorisations et privilèges

Les privilèges appliquent la stratégie de sécurité dans le noyau. La différence entre les autorisations et les privilèges réside dans le niveau auquel la stratégie de sécurité est appliquée. Sans le privilège adéquat, un processus peut se voir empêcher d'exécuter des opérations privilégiées par le noyau. Sans les autorisations adéquates, un utilisateur peut se voir empêcher d'utiliser une application privilégiée ou d'exécuter des opérations liées à la sécurité au sein d'une application privilégiée. Pour en savoir plus sur les privilèges, reportez-vous à la section [“Privilèges \(présentation\)” à la page 158](#).

## Applications privilégiées et RBAC

Les applications et les commandes pouvant ignorer les contrôles système sont considérées comme des applications privilégiées. Les attributs de sécurité tels que `UID=0`, les privilèges et les autorisations rendent une application privilégiée.

## Applications vérifiant les UID et GID

Les applications privilégiées vérifiant l'ID utilisateur root ( UID=0) ou autres UID (ID utilisateur) ou GID (ID de groupe) existent depuis longtemps dans l'environnement UNIX. Le mécanisme de profil de droits vous permet d'isoler les commandes nécessitant un ID spécifique. Au lieu de modifier l'ID sur une commande accessible par tous, vous pouvez placer la commande avec les attributs de sécurité affectés dans un profil de droits. Un utilisateur ou un rôle avec ce profil de droits peut alors exécuter le programme sans avoir à devenir superutilisateur.

Les ID peuvent être spécifiés en tant qu'ID réels ou effectifs. On préférera une affectation d'ID effectifs à une affectation d'ID réels. Les ID effectifs correspondent à la fonction `setuid` dans les bits d'autorisation de fichier. Les ID effectifs permettent également d'identifier l'UID pour l'audit. Cependant, étant donné que certains programmes et scripts shell nécessitent un UID réel de root, il est également possible de définir des ID utilisateur réels. Par exemple, la commande `reboot` requiert un ID utilisateur réel plutôt qu'un ID utilisateur effectif. Si un ID effectif n'est pas suffisant pour exécuter une commande, vous devez affecter l'ID réel à la commande.

## Applications vérifiant les privilèges

Les applications privilégiées peuvent vérifier l'utilisation des privilèges. Le mécanisme de profil de droits RBAC permet de spécifier les privilèges pour des commandes spécifiques qui requièrent des attributs de sécurité. Ensuite, vous pouvez isoler la commande avec des attributs de sécurité affectés dans un profil de droits. Un utilisateur ou un rôle doté de ce profil de droits peut ensuite exécuter la commande avec les privilèges nécessaires à la réussite de la commande.

Voici la liste des commandes vérifiant les privilèges :

- Commandes Kerberos, telles que `kadmin`, `kprop` et `kdb5_util`
- Commandes réseau, telles que `ipadm`, `routeadm` et `snoop`
- Commandes de fichier et de système de fichiers, telles que `chmod`, `chgrp` et `monter`
- Commandes qui contrôlent les processus, telles que `kill`, `pcréd` et `rcapadm`

Pour ajouter des commandes privilégiées à un profil de droits, reportez-vous à la section [“Procédure de création ou de modification d'un profil de droits” à la page 186](#) et à la page de manuel [profiles\(1\)](#). Pour déterminer quelles commandes vérifient les privilèges dans un profil particulier, reportez-vous à la section [“Procédure d'affichage de tous les attributs de sécurité définis” à la page 170](#).

## Applications vérifiant les autorisations

Oracle Solaris fournit également des commandes qui vérifient les autorisations. Par définition, les utilisateurs root possèdent toutes les autorisations. Par conséquent, l'utilisateur root peut exécuter n'importe quelle application. Voici la liste des applications qui vérifient les autorisations :

- Commandes d'administration d'audit, telles que `auditconfig` et `auditreduce`
- Commandes d'administration d'imprimante, telles que `lpadmin` et `lpfilter`
- Commandes de tâche par lot, telles que `at`, `atq`, `batch` et `crontab`
- Commandes orientées périphérique, telles que `allocate`, `deallocate`, `list_devices` et `cdwr`.

Pour tester un script ou un programme dans le cadre des autorisations, reportez-vous à l'[Exemple 9–16](#). Pour écrire un programme nécessitant des autorisations, reportez-vous à la rubrique “[About Authorizations](#)” du manuel *Developer's Guide to Oracle Solaris 11 Security*.

## Profils de droits RBAC

Un *profil de droits* est un ensemble d'attributs de sécurité pouvant être affecté à un rôle ou un utilisateur pour effectuer des tâches requérant des droits d'administration. Un profil de droits peut se composer d'autorisations, de privilèges, de commandes auxquelles des attributs de sécurité ont été affectés et d'autres profils de droits. Les privilèges qui sont affectés dans un profil de droits sont en vigueur pour toutes les commandes. Les profils de droits contiennent également des entrées afin de réduire ou d'étendre le premier ensemble hérité, et de réduire l'ensemble limite de privilèges.

Pour plus d'informations sur les profils de droits, reportez-vous aux sections suivantes :

- “[Profils de droits](#)” à la page 215
- “[Base de données prof\\_attr](#)” à la page 222
- “[Base de données exec\\_attr](#)” à la page 222

## Rôles RBAC

Un *rôle* est un type spécial de compte utilisateur à partir duquel vous pouvez exécuter des applications privilégiées. Les rôles sont créés de la même manière que les comptes utilisateur. Les rôles ont un répertoire personnel, une affectation de groupe, un mot de passe, et ainsi de suite. Les profils de droits et les autorisations attribuent les capacités administratives des rôles. Les rôles ne peuvent pas hériter des capacités d'autres rôles ou d'autres utilisateurs. Les rôles discrets répartissent les capacités de superutilisateur et permettent ainsi des pratiques administratives plus sécurisées.

Lorsqu'un utilisateur endosse un rôle, les attributs du rôle remplacent tous les attributs de l'utilisateur. Les informations sur les rôles sont stockées dans les bases de données `passwd`, `shadow` et `user_attr`. Les actions des rôles peuvent être auditées. Pour obtenir des informations détaillées sur la configuration des rôles, reportez-vous aux sections suivantes :

- [“Procédure de planification de votre implémentation RBAC” à la page 178](#)
- [“Procédure de création d'un rôle” à la page 181](#)
- [“Procédure de modification des attributs de sécurité d'un rôle” à la page 194](#)

Un rôle peut être affecté à plusieurs utilisateurs. Tous les utilisateurs qui peuvent endosser le même rôle possèdent le même répertoire personnel de rôle, fonctionnent dans le même environnement et ont accès aux mêmes fichiers. Les utilisateurs peuvent endosser les rôles à partir de la ligne de commande à l'aide de la commande `su` et en fournissant le mot de passe et le nom du rôle. Par défaut, les utilisateurs peuvent s'authentifier pour un rôle en fournissant le mot de passe du rôle. L'administrateur peut configurer le système pour permettre à un utilisateur de s'authentifier en fournissant le mot de passe de l'utilisateur. Pour la procédure, reportez-vous à la section [“Procédure d'octroi à un utilisateur de l'autorisation d'utiliser son propre mot de passe pour endosser un rôle” à la page 201](#).

Un rôle ne peut pas se connecter directement. Un utilisateur se connecte, puis endosse un rôle. Après avoir endossé un rôle, l'utilisateur ne peut pas en endosser un autre tant qu'il n'a pas quitté son rôle actuel. Après avoir quitté son rôle, l'utilisateur peut alors en endosser un autre.

Le fait que `root` soit un rôle dans Oracle Solaris empêche toute connexion `root` anonyme. Si la commande `shell` de profil, `pfexec`, est en cours d'audit, la piste d'audit contient l'UID réel de l'utilisateur de connexion, les rôles que l'utilisateur a endossés et les actions que le rôle a effectuées. Pour auditer le système ou un utilisateur particulier pour les opérations de rôle, reportez-vous à la section [“Procédure d'audit des rôles” à la page 184](#).

Les profils de droits livrés avec le logiciel sont conçus pour correspondre aux rôles. Par exemple, le profil de droits `System Administrator` (`administrateur système`) peut permettre de créer le rôle `Administrateur système`. Pour configurer un rôle, reportez-vous à la section [“Procédure de création d'un rôle” à la page 181](#).

## Shells de profil et RBAC

Les utilisateurs et les rôles peuvent exécuter des applications privilégiées à partir d'un [shell de profil](#). Un *shell de profil* est un shell spécial qui reconnaît les attributs de sécurité inclus dans un profil de droits. Les administrateurs peuvent affecter un shell de profil à un utilisateur spécifique en tant que shell de connexion, ou le shell de profil est démarré lorsqu'un utilisateur exécute la commande `su` pour endosser un rôle. Dans Oracle Solaris, chaque shell dispose d'un shell de profil homologue. Par exemple, les shells de profil correspondant aux `bourne shell` (`sh`), `bash shell` (`csh`) et `korn shell` (`ksh`), sont respectivement les shells `pfsh`, `pfbash` et `pfksh`. Pour obtenir une liste des shells de profil, reportez-vous à la page de manuel [pfexec\(1\)](#).

Les utilisateurs auxquels un profil de droits a été assigné directement et dont le shell de connexion n'est pas un shell de profil doivent appeler un shell de profil pour exécuter les commandes avec les attributs de sécurité. La section [“Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité” à la page 157](#) contient les points en prendre en considération en matière d'utilisation et de sécurité.

Toutes les commandes exécutées dans le cadre d'un shell de profil peuvent faire l'objet d'un audit. Pour plus d'informations, reportez-vous à la section [“Procédure d'audit des rôles” à la page 184](#).

## Champ d'application du service de noms et RBAC

Le champ d'application du service de noms permet de mieux comprendre RBAC. Le champ d'application d'un rôle peut être limité à un hôte unique. Il peut également inclure tous les hôtes pris en charge par un service de noms, tel que LDAP. Le champ d'application du service de noms pour un système est indiqué dans le service de commutation de nom, `svc:/system/name-service/switch`. La recherche s'arrête à la première correspondance. Si, par exemple, un profil de droits existe dans deux champs d'application du service de noms, seules les entrées dans le premier champ d'application du service de noms sont utilisées. Si `files` est la première correspondance, le champ d'application de ce rôle est limité à l'hôte local.

## Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité

En général, un utilisateur obtient ses capacités d'administration par le biais d'un rôle. Les autorisations, les privilèges et les commandes privilégiées sont regroupés dans un profil de droits. Le profil de droits est inclus dans un rôle et le rôle est assigné à un utilisateur.

L'affectation directe des profils de droits et des attributs de sécurité est également possible :

- Les profils de droits, privilèges et autorisations peuvent être attribués directement aux utilisateurs.
- Les privilèges et les autorisations peuvent être attribués directement aux utilisateurs et aux rôles.

Toutefois, l'affectation directe de privilèges ne constitue pas une pratique sécurisée. Les utilisateurs et les rôles auxquels un privilège est affecté directement peuvent remplacer la stratégie de sécurité partout où ce privilège est requis par le noyau. Une pratique plus sécurisée consiste à attribuer le privilège en tant qu'attribut de sécurité d'une commande dans un profil de droits. Ce privilège n'est alors disponible que pour cette commande par un utilisateur doté de ce profil de droits.

Etant donné que les autorisations agissent au niveau de l'utilisateur, l'affectation directe d'autorisations constitue un moindre risque que l'affectation directe de privilèges. Cependant, les autorisations peuvent permettre à un utilisateur d'effectuer des tâches hautement sécurisées, comme l'affectation d'indicateurs d'audit par exemple.

## Considérations relatives à l'utilisation lors de l'affectation directe d'attributs de sécurité

L'affectation directe de profils de droits et les attributs de sécurité peuvent avoir une incidence sur l'utilisation :

- Les autorisations et privilèges affectés directement et les commandes et autorisations dans un profil de droits affecté directement, doivent être interprétés par un shell de profil pour être effectifs. Par défaut, un shell de profil n'est pas affecté aux utilisateurs.

L'utilisateur ne doit pas oublier d'ouvrir un shell de profil, puis d'exécuter les commandes dans ce shell.

- L'affectation individuelle d'autorisations n'est pas évolutive. Les autorisations affectées directement ne suffisent peut-être pas pour réaliser une tâche. Une tâche peut requérir des commandes privilégiées.

Les profils de droits sont conçus pour lier des autorisations et des commandes privilégiées. Ceux-ci sont également évolutifs.

## Privilèges (présentation)

La gestion des droits de processus permet de restreindre les processus au niveau de la commande, du rôle, du système ou de l'utilisateur. Oracle Solaris met en oeuvre la gestion des droits de processus via des *privilèges*. En termes de sécurité, les privilèges diminuent le risque qu'un utilisateur ou un processus puisse disposer des capacités de superutilisateur complètes sur un système. Les privilèges et les contrôles RBAC offrent une solution de substitution intéressante au modèle superutilisateur traditionnel.

- Pour plus d'informations sur le contrôle RBAC, reportez-vous à la section [“Contrôle d'accès basé sur les rôles \(présentation\)” à la page 145](#).
- Pour plus d'informations sur la gestion des privilèges, reportez-vous à la section [“Utilisation des privilèges \(tâches\)” à la page 204](#).
- Pour plus d'informations sur les privilèges, reportez-vous à la section [“Privilèges” à la page 225](#).

## Protection des processus noyau par les privilèges

Un privilège est un droit discret dont a besoin un processus pour réaliser une opération. Le droit est appliqué dans le noyau. Un programme qui s'exécute dans les limites du *jeu de base* de privilèges fonctionne dans les limites de la stratégie de sécurité système. Les programmes `setuid` sont des exemples de programmes qui fonctionnent en dehors des limites de la stratégie de sécurité système. Les privilèges permettent aux programmes d'éliminer la nécessité d'appeler `setuid`.

Les privilèges énumèrent discrètement les types d'opérations possibles sur un système. Les programmes peuvent être exécutés avec les privilèges exacts nécessaires à leur réussite. Par exemple, un programme qui manipule des fichiers peut nécessiter les privilèges `file_dac_write` et `file_flag_set`. Cette capacité élimine la nécessité d'exécuter le programme en tant que `root`.

Historiquement, les systèmes n'ont pas suivi le modèle de privilège. Ils ont plutôt utilisé le modèle de superutilisateur. Dans le modèle de superutilisateur, les processus s'exécutaient en tant que `root` ou en tant qu'utilisateur. L'action des processus utilisateur était limitée au niveau des répertoires et fichiers de l'utilisateur. Les processus `root` pouvaient créer des répertoires et fichiers en tout point du système. Un processus qui devait créer un répertoire en dehors du répertoire de l'utilisateur devait s'exécuter avec `UID=0`, c'est-à-dire, en tant que `root`. La stratégie de sécurité s'appuyait sur le contrôle d'accès discrétionnaire (DAC, Discretionary Access Control) pour protéger les fichiers système. Les noeuds de périphérique étaient protégés par DAC. Par exemple, les périphériques appartenant au groupe `sys` ne pouvaient être ouverts que par les membres du groupe `sys`.

Cependant, les programmes `setuid`, les autorisations de fichier et les comptes d'administration sont vulnérables à une utilisation abusive. Les actions qu'un processus `setuid` est autorisé à réaliser sont plus nombreuses qu'il n'est nécessaire au processus pour terminer son opération. Un programme `setuid` peut être compromis par un intrus qui s'exécute ensuite en tant qu'utilisateur `root` disposant de tous les pouvoirs. De même, tout utilisateur ayant accès au mot de passe `root` peut compromettre l'ensemble du système.

En revanche, un système appliquant la stratégie avec des privilèges permet l'instauration d'une graduation entre les capacités utilisateur et les capacités `root`. Un utilisateur peut se voir accorder des privilèges nécessaires à la réalisation d'activités dépassant les capacités des utilisateurs standard et `root` peut voir le nombre de ses privilèges actuels réduit. Avec RBAC, une commande qui s'exécute avec les privilèges peut être isolée dans un profil de droits et assignée à un utilisateur ou à un rôle. Le [Tableau 8-1](#) résume la graduation entre les capacités utilisateur et les capacités `root` que le modèle RBAC plus privilèges fournit.

Le modèle de privilèges offre une plus grande sécurité que le modèle superutilisateur. Les privilèges supprimés d'un processus ne peuvent pas être exploités. Les privilèges de processus empêchent un programme ou compte d'administration d'accéder à toutes les capacités. Les privilèges de processus peuvent fournir une protection supplémentaire pour les fichiers sensibles, où les protections DAC seules peuvent être exploitées pour obtenir l'accès.

Les privilèges peuvent alors restreindre les programmes et processus aux capacités qu'ils nécessitent. Cette capacité s'appelle le *principe du moindre privilège*. Sur un système appliquant ce privilège, un intrus qui capture un processus ne peut accéder qu'aux privilèges dont dispose ce processus. Le reste du système ne peut pas être compromis.

## Descriptions des privilèges

Les privilèges sont logiquement regroupés sur la base de la zone du privilège.

- **Privilège FILE** : les privilèges qui commencent par la chaîne `file` fonctionnent sur les objets du système de fichiers. Par exemple, le privilège `file_dac_write` remplace le contrôle d'accès discrétionnaire lors de l'écriture dans les fichiers.
- **Privilèges IPC** : les privilèges qui commencent par la chaîne `ipc` remplacent les contrôles d'accès aux objets IPC. Par exemple, le privilège `ipc_dac_read` permet à un processus de lire une mémoire partagée distante et protégée par le contrôle DAC.
- **Privilège NET** : les privilèges qui commencent par la chaîne `net` offrent l'accès à des fonctionnalités réseau spécifiques. Par exemple, le privilège `net_rawaccess` permet à un périphérique de se connecter au réseau.
- **Privilège PROC** : les privilèges qui commencent par la chaîne `proc` permettent aux processus de modifier les propriétés restreintes du processus lui-même. Les privilèges PROC comprennent des privilèges ayant un effet très limité. Par exemple, le privilège `proc_clock_highres` permet à un processus d'utiliser des horloges haute résolution.
- **Privilège SYS** : les privilèges qui commencent par la chaîne `sys` offrent aux processus l'accès illimité à diverses propriétés système. Par exemple, le privilège `sys_linkdir` permet à un processus de créer et de rompre des liens physiques vers des répertoires.

D'autres groupes logiques comprennent CONTRACT, CPC, DTRACE, GRAPHICS, VIRT, WIN et XVM.

Certains privilèges ont un effet limité sur le système, d'autres un effet important. La définition du privilège `proc_taskid` indique son effet limité :

```
proc_taskid
    Allows a process to assign a new task ID to the calling process.
```

La définition du privilège `file_setid` indique son large effet :

```
net_rawaccess
    Allow a process to have direct access to the network layer.
```

La page de manuel [privileges\(5\)](#) contient la description de chaque privilège. La commande `ppriv -lv` imprime une description de chaque privilège à la sortie standard.



## Différences administratives sur un système disposant de privilèges

Un système disposant de privilèges présente plusieurs différences visibles avec un système qui n'en possède pas. Le tableau suivant énumère certaines différences.

**TABLEAU 8-2** Différences visibles entre un système avec des privilèges et un système sans privilèges

| Fonction                       | Aucun privilège                                                                                                                                                | Privilèges                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Démons                         | Les démons s'exécutent en tant que root.                                                                                                                       | Les démons s'exécutent en tant que démon utilisateur.<br><br>Par exemple, les démons suivants ont reçu les privilèges appropriés et s'exécutent en tant que démons : <code>lockd</code> , <code>nfsd</code> et <code>rpcbind</code> .                                                                                                                                                                   |
| Propriété du fichier journal   | Les fichiers journaux appartiennent à root.                                                                                                                    | Les fichiers journaux sont désormais la propriété du démon, qui a créé le fichier journal. L'utilisateur root ne détient pas la propriété du fichier.                                                                                                                                                                                                                                                   |
| Messages d'erreur              | Les messages d'erreur se rapportent au superutilisateur.<br><br>Par exemple, <code>chroot: not superuser</code> .                                              | Les messages d'erreur reflètent l'utilisation des privilèges.<br><br>Par exemple, le message d'erreur équivalent pour l'échec <code>chroot</code> est <code>chroot: exec failed</code> .                                                                                                                                                                                                                |
| Programmes <code>setuid</code> | Les programmes utilisent <code>setuid</code> pour terminer les tâches que les utilisateurs standard ne sont pas autorisés à effectuer.                         | De nombreux programmes <code>setuid</code> ont été modifiés afin d'être exécutés avec des privilèges.<br><br>Par exemple, les commandes suivantes utilisent des privilèges : <code>audit</code> , <code>ikeadm</code> , <code>ipadm</code> , <code>ipsecconf</code> , <code>ping</code> , <code>traceroute</code> et <code>newtask</code> .                                                             |
| Autorisations de fichier       | Les autorisations d'accès aux périphériques sont contrôlées par DAC. Par exemple, les membres du groupe <code>sys</code> peuvent ouvrir <code>/dev/ip</code> . | Les autorisations de fichier (DAC) ne prédisent pas qui peut ouvrir un périphérique. Les périphériques sont protégés par DAC <i>et</i> par la stratégie de périphériques.<br><br>Par exemple, le fichier <code>/dev/ip</code> a 666 autorisations, mais le périphérique ne peut être ouvert que par un processus disposant des privilèges appropriés. Les sockets bruts sont toujours protégés par CAD. |
| Événements d'audit             | L'audit de l'utilisation de la commande <code>su</code> couvre de nombreuses fonctions d'administration.                                                       | L'audit de l'utilisation des privilèges couvre la plupart des fonctions d'administration. Les classes d'audit <code>pm</code> , <code>ps</code> , <code>ex</code> , <code>ua</code> et <code>as</code> incluent des événements d'audit qui surveillent la stratégie de périphériques et l'utilisation des privilèges.                                                                                   |
| Processus                      | Les processus sont protégés par leur propriétaire.                                                                                                             | Les processus sont protégés par des privilèges. Les privilèges de processus et les indicateurs de processus sont visibles sous la forme d'une nouvelle entrée dans le répertoire <code>/proc/&lt;pid&gt;</code> , <code>priv</code> .                                                                                                                                                                   |

TABLEAU 8-2 Différences visibles entre un système avec des privilèges et un système sans privilèges (Suite)

| Fonction | Aucun privilège                                              | Privilèges                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Débogage | Aucune référence aux privilèges dans les fichiers core dump. | <p>La section de note ELF des fichiers core dump comprend des informations sur les privilèges et les indicateurs de processus dans les notes NT_PRPRIV et NT_PRPRIVINFO.</p> <p>La commande ppriv et d'autres commandes indiquent le nombre correct de jeux de taille adéquate. Les commandes font correspondre correctement les bits dans les jeux de bits avec les noms de privilège.</p> |

## Privilèges et ressources du système

Dans la version Oracle Solaris, les contrôles de ressources `project.max-locked-memory` et `zone.max-locked-memory` peuvent être utilisés pour limiter la consommation mémoire des processus auxquels le privilège `PRIV_PROC_LOCK_MEMORY` est affecté. Ce privilège permet à un processus de verrouiller des pages dans la mémoire physique.

Si vous affectez le privilège `PRIV_PROC_LOCK_MEMORY` à un profil de droits, vous pouvez attribuer aux processus qui disposent de ce privilège la capacité de verrouiller la totalité de la mémoire. A titre de protection, définissez un contrôle de ressources pour empêcher l'utilisateur de ce privilège de verrouiller toute la mémoire. Pour les processus privilégiés qui s'exécutent dans une zone non globale, définissez le contrôle de ressources `zone.max-locked-memory`. Pour les processus privilégiés qui s'exécutent sur un système, créez un projet et définissez le contrôle de ressources `project.max-locked-memory`. Pour plus d'informations sur ces contrôles de ressources, reportez-vous au [Chapitre 6, "Contrôles des ressources \(présentation\)" du manuel Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources](#) et au [Chapitre 16, "Configuration des zones non globales \(présentation\)" du manuel Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources](#).

## Mise en oeuvre des privilèges

Chaque processus dispose de quatre jeux de privilèges qui déterminent s'il peut utiliser un privilège particulier. Le noyau calcule automatiquement le *jeu effectif* de privilèges. Vous pouvez modifier le *jeu héritable* de privilèges. Un programme codé pour utiliser des privilèges peut réduire le *jeu autorisé* du programme. Vous pouvez réduire le *jeu limite* de privilèges.

- **Jeu de privilèges effectif ou E (Effective) :** jeu de privilèges actuellement en vigueur. Un processus peut ajouter des privilèges du jeu autorisé dans le jeu effectif. Un processus peut également supprimer des privilèges de E.
- **Jeu de privilèges autorisés ou P (Permitted) :** jeu de privilèges disponible pour l'utilisation. Les privilèges peuvent être disponibles à un programme après héritage ou par affectation. Un profil d'exécution est un moyen d'affecter des privilèges à un programme. La commande

setuid affecte tous les privilèges dont dispose root sur un programme. Les privilèges peuvent être supprimés du jeu autorisé, mais ils ne peuvent pas y être ajoutés. Les privilèges supprimés de P sont automatiquement supprimés de E.

Un programme *conscient des privilèges* supprime les privilèges qu'un programme n'utilise jamais de son jeu autorisé. De cette manière, les privilèges superflus ne peuvent pas être exploités par le programme ou un processus malveillant. Pour plus d'informations sur les programmes prenant en charge les privilèges, reportez-vous au [Chapitre 2, “Developing Privileged Applications”](#) du manuel *Developer's Guide to Oracle Solaris 11 Security*.

- **Jeu de privilèges héritable ou I (Inheritable)** : jeu de privilèges qu'un processus peut hériter d'un appel à exec. Après l'appel à exec, les jeux autorisé et effectif sont égaux, à l'exception du cas particulier d'un programme setuid.

Pour un programme setuid, après l'appel à exec, le jeu héritable est d'abord restreint par le jeu limite. Ensuite, les privilèges hérités (I), moins les privilèges qui se trouvaient dans le jeu limite (L), sont affectés à P et E pour ce processus.

- **Jeu de privilèges de limite ou L (Limit)** : limite extérieure des privilèges disponibles à un processus et à ses fils. Par défaut, le jeu limite contient tous les privilèges. Les processus peuvent réduire le jeu limite mais ne peuvent jamais l'étendre. L permet de limiter I. Par conséquent, L limite P et E au moment de exec.

Si un utilisateur s'est vu affecter un profil qui inclut un programme qui a reçu des privilèges, l'utilisateur peut généralement exécuter ce programme. Sur un système non modifié, les privilèges affectés du programme se trouvent dans le jeu limite de l'utilisateur. Les privilèges affectés au programme deviennent partie intégrante du jeu autorisé de l'utilisateur. C'est à partir d'un shell de profil que l'utilisateur doit exécuter le programme auquel des privilèges ont été affectés.

Le noyau reconnaît un *jeu de privilèges de base*. Sur un système non modifié, le jeu héritable initial de chaque utilisateur correspond au jeu de base défini au moment de la connexion. Si vous ne pouvez pas modifier le jeu de base, vous pouvez modifier les privilèges dont un utilisateur hérite du jeu de base.

Sur un système non modifié, les jeux de privilèges de l'utilisateur à la connexion ressemble à ce qui suit :

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

Par conséquent, au moment de la connexion, tous les utilisateurs ont le jeu de base dans leur jeu hérité, leur jeu autorisé et leur jeu effectif. Le jeu limite d'un utilisateur est l'équivalent du jeu limite par défaut pour la zone globale ou non globale. Pour ajouter des privilèges au jeu effectif de l'utilisateur, vous devez affecter un profil de droits à ce dernier. Le profil de droits doit inclure les commandes pour lesquelles vous avez ajouté les privilèges. Vous pouvez également affecter des privilèges directement à l'utilisateur ou au rôle, bien que de telles affectations de privilèges

puissent comporter un risque. Pour une description des risques, reportez-vous à la section [“Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité”](#) à la page 157.

## Comment les processus obtiennent des privilèges

Les processus peuvent hériter de privilèges. Des privilèges peuvent aussi leur être affectés. Un processus hérite des privilèges de son processus parent. Au moment de la connexion, le jeu de privilèges héréditaire initial détermine les privilèges disponibles pour les processus de l'utilisateur. Tous les processus fils de la connexion initiale de l'utilisateur héritent de ce jeu.

Vous pouvez également affecter directement des privilèges à des programmes, des utilisateurs et des rôles. Lorsqu'un programme requiert des privilèges, vous affectez les privilèges à l'exécutable du programme dans un profil de droits. Les utilisateurs et les rôles autorisés à exécuter le programme se voient affecter le profil qui comprend le programme. Au moment de la connexion ou lorsqu'un shell de profil est saisi, le programme s'exécute avec le privilège lorsque l'exécutable du programme est entré dans le shell de profil. Par exemple, un rôle qui inclut le profil Gestion de l'accès aux objets peut exécuter la commande `chmod` avec le privilège `file_chown`.

Lorsqu'un rôle ou un utilisateur exécute un programme auquel un privilège supplémentaire a été affecté directement, celui-ci est ajouté au jeu héréditaire du rôle ou de l'utilisateur. Les processus fils du programme auquel des privilèges ont été affectés héritent des privilèges de leur parent. Si le processus fils nécessite plus de privilèges que le processus parent, ces privilèges doivent lui être affectés directement.

**conscient des privilèges** Les programmes codés pour utiliser des privilèges sont appelés des programmes conscients des privilèges. Un programme *conscient des privilèges* active l'utilisation des privilèges et désactive l'utilisation des privilèges lors de l'exécution du programme. Pour réussir dans un environnement de production, le programme doit se voir affecter les privilèges qu'il active et désactive.

Pour des exemples de code prenant en charge les privilèges, reportez-vous au [Chapitre 2, “Developing Privileged Applications”](#) du manuel *Developer's Guide to Oracle Solaris 11 Security*. Pour affecter des privilèges à un programme qui requiert des privilèges, voir l'[Exemple 9–14](#).

## Affectation de privilèges

En votre qualité d'administrateur sécurité, vous êtes responsable de l'affectation des privilèges. La meilleure pratique consiste à affecter les privilèges à une commande dans un profil de droits. Le profil de droits est ensuite affecté à un rôle ou à un utilisateur.

Des privilèges peuvent également être directement affectés à un utilisateur, un rôle ou un profil de droits. Si vous estimez qu'un sous-ensemble d'utilisateurs est suffisamment responsable pour

utiliser un privilège au cours de sessions, vous pouvez lui affecter directement ce privilège. Les bons candidats à l'affectation directe sont les privilèges ayant un effet limité, tels que `proc_clock_highres`. Les mauvais candidats à l'affectation directe sont les privilèges ayant des effets importants, tels que `file_dac_write`.

Les privilèges peuvent également être refusés à un utilisateur ou à un système. Procédez avec prudence lorsque vous supprimez des privilèges du jeu héritable initial ou du jeu limite d'un utilisateur ou d'un système.

## Extension des privilèges d'un utilisateur ou d'un rôle

Les utilisateurs et les rôles disposent d'un jeu héritable de privilèges. Le jeu limite ne peut pas être étendu, car il contient initialement tous les privilèges. Le jeu héritable initial peut être étendu pour les utilisateurs, les rôles et les systèmes. Un privilège qui ne figure pas dans le jeu héritable peut également être affecté à un processus.

Vous pouvez étendre les privilèges qui sont disponibles de deux manières.

- Le jeu héritable initial peut être étendu pour les utilisateurs, les rôles et les systèmes.
- Un privilège qui ne figure pas dans le jeu héritable peut également être affecté à un processus de manière explicite.

L'affectation des privilèges par processus est le moyen le plus précis pour ajouter des privilèges. Vous pouvez augmenter le nombre des opérations privilégiées qu'un utilisateur est autorisé à effectuer en affectant un rôle à l'utilisateur. Le rôle se voit affecter des profils de droits qui comprennent des commandes avec des privilèges ajoutés. Lorsque l'utilisateur endosse le rôle, il reçoit le shell de profil du rôle. Lorsque les commandes du profil de droits sont saisies dans le shell du rôle, les commandes s'exécutent avec les privilèges ajoutés.

Vous pouvez également affecter un profil de droits à l'utilisateur plutôt qu'à un rôle que l'utilisateur endosse. Lorsque l'utilisateur ouvre un shell de profil, tel que `pfksh`, il peut exécuter les commandes dans son profil de droits avec privilège. Dans un shell standard, les commandes ne s'exécutent pas avec des privilèges. Le processus privilégié peut s'exécuter uniquement dans un shell privilégié.

Développer le jeu héritable initial de privilèges pour des utilisateurs, des rôles ou des systèmes est une manière d'affecter des privilèges plus risquée. Tous les privilèges dans le jeu héritable figurent dans le jeu autorisé et le jeu effectif. Toutes les commandes que l'utilisateur ou le rôle tape dans un shell peuvent utiliser les privilèges affectés directement. Les privilèges affectés directement permettent à un utilisateur ou à un rôle d'effectuer facilement des opérations qui peuvent figurer en dehors des limites de leurs responsabilités administratives.

Lorsque vous ajoutez des privilèges au jeu héritable initial sur un système, tous les utilisateurs qui se connectent au système disposent d'un jeu de privilèges de base plus grand. Cette affectation directe permet à tous les utilisateurs du système d'effectuer facilement des opérations qui figurent probablement en dehors des limites des utilisateurs standard.

---

**Remarque** – Le jeu limite ne peut pas être étendu, car il contient initialement tous les privilèges.

---

## Restriction des privilèges d'un utilisateur ou d'un rôle

La suppression de privilèges permet d'empêcher les utilisateurs et les rôles d'exécuter certaines tâches. Vous pouvez supprimer des privilèges du jeu héritable initial et du jeu limite. Vous devez soigneusement tester la suppression de privilèges avant de distribuer un jeu héritable initial ou un jeu limite, plus petit que le jeu par défaut. En supprimant des privilèges du jeu héritable initial, vous risquez d'empêcher les utilisateurs de se connecter. Lorsque des privilèges sont supprimés du jeu limite, un ancien programme `setuid` peut échouer, car il nécessite un privilège qui a été supprimé.

## Affectation de privilèges à un script

Les scripts sont exécutables, tout comme les commandes. Par conséquent, dans un profil de droits, vous pouvez ajouter des privilèges à un script de la même façon que vous pouvez ajouter des privilèges à une commande. Le script s'exécute avec les privilèges ajoutés lorsqu'un utilisateur ou un rôle à qui le profil de droits a été affecté exécute le script dans un shell de profil. Si le script contient des commandes qui nécessitent des privilèges, les commandes avec les privilèges ajoutés doivent également figurer dans un profil de droits affecté.

Les programmes conscients des privilèges peuvent restreindre les privilèges par processus. Votre tâche en ce qui concerne un programme conscient des privilèges consiste à affecter à l'exécutable seulement les privilèges dont le programme a besoin. Vous devez ensuite tester le programme pour vérifier qu'il accomplit ses tâches correctement. Vous devez également vérifier que le programme ne fait pas une utilisation abusive des privilèges.

## Privilèges et périphériques

Le modèle de privilège utilise des privilèges pour protéger les interfaces système qui, dans le modèle de superutilisateur, ne sont protégées par des autorisations de fichier. Dans un système doté de privilèges, les autorisations de fichier sont trop faibles pour protéger les interfaces. Un privilège comme `proc_owner` peut remplacer les autorisations de fichier et donner ensuite l'accès complet au système.

Par conséquent, dans Oracle Solaris la propriété du répertoire de périphérique n'est pas suffisante pour ouvrir un périphérique. Par exemple, les membres du groupe `sys` ne sont plus automatiquement autorisés à accéder au périphérique `/dev/ip`. Les autorisations de fichier sur `/dev/ip` sont `0666`, mais le privilège `net_rawaccess` est requis pour ouvrir le périphérique.

La stratégie de périphériques est contrôlée par des privilèges. La commande `getdevpolicy` affiche la stratégie pour chaque périphérique. La commande de configuration de périphérique `devfsadm` installe la stratégie de périphérique. La commande `devfsadm` lie les jeux de privilèges

avec `open` pour la lecture ou l'écriture de périphériques. Pour plus d'informations, reportez-vous aux pages de manuel [getdevpolicy\(1M\)](#) et [devfsadm\(1M\)](#).

La stratégie de périphériques offre une plus grande souplesse dans l'octroi d'autorisations pour ouvrir des périphériques. Vous pouvez nécessiter d'autres privilèges ou plus de privilèges que ceux prévus par la stratégie de périphérique par défaut. Les exigences en matière de privilèges peuvent être modifiées pour la stratégie de périphérique et les propriétés du pilote. Vous pouvez modifier les privilèges lors de l'installation, de l'ajout ou de la mise à jour d'un pilote de périphérique.

Les commandes `add_drv` et `update_drv` servent à modifier les entrées de stratégie de périphérique et les privilèges spécifiques au pilote. Vous devez exécuter un processus avec le jeu complet de privilèges pour modifier la stratégie de périphérique. Pour plus d'informations, reportez-vous aux pages de manuel [add\\_drv\(1M\)](#) et [update\\_drv\(1M\)](#).

## Privilèges et débogage

Oracle Solaris fournit des outils pour déboguer les défaillances des privilèges. Les commandes `ppriv` et `truss` fournissent le résultat du débogage. Pour consulter des exemples, reportez-vous à la page de manuel [ppriv\(1\)](#). Pour connaître la procédure, reportez-vous à la section [“Procédure de détermination des privilèges requis par un programme” à la page 211](#). Vous pouvez également exécuter la commande `dt race`. Pour plus d'informations, reportez-vous à la page de manuel [dt race\(1M\)](#).





# Utilisation du contrôle d'accès basé sur les rôles (tâches)

Ce chapitre traite des tâches permettant de répartir les capacités de superutilisateur à l'aide de rôles discrets. Les mécanismes pouvant être utilisés par les rôles comprennent les profils de droits, les autorisations et les privilèges. Vous trouverez ci-après une liste des tâches contenues dans ce chapitre.

- [“Utilisation de RBAC \(tâches\)” à la page 169](#)
- [“Utilisation des privilèges \(tâches\)” à la page 204](#)

Pour une présentation de RBAC, reportez-vous à la section [“Contrôle d'accès basé sur les rôles \(présentation\)” à la page 145](#). Pour des informations de référence, reportez-vous au [Chapitre 10, “Attributs de sécurité dans Oracle Solaris \(référence\)”](#). Pour utiliser les privilèges, reportez-vous à la section [“Utilisation des privilèges \(tâches\)” à la page 204](#).

## Utilisation de RBAC (tâches)

L'utilisation de RBAC requiert de planifier et configurer RBAC et de savoir endosser un rôle. Une fois familiarisé avec les rôles, vous pouvez personnaliser davantage RBAC pour gérer de nouvelles opérations. La liste des tâches suivante fait référence à ces tâches principales, y compris l'utilisation de privilège.

| Tâche                                                | Description                                                         | Voir                                                                                                    |
|------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Utilisation de la configuration RBAC par défaut.     | Affichez et utilisez le RBAC sans modifier l'installation initiale. | <a href="#">“Affichage et utilisation des valeurs par défaut RBAC (liste des tâches)” à la page 170</a> |
| Planification, configuration et utilisation du RBAC. | Personnalisez RBAC pour votre site.                                 | <a href="#">“Configuration initiale RBAC (liste des tâches)” à la page 177</a>                          |
| Administration de RBAC.                              | Mettez à jour la configuration du RBAC de votre site.               | <a href="#">“Gestion de RBAC (liste des tâches)” à la page 192</a>                                      |

| Tâche                                  | Description                                                                                                                                                                                | Voir                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Gestion et utilisation des privilèges. | Ajoutez et supprimez des privilèges d'utilisateurs, de rôles, de systèmes et de processus. Utilisez les privilèges. Affichez et résolvez les problèmes liés à l'utilisation de privilèges. | <a href="#">“Utilisation des privilèges (tâches)” à la page 204</a> |

## Affichage et utilisation des valeurs par défaut RBAC (tâches)

Des droits sont affectés aux utilisateurs par défaut. Les droits pour tous les utilisateurs d'un système sont affectés dans le fichier `/etc/security/policy.conf`.

### Affichage et utilisation des valeurs par défaut RBAC (liste des tâches)

Lors de l'installation d'Oracle Solaris, votre système est configuré avec des droits d'utilisateurs et des droits de processus. Sans autre configuration, utilisez la liste des tâches ci-dessous pour afficher et utiliser RBAC.

| Tâche                                                              | Description                                                                                                                   | Voir                                                                                            |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Affichage du contenu des bases de données d'attributs de sécurité. | Répertoriez toutes les autorisations, les profils de droits et les commandes avec les attributs de sécurité sur le système.   | <a href="#">“Procédure d'affichage de tous les attributs de sécurité définis” à la page 170</a> |
| Affichage de vos droits.                                           | Dressez la liste de vos profils de droits, vos autorisations, vos privilèges et vos rôles affectés.                           | <a href="#">“Procédure d'affichage des droits qui vous sont affectés” à la page 171</a>         |
| Adoption du rôle root.                                             | L'utilisateur initial acquiert des droits d'administration.                                                                   | <a href="#">“Procédure d'endossement d'un rôle” à la page 174</a>                               |
| Connexion en tant qu'administrateur.                               | Les utilisateurs auxquels des droits d'administration sont affectés disposent de plusieurs méthodes pour utiliser ces droits. | <a href="#">“Procédure d'obtention des droits d'administration” à la page 175</a>               |

#### ▼ Procédure d'affichage de tous les attributs de sécurité définis

Utilisez les commandes suivantes pour répertorier toutes les autorisations et tous les profils de droits et les commandes avec les attributs de sécurité sur le système. Pour répertorier tous les privilèges définis, reportez-vous à la section [“Procédure de création d'une liste des privilèges sur le système” à la page 205](#).

**1 Répertoriez toutes les autorisations.**

```
% getent auth_attr | more
solaris.:::All Solaris Authorizations::help=AllSolAuthsHeader.html
solaris.account.:::Account Management::help=AccountHeader.html
...
solaris.zone.login:::Zone Login::help=ZoneLogin.html
solaris.zone.manage:::Zone Deployment::help=ZoneManage.html
```

**2 Répertoriez tous les profils de droits.**

```
% getent prof_attr | more
All:::Execute any command as the user or role:help=RtAll.html
Audit Configuration:::Configure Solaris Audit:auths=solaris.smf.value.audit;
help=RtAuditCfg.html
...
Zone Management:::Zones Virtual Application Environment Administration:
help=RtZoneMngmnt.html
Zone Security:::Zones Virtual Application Environment Security:auths=solaris.zone.*,
solaris.auth.delegate;help=RtZoneSecurity.html ...
```

**3 Répertoriez toutes les commandes avec des attributs de sécurité.**

```
% getent exec_attr | more
All:solaris:cmd:::*:
Audit Configuration:solaris:cmd:::/usr/sbin/auditconfig:privs=sys_audit
...
Zone Security:solaris:cmd:::/usr/sbin/txzonemgr:uid=0
Zone Security:solaris:cmd:::/usr/sbin/zonecfg:uid=0 ...
```

**▼ Procédure d'affichage des droits qui vous sont affectés**

Utilisez les commandes suivantes pour afficher vos affectations RBAC. Pour afficher tous les droits qui peuvent être affectés, reportez-vous à la section [“Procédure d'affichage de tous les attributs de sécurité définis” à la page 170](#).

**1 Répertoriez vos autorisations.**

```
% auths
solaris.device.cdrw,solaris.device.mount.removable,solaris.mail.mailq
```

Ces autorisations sont affectées à l'ensemble des utilisateurs par défaut.

**2 Répertoriez vos profils de droits.**

```
% profiles
Basic Solaris User
All
```

Par défaut, ces profils de droits sont affectés à tous les utilisateurs par défaut.

**3 Répertoriez les rôles qui vous sont affectés.**

```
% roles
root
```

Ce rôle est affecté à l'utilisateur initial par défaut. Aucun rôle indique qu'aucun rôle ne vous est affecté.

#### 4 Répertoriez les privilèges dans votre shell par défaut.

```
% ppriv $$
1234:    /bin/csh
flags = <none>
  E: basic
  I: basic
  P: basic
  L: all
```

Le jeu de privilèges de base est affecté par défaut à tous les utilisateurs. Le jeu limite contient tous les privilèges.

```
% ppriv -vl basic
file_link_any
    Allows a process to create hardlinks to files owned by a uid
    different from the process' effective uid.
file_read
    Allows a process to read objects in the filesystem.
file_write
    Allows a process to modify objects in the filesystem.
net_access
    Allows a process to open a TCP, UDP, SDP or SCTP network endpoint.
proc_exec
    Allows a process to call execve().
proc_fork
    Allows a process to call fork1()/forkall()/vfork()
proc_info
    Allows a process to examine the status of processes other
    than those it can send signals to. Processes which cannot
    be examined cannot be seen in /proc and appear not to exist.
proc_session
    Allows a process to send signals or trace processes outside its session.
```

#### 5 Répertoriez les privilèges sur les commandes dans vos profils de droits.

```
% profiles -l
Basic Solaris User
  /usr/bin/cdda2wav.bin  privs=file_dac_read,sys_devices,
    proc_priocntl,net_privaddr
  /usr/bin/cdrecord.bin  privs=file_dac_read,sys_devices,
    proc_lock_memory,proc_priocntl,net_privaddr
  /usr/bin/readcd.bin    privs=file_dac_read,sys_devices,net_privaddr
All
*
```

Les profils de droit d'un utilisateur peuvent comprendre des commandes qui s'exécutent avec des privilèges particuliers. Le profil d'utilisateur de base Solaris comprend des commandes permettant de lire et d'écrire sur des CD-ROM.

**Exemple 9–1** Liste des autorisations d'un utilisateur

```
% auths username
solaris.device.cdrw,solaris.device.mount.removable,solaris.mail.mailq
```

**Exemple 9–2** Liste des profils de droits d'un utilisateur ou d'un rôle

La commande suivante répertorie les profils de droits d'un utilisateur spécifique.

```
% profiles jdoe
jdoe:
    Basic Solaris User
    All
```

La commande suivante répertorie les profils de droits du rôle cryptomgt.

```
% profiles cryptomgt
cryptomgt:
    Crypto Management
    Basic Solaris User
    All
```

La commande suivante répertorie les profils de droits du rôle root :

```
% profiles root
root:
    All
    Console User
    Network Wifi Info
    Desktop Removable Media User
    Suspend To RAM
    Suspend To Disk
    Brightness
    CPU Power Management
    Network Autoconf User
    Basic Solaris User
```

**Exemple 9–3** Liste des rôles affectés à un utilisateur

La commande suivante répertorie les rôles affectés à un utilisateur spécifique.

```
% roles jdoe
root
```

**Exemple 9–4** Liste des privilèges d'un utilisateur sur des commandes spécifiques

La commande suivante répertorie les commandes privilégiées dans les profils de droits d'un utilisateur standard.

```
% profiles -l jdoe
jdoe:
    Basic Solaris User
```

```

/usr/bin/cdda2wav.bin   privs=file_dac_read,sys_devices,
                        proc_priocntl,net_privaddr
/usr/bin/cdrecord.bin   privs=file_dac_read,sys_devices,
                        proc_lock_memory,proc_priocntl,net_privaddr
/usr/bin/readcd.bin     privs=file_dac_read,sys_devices,net_privaddr
All
*
```

## ▼ Procédure d'endossement d'un rôle

### Avant de commencer

Le rôle doit déjà vous être affecté. Le service de noms doit être mis à jour avec ces informations.

#### 1 Dans une fenêtre de terminal, déterminez les rôles que vous pouvez endosser.

```
% roles
Comma-separated list of role names is displayed
```

#### 2 Utilisez la commande su pour endosser un rôle.

```
% su - rolename
Password:      <Type rolename password>
$
```

La commande `su - rolename` change le shell en shell de profil pour le rôle. Un shell de profil reconnaît les attributs de sécurité, tels que les autorisations, les privilèges et les bits ID définis.

#### 3 (Facultatif) Vérifiez que vous endossez à présent un rôle.

```
$ /usr/bin/whoami
rolename
```

Vous pouvez maintenant effectuer des tâches de ce rôle dans cette fenêtre de terminal.

#### 4 (Facultatif) Affichez les capacités de votre rôle.

Pour plus d'informations sur cette procédure, reportez-vous à la section [“Procédure d'affichage des droits qui vous sont affectés”](#) à la page 171.

### Exemple 9-5 Endossement du rôle root

Dans l'exemple suivant, l'utilisateur initial endosse le rôle root et répertorie les privilèges dans le shell du rôle.

```
% roles
root
% su - root
Password:      <Type root password>
#             Prompt changes to root prompt
# ppriv $$
1200:   pfksh
flags = <none>
```

```
E: all
I: basic
P: all
L: all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section [“Privilèges \(présentation\)”](#) à la page 158.

## ▼ Procédure d'obtention des droits d'administration

Des droits d'administration sont en vigueur lorsque vous exécutez un shell de profil. Par défaut, un compte du rôle obtient un shell de profil. Les rôles sont des comptes spéciaux qui obtiennent des droits d'administration spécifiques, généralement liés à un jeu de tâches d'administration, telles que l'examen des fichiers d'audit

Dans le rôle root, l'utilisateur initial dispose de tous les droits d'administration, c'est-à-dire que l'utilisateur initial est superutilisateur. Le rôle root peut créer d'autres rôles.

### Avant de commencer

Pour administrer le système, vous devez disposer de droits qui ne sont pas affectés aux utilisateurs standard. Si vous n'êtes pas superutilisateur, vous devez obtenir un rôle, un profil de droits d'administration ou des autorisations ou privilèges spécifiques.

### ● Choisissez l'une des méthodes suivantes pour exécuter des commandes d'administration.

Ouvrez une fenêtre de terminal.

#### ■ Connectez-vous en tant que root

```
% su -
Password:      Type the root password
#
```

---

**Remarque** – Cette méthode fonctionne aussi bien lorsque root est un utilisateur que lorsqu'il est un rôle. L'invite avec le signe dièse (#) indique que vous êtes maintenant superutilisateur.

---

#### ■ Endossez un rôle qui vous a été affecté.

Dans l'exemple suivant, vous endossez un rôle de gestion du réseau. Ce rôle inclut le profil de droits Network Management (gestion du réseau).

```
% su - networkadmin
Password:      Type the networkadmin password
$
```

Vous êtes à présent dans un shell de profil. Dans ce shell, vous pouvez exécuter snoop, router, dladm, et d'autres commandes. Pour en savoir plus sur les shells de profil, reportez-vous à la section [“Shells de profil et RBAC”](#) à la page 156.

---

**Astuce** – Suivez les étapes décrites à la section “[Procédure d’affichage des droits qui vous sont affectés](#)” à la page 171 pour afficher les capacités de votre rôle.

---

- **Utilisez la commande `pfbash` pour créer un shell qui s'exécute avec les droits d'administration.**

Par exemple, le jeu de commandes ci-après vous permet d'examiner les paquets du réseau dans le shell `pfbash` :

```
% pfbash
$ anoop
```

Si le privilège `net_observability` ne vous est pas affecté, la commande `snoop` échoue avec un message d'erreur similaire à celui-ci : `snoop: cannot open "net0": Permission denied`. Si le privilège vous est affecté directement ou par l'intermédiaire d'un profil de droits ou d'un rôle, cette commande réussira. Vous pouvez également exécuter d'autres commandes privilégiées dans ce shell.

- **Utilisez la commande `pfexec` pour créer un processus qui s'exécute avec les droits d'administration.**

Exécutez la commande `pfexec` avec le nom d'une commande privilégiée de votre profil de droits. Par exemple, la commande suivante vous permet d'examiner les paquets du réseau :

```
% pfexec snoop
```

Les mêmes limitations de privilèges s'appliquent à `pfexec` comme à `pfbash`. Cependant, pour exécuter une autre commande privilégiée, vous devez saisir `pfexec` une nouvelle fois avant de taper la commande privilégiée.

### Exemple 9–6 Mise en cache de l'authentification pour faciliter l'utilisation des rôles

Dans cet exemple, l'administrateur configure un rôle pour gérer le réseau et facilite son utilisation mettant en cache l'authentification de l'utilisateur. Tout d'abord, l'administrateur crée et affecte le rôle.

```
# roleadd -K roleauth=user -P "Network Management" netmgt
# usermod -R +netmgt jdoe
```

Quand `jdoe` utilise l'option `-c` lors du changement de rôle, un mot de passe est requis avant que la sortie `snoop` ne s'affiche :

```
% su - netmgt -c snoop options
Password:
```

```
snoop output
```

Si l'authentification n'est pas mise en cache, et `jdoe` réexécute immédiatement la commande, une invite de mot de passe s'affiche.



L'administrateur configure le fichier `pam.conf` pour mettre en cache l'authentification, de sorte qu'un mot de passe est requis initialement mais pas par la suite jusqu'à ce qu'un certain laps de temps se soit écoulé. L'administrateur place toutes les piles personnalisées `pam.conf` à la fin du fichier.

```
# vi /etc/pam.conf
...
#
## Cache authentication for switched user
#
su      auth required          pam_unix_cred.so.1
su      auth sufficient        pam_tty_tickets.so.1
su      auth requisite         pam_authtok_get.so.1
su      auth required          pam_dhkeys.so.1
su      auth required          pam_unix_auth.so.1
```

Après avoir créé les entrées, l'administrateur vérifie les fautes de frappe, omissions ou répétitions dans les entrées.

L'intégralité de la pile `su` est requise. Le module `pam_tty_tickets.so.1` fournit le cache. Pour plus d'informations sur PAM, reportez-vous à la page de manuel [pam.conf\(4\)](#) et au [Chapitre 15](#), “Utilisation de PAM”.

Une fois la pile PAM `su` ajoutée au fichier `pam.conf`, le rôle `netmgt` n'est invité qu'une seule fois à indiquer son mot de passe lors de l'exécution d'une série de commandes.

```
% su - netmgt -c snoop options
Password:

      snoop output
% su - netmgt -c snoop options
      snoop output
...
```

## Personnalisation RBAC pour votre site (tâches)

La configuration initiale de RBAC inclut la création d'utilisateurs qui peuvent endosser des rôles spécifiques, créer des rôles et les affecter aux utilisateurs appropriés.

### Configuration initiale RBAC (liste des tâches)

Utilisez la liste des tâches ci-dessous pour planifier et implémenter initialement RBAC sur votre site. Certaines tâches sont triées.

| Tâche                                                           | Description                                                                                                                                                                                                           | Voir                                                                                                                                                             |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Planification de RBAC.                                       | Analysez les besoins de sécurité de votre site et décidez de l'utilisation de RBAC sur votre site.                                                                                                                    | <a href="#">“Procédure de planification de votre implémentation RBAC” à la page 178</a>                                                                          |
| 2. Configuration des utilisateurs qui peuvent endosser un rôle. | Assurez-vous qu'il existe des utilisateurs qui peuvent endosser un rôle d'administration.                                                                                                                             | <a href="#">“Configuration et administration des comptes utilisateur (liste des tâches)” du manuel <i>Administration d'Oracle Solaris : Tâches courantes</i></a> |
| 3. Création de rôles.                                           | Créez les rôles et affectez-les à des utilisateurs.                                                                                                                                                                   | <a href="#">“Procédure de création d'un rôle” à la page 181</a><br><a href="#">“Procédure d'attribution de rôle” à la page 183</a>                               |
| (Recommandé) Audit des actions des rôles.                       | Présélectionnez une classe d'audit incluant un événement d'audit qui enregistre les actions de rôles.                                                                                                                 | <a href="#">“Procédure d'audit des rôles” à la page 184</a>                                                                                                      |
| Création ou modification de profils de droits.                  | Créez un profil de droits. Ou modifiez les attributs de sécurité ou les profils de droits supplémentaires dans un profil de droits.<br><br>Ajoutez des privilèges à une commande.                                     | <a href="#">“Procédure de création ou de modification d'un profil de droits” à la page 186</a><br><br><a href="#">Exemple 9–14</a>                               |
| Sécurisation d'anciennes applications.                          | Active les autorisations d'ID définis pour les anciennes applications. Les scripts peuvent contenir des commandes avec des ID définis. Les anciennes applications peuvent vérifier les autorisations, le cas échéant. | <a href="#">“Procédure d'ajout de propriétés RBAC aux anciennes applications” à la page 188</a><br><br><a href="#">Exemple 9–16</a>                              |
| Dépannage de l'affectation d'attributs de sécurité.             | Déterminez les raisons pour lesquelles les attributs de sécurité peuvent ne pas être disponibles pour les utilisateurs, les rôles ou les processus.                                                                   | <a href="#">“Procédure de dépannage de RBAC et de l'affectation de privilèges” à la page 189</a>                                                                 |

## ▼ Procédure de planification de votre implémentation RBAC

RBAC peut faire partie intégrante de la façon dont une entreprise gère ses sources d'informations. La planification requiert une connaissance approfondie des fonctionnalités de RBAC et des exigences en matière de sécurité de votre organisation.

---

**Remarque** – Des droits par défaut sont affectés dans le fichier `/etc/security/policy.conf`.

---

### 1 Découvrez les concepts RBAC de base.

Lisez la section [“Contrôle d'accès basé sur les rôles \(présentation\)” à la page 145](#). L'utilisation de RBAC pour administrer un système est très différente de l'utilisation des pratiques

administratives UNIX conventionnelles. Pour vous familiariser avec les concepts RBAC avant de commencer l'implémentation, reportez-vous au [Chapitre 10, “Attributs de sécurité dans Oracle Solaris \(référence\)”](#).

## 2 Examinez votre stratégie de sécurité.

La stratégie de sécurité de votre entreprise détaille les menaces potentielles pour votre système, mesure les risques de chaque menace et fournit des stratégies pour les contrer. L'isolation des tâches liées à la sécurité par le biais de RBAC peut être une partie de la stratégie. Bien que vous puissiez utiliser les configurations RBAC en l'état, vous pouvez être amené à les personnaliser pour adhérer à la stratégie de sécurité en vigueur.

## 3 Décidez du degré de nécessité de RBAC pour votre organisation.

En fonction de vos besoins en matière de sécurité, vous pouvez utiliser différents degrés de RBAC, comme suit :

- **Root en tant que rôle** : cette méthode est fournie par défaut. Elle empêche tout utilisateur de se connecter en tant que root. Au lieu de cela, un utilisateur doit se connecter à l'aide de la connexion qui leur est affectée avant d'endosser le rôle root.
- **Rôles discrets** : cette méthode crée des rôles qui sont basés sur des profils de droits fournis. Les rôles peuvent être affectés selon le niveau de responsabilité, l'étendue de la tâche et le type de tâche. Par exemple, le rôle d'administrateur système peut effectuer un grand nombre de tâches que le superutilisateur peut effectuer, tandis que le rôle de gestion IPsec réseau peut gérer IPsec.

Vous pouvez également séparer les responsabilités de sécurité des autres responsabilités, le rôle de gestion des utilisateurs peut créer des utilisateurs, tandis que le rôle de sécurité des utilisateurs peut affecter les attributs de sécurité, tels que les rôles et les profils de droits. Cependant, le rôle de sécurité des utilisateurs ne peut pas créer un utilisateur, et le rôle de gestion des utilisateurs ne peut pas affecter un profil de droits à un utilisateur.

- **Aucun rôle root** : pour utiliser cette méthode, vous devez modifier la configuration par défaut du système. Dans cette configuration, tout utilisateur connaissant le mot de passe pour root peut se connecter et modifier le système. Vous ne pouvez pas connaître l'identité de l'utilisateur ayant agi en tant que superutilisateur.

## 4 Déterminez les rôles appropriés pour votre organisation.

Passer en revue les capacités des rôles recommandés et leurs profils de droits par défaut. Les profils de droits par défaut permettent aux administrateurs de configurer un rôle recommandé en utilisant un seul profil.

Pour examiner de manière plus approfondie les profils de droits, procédez de l'une des manières suivantes :

- Pour les profils de droits disponibles sur votre système, utilisez la commande `getent prof_attr`.
- Dans ce guide, reportez-vous à la section “[Profils de droits](#)” à la [page 215](#) pour obtenir le résumé de certains profils de droits habituels.

## **5 Déterminez si l'un des rôles ou des profils de droits supplémentaires sont appropriés pour votre organisation.**

Recherchez d'autres applications ou familles d'applications sur votre site susceptibles de bénéficier d'un accès limité. Les applications affectant la sécurité, pouvant entraîner des problèmes de déni de service ou nécessitant une formation d'administrateur système particulière constituent de bons candidats pour RBAC. Vous pouvez personnaliser des rôles et des profils de droits pour gérer les exigences de sécurité de votre organisation.

### **a. Déterminez les commandes nécessaires pour la nouvelle tâche.**

### **b. Choisissez le profil de droits approprié pour cette tâche.**

Vérifiez si un profil de droits existant peut traiter cette tâche ou si un autre profil de droits doit être créé.

---

**Remarque** – Les profils de droits Media Backup (sauvegarde des médias) et Media Restore (restauration des médias) fournissent un accès à l'intégralité du système de fichiers racine. Par conséquent, ces profils de droits sont affectés aux utilisateurs de confiance uniquement. Vous pouvez également choisir de ne pas affecter ces profils de droits. Par défaut, seul le rôle root est autorisé à sauvegarder et restaurer.

---

### **c. Déterminez le rôle approprié pour ce profil de droits.**

Choisissez si le profil de droits pour cette tâche doit être attribué à un rôle existant ou si un nouveau rôle doit être créé. Si vous utilisez un rôle existant, assurez-vous que les profils de droits d'origine du rôle sont appropriés pour les utilisateurs affectés à ce rôle. Classez le nouveau profil de droits de sorte que les commandes s'exécutent avec leurs privilèges requis. Pour plus d'informations sur le classement, reportez-vous à la section “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la [page 217](#).

## **6 Déterminez les utilisateurs devant être affectés aux rôles.**

Selon le principe du [moindre privilège](#), vous devez affecter des utilisateurs à des rôles adaptés à leur niveau de confiance. Lorsque vous empêchez les utilisateurs d'effectuer des tâches qu'ils n'ont pas besoin d'effectuer, vous réduisez les problèmes potentiels.

## ▼ Procédure de création d'un rôle

Les rôles peuvent être créés localement et dans un référentiel LDAP.

**Avant de commencer**

Pour créer un rôle et affecter son mot de passe initial, le profil de droits User Management (gestion des utilisateurs) doit vous être affecté. Pour affecter des attributs de sécurité au rôle, le profil de droits User Security (sécurité des utilisateurs) doit vous être affecté.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

**2 Pour créer un rôle, utilisez la commande `roleadd`.**

Les arguments RBAC de la commande sont les suivants :

```
# roleadd [-e expire] [-f inactive] [-s shell] [-m] [-S repository] \
[-A authorization-list] -K key=value rolename
```

|                                 |                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-e <i>expire</i></code>   | Date d'expiration d'un rôle. Utilisez cette option pour créer des rôles temporaires.                                                                                                                       |
| <code>-f <i>inactive</i></code> | Nombre maximal de jours autorisé entre les utilisations d'un rôle. Lorsque la valeur <i>inactive</i> est dépassée, le rôle ne peut pas être utilisé. La valeur par défaut est 0, aucune date d'expiration. |
| <code>-m</code>                 | Crée un répertoire personnel pour <i>rolename</i> à l'emplacement par défaut.                                                                                                                              |
| <code>-s <i>shell</i></code>    | Shell de connexion pour <i>rolename</i> . Ce shell doit être un shell de profil. Pour obtenir une liste des shells de profil, reportez-vous à la page de manuel <a href="#">pfexec(1)</a> .                |

---

**Astuce** – Vous pouvez également répertorier les shells de profil dans le répertoire `/usr/binsur` votre système, comme dans `ls /usr/bin/pf*sh`.

---

|                                           |                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-S <i>repository</i></code>         | L'un de <code>files</code> ou <code>ldap</code> . La valeur par défaut correspond à des fichiers locaux.                                                                                                                                                                                                               |
| <code>-A <i>authorization-list</i></code> | Une ou plusieurs autorisations séparées par des virgules. Pour obtenir la liste des autorisations, reportez-vous au fichier <code>/etc/security/auth_attr</code> .                                                                                                                                                     |
| <code>-K <i>key=value</i></code>          | Paire <i>key=value</i> . Cette option peut être répétée. Les clés suivantes sont disponibles : <code>audit_flags</code> , <code>auths</code> , <code>profiles</code> , <code>project</code> , <code>defaultpriv</code> , <code>limitpriv</code> , <code>lock_after_retries</code> et <code>roleauth</code> . Pour plus |

d'informations sur les clés, leurs valeurs et les autorisations requises pour définir les valeurs, reportez-vous à la page de manuel [user\\_attr\(4\)](#).

*rolename*

Nom du nouveau rôle. Pour connaître les restrictions sur les chaînes acceptables, reportez-vous à la page de manuel [roleadd\(1M\)](#).

---

**Astuce** – Lorsque le nom du rôle reflète le nom d'un profil de droits, vous pouvez facilement comprendre l'objectif de ce rôle. Par exemple, affectez le profil de droits Audit Review (vérification d'audit) au rôle `audit review` pour permettre au rôle de lire, de filtrer et d'archiver des enregistrements d'audit.

---

Par exemple, la commande suivante crée un rôle d'administrateur des utilisateurs local et un répertoire personnel.

```
# roleadd -c "User Administrator role, local" -s /usr/bin/pfbbash \
-m -K profiles="User Security,User Management" useradm
80 blocks
# ls /export/home/useradm
local.cshrc      local.login      local.profile
```

### 3 Créez le mot de passe initial du rôle.

```
# passwd -r files useradmPassword:      <Type useradm password>
Confirm Password:    <Retype useradm password>
#
```

---

**Remarque** – En règle générale, un compte de rôle est affecté à plusieurs utilisateurs. Par conséquent, un administrateur crée généralement un mot de passe du rôle et fournit aux utilisateurs le mot de passe du rôle hors bande.

---

### 4 Pour affecter un rôle à un utilisateur, exécutez la commande `usermod`.

Pour connaître la procédure, reportez-vous à la section [“Procédure d'attribution de rôle”](#) à la page 183 et à l'[Exemple 9–10](#).

## Exemple 9–7 Création d'un rôle d'administrateur des utilisateurs dans le référentiel LDAP

Dans cet exemple, le site de l'administrateur utilise un référentiel LDAP. En exécutant la commande suivante, l'administrateur crée un rôle d'administrateur des utilisateurs dans LDAP.

```
# roleadd -c "User Administrator role, LDAP" -s /usr/bin/pfbbash \
-m -S ldap -K profiles="User Security,User Management" useradm
```

**Exemple 9–8** Création de rôles pour la séparation des tâches

Dans cet exemple, le site de l'administrateur utilise un référentiel LDAP. En exécutant les commandes suivantes, l'administrateur crée deux rôles. Le rôle `usermgt` peut créer des utilisateurs, leur attribuer des répertoires personnels, leur assigner un mot de passe initial et effectuer d'autres tâches non liées à la sécurité. Le rôle `usersec` ne peut pas créer d'utilisateurs, mais peut modifier les mots de passe d'utilisateur et d'autres propriétés RBAC.

```
# roleadd -c "User Management role, LDAP" -s /usr/bin/pfbash \
-m -S ldap -K profiles="User Management" usermgt
# roleadd -c "User Security role, LDAP" -s /usr/bin/pfbash \
-m -S ldap -K profiles="User Security" usersec
```

**Exemple 9–9** Création d'un rôle de sécurité des dispositifs et des fichiers

Dans cet exemple, l'administrateur crée un rôle de sécurité des dispositifs et des fichiers pour ce système :

```
# roleadd -c "Device and File System Security admin, local" -s /usr/bin/pfbash \
-m -K profiles="Device Security,File System Security" devflsec
```

▼ **Procédure d'attribution de rôle**

Cette procédure permet d'attribuer un rôle à un utilisateur, redémarre le démon cache du nom, puis affiche la manière dont l'utilisateur peut endosser le rôle.

**Avant de commencer**

Vous avez ajouté un rôle et lui avez attribué un mot de passe, comme indiqué à la section [“Procédure de création d'un rôle” à la page 181](#).

Pour modifier la plupart des attributs de sécurité d'un utilisateur, le profil de droits User Security (sécurité des utilisateurs) doit vous être affecté. Pour modifier les indicateurs d'audit d'un utilisateur, vous devez être connecté en tant que superutilisateur. Pour modifier d'autres attributs, le profil de droits User Management (gestion des utilisateurs) doit vous être affecté.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

**2 Attribuez le rôle à un utilisateur.**

```
usermod [-S repository] [RBAC-arguments] login
```

Par exemple, attribuez le rôle à un utilisateur local :

```
# usermod -R +useradm jdoe-local
```

Pour connaître les options de la commande `usermod`, reportez-vous à la page de manuel [usermod\(1M\)](#) ou à la description de l'Étape 2 in “[Procédure de création d'un rôle](#)” à la page 181.

### 3 Pour appliquer les modifications apportées, redémarrez le démon `nscd`.

```
# svcadm restart system/name-service-cache
```

## Exemple 9–10 Création et attribution d'un rôle pour administrer la cryptographie

Dans cet exemple, l'administrateur sur un réseau LDAP crée un rôle pour administrer la structure cryptographique et affecte le rôle à l'UID 1111. L'administrateur redémarre le démon `nscd` pour appliquer l'affectation.

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m -u 104 -s /usr/bin/pfksh \
-S ldap -K profiles="Crypto Management" cryptmgt
# passwd cryptmgt
New Password:      <Type cryptmgt password>
Confirm password:  <Retype cryptmgt password>
# usermod -u 1111 -R +cryptmgt
# svcadm restart system/name-service-cache
```

L'utilisateur avec l'UID 1111 se connecte, puis endosse le rôle et affiche les attributs de sécurité affectés.

```
% su - cryptmgt
Password:      <Type cryptmgt password>
Confirm Password:  <Retype cryptmgt password>
$ profiles -l
    Crypto Management
        /usr/bin/kmfcfg          euid=0
        /usr/sbin/cryptoadm      euid=0
        /usr/sfw/bin/CA.pl       euid=0
        /usr/sfw/bin/openssl     euid=0
$
```

Pour plus d'informations sur la structure cryptographique, reportez-vous au [Chapitre 11](#), “[Structure cryptographique \(présentation\)](#)”. Pour l'administration de la structure, reportez-vous à la rubrique “[Administration de la structure cryptographique \(liste des tâches\)](#)” à la page 254.

## ▼ Procédure d'audit des rôles

Les actions qu'un rôle effectue peuvent faire l'objet d'un audit. Le nom de connexion de l'utilisateur qui endosse le rôle, le nom de rôle, ainsi que l'action que le rôle effectue sont inclus



dans l'enregistrement d'audit. L'événement d'audit 116: AUE\_PFEXEC:execve(2) with pfexec enabled: ps, ex, ua, as capture les actions des rôles. En présélectionnant l'une des classes as, ex, ps, ou ua, les actions du rôle sont auditées.

**Avant de commencer**

Pour configurer l'audit, le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué. Pour activer ou actualiser le service d'audit, vous devez disposer du profil de droits Audit Control (contrôle d'audit).

**1 Incluez l'audit des rôles dans votre plan d'audit.**

Pour obtenir des informations de planification, reportez-vous au [Chapitre 27, “Planification de l'audit”](#).

**2 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

**3 Présélectionnez l'une des classes as, ex, ps, ou ua.**

■ **Si le service d'audit est activé, passez en revue les classes présélectionnées.**

```
# auditconfig -getflags
```

Si l'une des classes as, ex, ps, ou ua est présélectionnée, les actions du rôle sont auditées. Si ce n'est pas le cas, ajoutez l'un de ces classes aux classes existantes.

```
# auditconfig -setflags existing preselections,as
```

■ **Si l'audit n'est pas encore activé, présélectionnez une classe qui audite les actions du rôle.**

```
# auditconfig -setflags as
```

Dans cet exemple, l'administrateur choisit la classe as. Cette classe comprend d'autres événements d'audit. Pour afficher les événements d'audit inclus dans une classe, utilisez la commande `audit record`, comme illustré dans l'[Exemple 28–25](#).

**4 Activez ou actualisez le service d'audit.**

```
# audit -s
```

## ▼ Procédure de création ou de modification d'un profil de droits

Vous pouvez créer ou modifier un profil de droits lorsque les profils de droits fournis ne contiennent pas l'ensemble des attributs de sécurité dont vous avez besoin. Pour plus d'informations sur les profils de droits, reportez-vous à la section “[Profils de droits RBAC](#)” à la page 155.

La façon la plus simple de créer un nouveau profil de droits est de copier et modifier un profil de droits existant.

### Avant de commencer

Pour créer ou modifier un profil de droits, vous devez disposer du profil de droits File Security (sécurité des fichiers).

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Créez un nouveau profil de droits à partir d'un profil existant.

```
# profiles [-S repository] existing-profile-name
```

Vous êtes invité à saisir un nouveau nom. Le contenu du profil de droits existant est dupliqué dans le nouveau profil.

#### 3 Continuez à modifier le nouveau profil de droits.

Ajoutez ou supprimez des profils de droits, des autorisations et d'autres attributs de sécurité, comme indiqué dans les exemples suivants.

### Exemple 9–11 Création d'un nouveau profil de droits à partir d'un profil existant

Dans cet exemple, l'administrateur personnalise le profil de droits Console User (utilisateur de la console) dans le référentiel LDAP.

```
# profiles -S ldap Console User
New name: ExampleCo Console User
ExampleCo Console User >
Description > Manage MyCompany Systems as the Console User
Help > ExCoConsUser.html
```

L'administrateur définit l'attribut `roleauth` pour ce profil de droits.

```
roleauth=yes
```

**Exemple 9–12** Suppression d'un privilège de base d'un profil de droits

Dans l'exemple suivant, après des tests approfondis, l'administrateur de la sécurité supprime un privilège de base de tous les utilisateurs auxquels le profil de droits SunRayUser est affecté. Ils sont dans l'impossibilité d'utiliser le privilège `proc_session`. C'est-à-dire que ces utilisateurs ne peuvent pas examiner les processus à l'extérieur de la session actuelle de l'utilisateur.

```
$ profiles -K defaultpriv=basic,!proc_session SunRayUser
```

**Exemple 9–13** Suppression de privilèges du jeu limite d'un profil de droits

Dans l'exemple suivant, après des tests approfondis, l'administrateur de la sécurité supprime un privilège limite de tous les utilisateurs auxquels le profil de droits SunRayUser est affecté. Cette suppression empêche les utilisateurs d'afficher les processus d'autres utilisateurs.

```
$ profiles -K limitpriv=all,!proc_session SunRayUser
```

**Exemple 9–14** Ajout de privilèges à une commande

Dans cet exemple, l'administrateur de la sécurité ajoute des privilèges à une application dans un profil de droits. L'application est consciente des privilèges.

```
# profiles -p SiteApp
profiles:SiteApp> set desc="Site application"
profiles:SiteApp> add cmd=/opt/site-app/bin/site-cmd
profiles:SiteApp:site-cmd> add privs=proc_fork,proc_taskid
profiles:SiteApp:site-cmd> end
profiles:SiteApp> exit
```

Pour vérifier, l'administrateur sélectionne la commande `site-cmd`.

```
# profiles -p SiteApp "select cmd=/opt/site-app/bin/site-cmd; info;end"
Found profile in files repository.
  id=/opt/site-app/bin/site-cmd
  privs=proc_fork,proc_taskid
```

**Voir aussi** Pour dépanner l'affectation d'attributs de sécurité, reportez-vous à la section [“Procédure de dépannage de RBAC et de l'affectation de privilèges”](#) à la page 189. Pour plus d'informations, reportez-vous à la section [“Ordre de recherche pour les attributs de sécurité affectés”](#) à la page 217.

## ▼ Procédure d'ajout de propriétés RBAC aux anciennes applications

Une ancienne application est une commande ou un jeu de commandes. Les attributs de sécurité sont définis pour chaque commande dans un profil de droits. Le profil de droits est ensuite inclus dans un rôle. Un utilisateur qui endosse le rôle peut exécuter l'ancienne application avec les attributs de sécurité.

### Avant de commencer

Pour créer le profil de droits, le profil de droit Information Security (sécurité des informations) ou Rights Management (gestion des droits) doit vous être affecté. Pour affecter le profil de droits, le profil de droits User Security (sécurité des utilisateurs) doit vous être affecté.

#### 1 Ajoutez les attributs de sécurité aux commandes qui implémentent l'ancienne application.

Vous pouvez ajouter les attributs de sécurité à une ancienne application de la même façon que vous le feriez pour n'importe quelle commande. Vous devez ajouter la commande avec les attributs de sécurité à un profil de droits. Pour une commande héritée, donnez-lui les attributs de sécurité `euclid=0` ou `uid=0`. Pour plus d'informations sur cette procédure, reportez-vous à la section [“Procédure de création ou de modification d'un profil de droits”](#) à la page 186.

##### a. Créez un nouveau profil de droits pour votre ancienne application.

Pour plus d'informations sur les étapes à suivre, reportez-vous à la section [“Procédure de création ou de modification d'un profil de droits”](#) à la page 186.

##### b. Ajoutez les commandes avec les attributs de sécurité requis.

Pour consulter un exemple, reportez-vous à l'[Exemple 9–14](#).

#### 2 Incluez le profil de droits dans la liste des profils d'un rôle.

Pour affecter un profil de droits à un rôle, reportez-vous à l'[Exemple 9–10](#).

### Exemple 9–15 Ajout d'attributs de sécurité à des commandes dans un script

Si une commande d'un script doit avoir le bit `setuid` ou `setgid` défini pour s'exécuter correctement, les attributs de sécurité du fichier exécutable du script *et* de la commande doivent être ajoutés dans un profil de droits. Ensuite, le profil de droits est inclus dans un rôle et le rôle est assigné à un utilisateur. Lorsque l'utilisateur endosse le rôle et exécute le script, la commande s'exécute avec les attributs de sécurité.

**Exemple 9–16 Recherche d'autorisations dans un script ou un programme**

Pour avoir un script pour les autorisations, vous devez ajouter un test basé sur la commande `auths`. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel [auths\(1\)](#).

Par exemple, la ligne suivante vérifie si l'utilisateur dispose de l'autorisation fournie comme argument `$1` :

```
if [ '/usr/bin/auths|/usr/xpg4/bin/grep $1' ]; then
    echo Auth granted
else
    echo Auth denied
fi
```

Pour être plus complet, le test doit inclure une logique vérifiant la présence d'autres autorisations utilisant des caractères génériques. Par exemple, pour tester si l'utilisateur dispose de l'autorisation `solaris.system.date`, vous devez rechercher les chaînes suivantes :

- `solaris.system.date`
- `solaris.system.*`
- `solaris.*`

Si vous écrivez un programme, utilisez la fonction `getauthattr()` pour effectuer un test d'autorisation.

## ▼ Procédure de dépannage de RBAC et de l'affectation de privilèges

Les processus d'un utilisateur ou d'un rôle peuvent ne pas s'exécuter avec les attributs de sécurité qui leurs sont affectés pour différentes raisons.

- L'attribut de sécurité est mal orthographié. Les autorisations mal orthographiées échouent en silence.
- L'utilisateur ou le rôle n'utilise pas le service de noms qui inclut les affectations.
- L'affectation que vous êtes en droit d'attendre n'est pas la première affectation de cet attribut.

L'ordre dans lequel les attributs de sécurité d'un utilisateur ou d'un rôle sont recherchés, puis affectés lors de l'authentification détermine les affectations correctes, sauf pour les autorisations. Lors de la recherche, les autorisations qui sont affectées à l'utilisateur ou au rôle s'accumulent. En revanche, l'affectation de privilèges et l'affectation d'attributs de sécurité dans des profils de droits dépendent de la recherche effectuée. La première affectation est retenue, les suivantes sont ignorées.

- La commande n'est pas exécutée dans un shell de profil.

**Avant de commencer**

Vous devez être dans le rôle root.

**1 Vérifiez et redémarrez le service de noms.**

**a. Vérifiez que les affectations de sécurité pour l'utilisateur ou le rôle sont dans le service de noms activé sur le système.**

**b. Redémarrez le cache du service de noms, `svc:/system/name-service/cache`.**

Le démon `nscd` peut présenter un long intervalle de durée de vie. En redémarrant le démon, vous mettez à jour le service de noms avec les données en cours.

**2 Déterminez le lieu d'affectation d'un attribut de sécurité.**

Utilisez l'attribut de sécurité comme valeur pour la commande `userattr -v`. Par exemple, les commandes suivantes indiquent les attributs de sécurité affectés et le lieu où l'affectation a été effectuée pour l'utilisateur `jdoe` :

```
# userattr -v audit_flags jdoe      Modifications to the system defaults
user_attr: fw:no
# userattr -v auths jdoe           Assigned authorizations
solaris.admin.wusb.read,solaris.device.cdrw,solaris.device.mount.removable,
solaris.mail.mailq,solaris.profmgr.read,solaris.smf.manage.audit,
solaris.smf.value.audit
# userattr -v audit_flags jdoe      Modifications to audit preselection mask
# userattr -v auths jdoe           Assigned authorizations
# userattr -v defaultpriv jdoe      Modifications to basic user privileges
# userattr -v limitpriv jdoe        Modifications to limit privileges
# userattr -v lock_after_retries jdoe Automatic lockout attribute
# userattr -v profiles jdoe        Assigned rights profiles
user_attr: Audit Review,Stop
# userattr roles jdoe             Assigned roles
user_attr : cryptomgt,infosec
```

**3 Pour les profils de droits que vous avez créés, vérifiez que vous avez affecté les attributs de sécurité appropriés à la commande.**

Par exemple, certaines commandes requièrent `uid=0` plutôt que `euid=0` pour s'exécuter correctement. Certains aspects de certaines commandes peuvent requérir des autorisations.

**4 Vérifiez les points suivants si des attributs de sécurité ne sont pas disponibles pour un utilisateur.**

**a. Vérifiez si les attributs de sécurité sont directement affectés à l'utilisateur.**

Utilisez la commande `userattr`.

**b. Si les attributs de sécurité ne sont pas directement affectés, vérifiez les profils de droits qui sont directement affectés à l'utilisateur.**

**i. Dans l'ordre, recherchez l'affectation de l'attribut de sécurité dans la liste des profils de droits.**

La valeur de l'attribut dans les premiers profils de droits de la liste est la valeur que l'utilisateur peut utiliser. Si cette valeur est incorrecte, modifiez-la dans ce profil de droits, ou réorganisez la liste des profils.

Dans le cas de commandes privilégiées, vérifiez si un privilège est affecté dans le mot-clé `defaultpriv`. Cette affectation s'ajoute aux privilèges sur une commande particulière.

**ii. Si aucune affectation d'attribut n'est répertoriée, vérifiez les rôles affectés à l'utilisateur.**

Si l'attribut est affecté à un rôle, l'utilisateur doit endosser le rôle pour obtenir les attributs de sécurité. Si l'attribut est affecté à plusieurs rôles, l'affectation dans le premier rôle de la liste est valide. Si cette valeur est incorrecte, affectez la valeur correcte au premier rôle de la liste ou réorganisez l'affectation de rôle.

**5 Si vous avez assigné un privilège directement à un utilisateur ou un rôle, vérifiez si l'échec d'une commande requiert des autorisations pour s'exécuter correctement.**

---

**Remarque** – Certains aspects de certaines commandes peuvent requérir une autorisation. La pratique recommandée consiste à affecter un profil de droits incluant la commande d'administration, au lieu d'affecter un privilège directement.

---

Passez en revue les profils de droits incluant la commande d'administration. Si un profil de droits incluant les autorisations existe, affectez le profil de droits à l'utilisateur, et pas simplement les privilèges. Placez ce profil de droits devant les autres profils de droits incluant la commande.

**6 Vérifiez les points suivants si une commande continue d'échouer pour un utilisateur.**

**a. Vérifiez que l'utilisateur exécute la commande dans un shell de profil.**

Les commandes d'administration doivent être exécutées dans un shell de profil. Pour réduire les erreurs de l'utilisateur, vous pouvez affecter un shell de profil comme shell de connexion d'utilisateur. Ou bien, vous pouvez rappeler à l'utilisateur d'exécuter les commandes d'administration dans un shell de profil.

**b. Vérifiez si des attributs de sécurité directement affectés à l'utilisateur empêchent la commande de s'exécuter correctement.**

En particulier, vérifiez les valeurs des attributs `defaultpriv` et `limitpriv` de l'utilisateur.

**c. Déterminez le profil de droits ou le rôle qui inclut la commande.**

**i. Dans l'ordre, recherchez la commande avec des attributs de sécurité dans la liste des profils de droits.**

La première valeur dans la liste des profils de droits est la valeur que l'utilisateur peut utiliser. Si cette valeur est incorrecte, modifiez-la dans ce profil de droits, ou réorganisez la liste des profils.

En particulier, vérifiez les valeurs des attributs `defaultpriv` et `limitpriv` du profil.

**ii. Si aucune affectation d'attribut n'est répertoriée, vérifiez les rôles affectés à l'utilisateur.**

Si la commande est affectée à un rôle, l'utilisateur doit endosser le rôle pour obtenir les attributs de sécurité. Si l'attribut est affecté à plusieurs rôles, l'affectation dans le premier rôle de la liste est valide. Si cette valeur est incorrecte, affectez la valeur correcte au premier rôle de la liste ou réorganisez l'affectation de rôle.

**7 Vérifiez les points suivants si une commande échoue pour un rôle.**

Les commandes d'administration nécessitent des privilèges pour s'exécuter correctement. Certains aspects de certaines commandes peuvent requérir une autorisation. La pratique recommandée consiste à affecter un profil de droits incluant la commande d'administration.

**a. Vérifiez si des attributs de sécurité directement affectés au rôle empêchent la commande de s'exécuter correctement.**

En particulier, vérifiez les valeurs des attributs `defaultpriv` et `limitpriv` du rôle.

**b. Dans l'ordre, recherchez la commande avec des attributs de sécurité dans la liste des profils de droits.**

La première valeur dans la liste des profils de droits est la valeur que l'utilisateur peut utiliser. Si cette valeur est incorrecte, modifiez-la dans ce profil de droits, ou réorganisez la liste des profils.

## Gestion de RBAC (tâches)

Une fois que vous avez configuré RBAC et que vous l'utilisez, suivez les procédures suivantes pour tenir à jour et modifier RBAC sur vos systèmes.

### Gestion de RBAC (liste des tâches)

La liste des tâches suivante présente les procédures de gestion du contrôle d'accès basé sur les rôles (RBAC) après son implémentation initiale.



| Tâche                                                                                                   | Description                                                                                                                                                                                     | Voir                                                                                                                           |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Changement du mot de passe d'un rôle.                                                                   | Un utilisateur ou un rôle autorisé modifie le mot de passe d'un autre rôle.                                                                                                                     | “Procédure de modification du mot de passe d'un rôle” à la page 193                                                            |
| Modification des droits affectés à un rôle.                                                             | Modifiez les attributs de sécurité d'un rôle.                                                                                                                                                   | “Procédure de modification des attributs de sécurité d'un rôle” à la page 194<br>Exemple 9–19                                  |
| Modification des droits d'un utilisateur.                                                               | Ajoutez des attributs de sécurité à un utilisateur standard ou les supprimez.                                                                                                                   | “Procédure de modification des propriétés RBAC d'un utilisateur” à la page 196<br>Exemple 9–24<br>Exemple 9–12                 |
| Modification des droits d'un utilisateur dans un profil de droits.                                      | Affectez des valeurs d'attribut de sécurité dans un profil de droits, tels que des indicateurs d'audit, des privilèges par défaut.                                                              | Exemple 9–21<br>Exemple 9–13                                                                                                   |
| Création d'un shell de profil limité.                                                                   | Empêchez les utilisateurs ou les rôles d'avoir un accès total à toutes les commandes dans le logiciel.                                                                                          | “Procédure de limitation d'un administrateur aux droits affectés de manière explicite” à la page 199                           |
| Suppression de droits par défaut d'un système.                                                          | Créez un système pour des utilisations spéciales.                                                                                                                                               | Exemple 9–25                                                                                                                   |
| Limitation des privilèges d'un utilisateur.                                                             | Limitez le jeu de privilèges de base ou limite d'un utilisateur.                                                                                                                                | Exemple 9–21                                                                                                                   |
| Octroi de l'autorisation à un utilisateur de fournir le mot de passe utilisateur pour endosser un rôle. | Modifiez les attributs de sécurité d'un utilisateur pour que le mot de passe utilisateur authentifie l'utilisateur à un rôle. Ce comportement est similaire au comportement des rôles de Linux. | “Procédure d'octroi à un utilisateur de l'autorisation d'utiliser son propre mot de passe pour endosser un rôle” à la page 201 |
| Transformation de root en un utilisateur.                                                               | Avant la désactivation d'un système, transformez le rôle root en un utilisateur.                                                                                                                | “Procédure de modification du rôle root en utilisateur” à la page 202                                                          |

Ces procédures gèrent les attributs de sécurité relatifs aux utilisateurs, aux rôles et aux profils de droits. Pour les procédures de gestion des utilisateurs de base, reportez-vous au [Chapitre 2, “Gestion des comptes utilisateur et des groupes \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

## ▼ Procédure de modification du mot de passe d'un rôle

### Avant de commencer

Vous devez être dans le rôle root.

#### ● Exécutez la commande `passwd`.

```
# passwd [-r naming-service] target-rolename
```

-r *naming-service* Applique la modification de mot de passe au référentiel `files` ou `ldap`. Le référentiel par défaut est `files`. Si vous ne spécifiez pas de référentiel, le mot de passe est modifié dans tous les référentiels.

*target-rolename* Nom d'un rôle existant que vous souhaitez modifier.

Pour obtenir d'autres options de commande, reportez-vous à la page de manuel [passwd\(1\)](#).

### Exemple 9–17 Modification du mot de passe d'un rôle

Dans cet exemple, le rôle `root` modifie le mot de passe du rôle `devmgt` local.

```
# passwd -r files devmgt
New password:      Type new password
Confirm password:  Retype new password
```

Dans cet exemple, le rôle `root` modifie le mot de passe du rôle `devmgt` dans le service d'annuaire LDAP.

```
# passwd -r ldap devmgt
New password:      Type new password
Confirm password:  Retype new password
```

Dans cet exemple, le rôle `root` modifie le mot de passe du rôle `devmgt` dans le fichier et LDAP.

```
# passwd devmgt
New password:      Type new password
Confirm password:  Retype new password
```

## ▼ Procédure de modification des attributs de sécurité d'un rôle

### Avant de commencer

Le profil de droits User Security (sécurité des utilisateurs) doit vous être affecté pour modifier les attributs de sécurité d'un rôle, à l'exception des indicateurs d'audit et du mot de passe pour le rôle. Les propriétés du rôle incluent les profils de droits et les autorisations. Pour affecter des indicateurs d'audit ou modifier le mot de passe d'un rôle, vous devez être dans le rôle `root`.

---

**Remarque** – Pour changer le mot de passe, reportez-vous à la section “[Procédure de modification du mot de passe d'un rôle](#)” à la page 193.

---

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

## 2 Utilisez la commande `rolemod`.

Cette commande modifie les attributs d'un rôle défini dans le service de noms local ou dans LDAP. Les valeurs des options -A, -P et -R peuvent être modifiées par - ou ++. - indique de soustraire la valeur aux valeurs actuellement affectées. ++ indique d'ajouter la valeur aux valeurs actuellement affectées

Pour plus d'informations sur la commande `rolemod`, reportez-vous aux sections suivantes :

- Pour une brève description, reportez-vous à la description de la commande `roleadd` dans la section “[Procédure de création d'un rôle](#)” à la [page 181](#).
- La page de manuel `rolemod(1M)` contient tous les arguments associés à cette commande.
- Pour obtenir la liste des valeurs clé pour l'option -K, reportez-vous à la page de manuel `user_attr(4)`.

La commande suivante remplace les profils de droits affectés au rôle `devmgt` dans le référentiel LDAP :

```
$ rolemod -P "Device Management,File Management" -S ldap devadmin
```

### Exemple 9–18 Modification des attributs de sécurité d'un rôle local

Dans cet exemple, l'administrateur de sécurité modifie le rôle `prtmgt` afin d'inclure le profil de droits VSCAN Management (gestion VSCAN).

```
$ rolemod -c "Handles printers and virus scanning" \
-P "Printer Management,VSCAN Management,All" prtmgt
```

Ces profils de droits sont ajoutés aux profils accordés par l'intermédiaire du fichier `policy.conf`.

### Exemple 9–19 Affectation de privilèges directement à un rôle

Dans cet exemple, l'administrateur de sécurité confie au rôle `sys time` un privilège très spécifique qui affecte le temps système.

```
$ rolemod -K priv=proc_clock_highres sys time
```

Les valeurs pour le mot-clé `priv` se trouvent dans la liste des privilèges dans les processus du rôle à tout moment.

## ▼ Procédure de modification des propriétés RBAC d'un utilisateur

Les propriétés de l'utilisateur comprennent le shell de connexion, les profils de droits et les rôles. La méthode la plus sûre pour accorder des capacités d'administration à un utilisateur est de lui attribuer un rôle. Pour plus de détails, reportez-vous à la section [“Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité”](#) à la page 157.

### Avant de commencer

Le profil de droits User Security (sécurité des utilisateurs) doit vous être affecté pour modifier les attributs de sécurité d'un utilisateur, à l'exception des indicateurs d'audit et du mot de passe pour l'utilisateur. Pour affecter des indicateurs d'audit ou modifier le mot de passe d'un rôle, vous devez être dans le rôle root. Pour modifier d'autres attributs de l'utilisateur, le profil de droits User Management (gestion des utilisateurs) doit vous être affecté.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Utilisez la commande `usermod`.

Cette commande permet de modifier les attributs d'un utilisateur défini dans le service de noms local ou le LDAP. Les arguments RBAC de cette commande sont similaires aux arguments de la commande `useradd`, tel que décrit dans les pages de manuel [user\\_attr\(4\)](#) et indiqué dans l'[Exemple 9–23](#).

Dans l'exemple suivant, un le rôle `devmgt` est affecté à l'utilisateur LDAP. Ce rôle remplace les affectations de rôle précédentes. Le rôle `devmgt` doit exister dans le service de noms LDAP.

```
$ usermod -R devmgt -S ldap jdoe-ldap
```

Dans l'exemple suivant, ce rôle est ajouté aux affectations de rôle précédentes.

```
$ usermod -R +devmgt -S ldap jdoe-ldap
```

### Exemple 9–20 Affectation d'un rôle à un utilisateur local

Dans cet exemple, l'utilisateur `jdoe` peut désormais prendre le rôle d'administrateur système `sysadmin`.

```
$ userattr roles jdoe
secdevice
$ usermod -R secdevice,sysadmin jdoe
$ userattr roles jdoe
secdevice,sysadmin
```

**Exemple 9–21** Suppression de privilèges du jeu limite d'un utilisateur

Dans l'exemple suivant, toutes les sessions dérivées de la connexion initiale de `jdoe` ne peuvent pas utiliser le privilège `sys_linkdir`. C'est-à-dire que l'utilisateur ne peut pas créer de liens physiques vers les répertoires, ni rompre un lien vers des répertoires et ce, même après avoir exécuté la commande `su`.

```
$ usermod -K limitpriv=all,!sys_linkdir jdoe
$ userattr limitpriv jdoe
all,!sys_linkdir
```

**Exemple 9–22** Création d'un utilisateur pouvant gérer DHCP

Dans cet exemple, l'administrateur de sécurité crée un utilisateur dans LDAP. Au moment de la connexion, l'utilisateur `jdoe-dhcp` peut gérer DHCP.

```
# useradd -P "DHCP Management" -s /usr/bin/pfbash -S ldap jdoe-dhcp
```

Dans la mesure où `pfbash` est affecté à l'utilisateur comme shell de connexion, les attributs de sécurité dans le profil de droits DHCP Management (gestion DHCP) sont disponibles pour l'utilisateur dans son shell par défaut.

**Exemple 9–23** Affectation d'autorisations directement à un utilisateur

Dans cet exemple, l'administrateur de sécurité crée un utilisateur local qui peut contrôler la luminosité de l'écran.

```
# useradd -c "Screened JDoe, local" -s /usr/bin/pfbash \
-A solaris.system.power.brightness jdoe-scr
```

Cette autorisation est ajoutée aux affectations d'autorisation existantes de l'utilisateur.

**Exemple 9–24** Affectation de privilèges directement à un utilisateur

Dans cet exemple, l'administrateur de sécurité confie à l'utilisateur `jdoe` un privilège très spécifique qui affecte le temps système.

```
$ usermod -K defaultpriv=basic,proc_clock_highres jdoe
```

Les valeurs pour le mot-clé `defaultpriv` remplacent les valeurs existantes. Par conséquent, pour que l'utilisateur conserve les privilèges `basic`, la valeur `basic` est spécifiée. Dans la configuration par défaut, tous les utilisateurs disposent de privilèges de base.

## ▼ Procédure de limitation d'un utilisateur aux applications de bureau

Vous pouvez restreindre un utilisateur d'Oracle Solaris aux applications de bureau uniquement

### Avant de commencer

Vous devez être dans le rôle root.

#### 1 Attribuez à l'utilisateur un shell de profil comme shell de connexion.

Vous pouvez, par exemple, affecter le shell `pfbash` à l'utilisateur.

```
# usermod -s /usr/bin/pfbash username
```

Tous les processus utilisateur sont maintenant sous le contrôle de RBAC.

#### 2 Créez un profil de droits permettant à un utilisateur d'exécuter les applets de base sur le bureau Oracle.

La commande suivante crée le profil de droits. La commande `end` indique que la commande ajoutée n'exige pas d'attributs de sécurité. Pour créer le profil de droits dans votre référentiel LDAP, utilisez l'option `-S ldap`.

```
# profiles -p "Desktop Applets"
profiles:Desktop Applets> set desc="Can use basic desktop applications"
profiles:Desktop Applets> add cmd=/usr/bin/nautilus;end
profiles:Desktop Applets> add cmd=/usr/bin/dbus-launch;end
profiles:Desktop Applets> add cmd=/usr/lib/dbus-daemon;end
profiles:Desktop Applets> add cmd=/usr/lib/clock-applet;end
profiles:Desktop Applets> add cmd=/usr/lib/gconfd-2;end
profiles:Desktop Applets> add cmd=/usr/lib/gvfsd;end
profiles:Desktop Applets> add cmd=/usr/lib/gvfsd-metadata;end
profiles:Desktop Applets> add cmd=/usr/lib/gvfs-hal-volume-monitor;end
profiles:Desktop Applets> add cmd=/usr/lib/gnome-pty-helper;end
profiles:Desktop Applets> add cmd=/usr/lib/utmp_update;end
profiles:Desktop Applets> add cmd=/usr/bin/sh;end
profiles:Desktop Applets> add cmd=/usr/bin/bash;end
profiles:Desktop Applets> add cmd=/usr/bin/csh;end
profiles:Desktop Applets> add cmd=/usr/bin/ksh;end
profiles:Desktop Applets> commit
profiles:Desktop Applets> exit
```

#### 3 Vérifiez que le profil de droits contient les entrées correctes.

Recherchez les erreurs, tels que les fautes de frappe, les omissions ou les répétitions dans les entrées.

```
# profiles -p "Desktop Applets" info
Found profile in files repository.
name=Desktop Applets
desc=Can use basic desktop applications
cmd=/usr/bin/nautilus
cmd=/usr/bin/dbus-launch
cmd=/usr/lib/dbus-daemon
```

```

cmd=/usr/lib/clock-applet
cmd=/usr/lib/gconfd-2
cmd=/usr/lib/gvfsd
cmd=/usr/lib/gvfsd-metadata
cmd=/usr/lib/gvfsd-trash
cmd=/usr/lib/gvfs-hal-volume-monitor
cmd=/usr/lib/gnome-pty-helper
cmd=/usr/lib/utmp_update
cmd=/usr/bin/sh
cmd=/usr/bin/bash
cmd=/usr/bin/csh
cmd=/usr/bin/ksh

```

---

**Astuce** – Vous pouvez créer un profil de droits pour une application ou une classe d'applications disposant d'icônes de bureau. Ensuite, ajoutez Desktop Applets (applets de bureau) comme profil de droits supplémentaires à ce nouveau profil de droits. Ces deux profils de droits permettent à l'utilisateur d'utiliser les applications de bureau appropriées.

---

#### 4 Affectez le profil de droits Desktop Applets (applets de bureau) et le profil de droits Stop (arrêt) à l'utilisateur.

```
# usermod -P "Desktop Applets,Stop" username
```

Cet utilisateur ne dispose pas des profils de droits Basic Solaris User (utilisateur Solaris de base) et Console User (utilisateur de la console). Par conséquent, seules les commandes dans le profil de droits Desktop Applets (applets de bureau) peuvent être exécutées par cet utilisateur. Par exemple, l'utilisateur n'a pas accès à une fenêtre de terminal.

Pour plus d'informations, reportez-vous aux sections “[Profils de droits](#)” à la page 215, “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la page 217 et “[Limitation d'un utilisateur à des applications de bureau](#)” du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.

La commande `usermod` permet de modifier les attributs d'utilisateur définis dans le service de noms local ou le LDAP. La page de manuel [usermod\(1M\)](#) contient les arguments associés à cette commande.

## ▼ Procédure de limitation d'un administrateur aux droits affectés de manière explicite

Vous pouvez limiter un rôle ou un utilisateur à un nombre restreint d'actions d'administration de deux manières.

- Vous pouvez utiliser le profil de droits Stop (arrêt).

Ce profil constitue le moyen le plus simple de créer un shell limité. Les autorisations et les profils de droits affectés dans le fichier `policy.conf` ne sont pas consultés. Dans la configuration par défaut, le profil de droits Basic Solaris User (utilisateur Solaris de base), le

profil de droits Console User (utilisateur de la console) ou l'autorisation `solaris.device.cdrw` ne sont pas affectés au rôle ou à l'utilisateur.

- Vous pouvez modifier le fichier `policy.conf` sur un système et exiger que le rôle ou l'utilisateur utilisent ce système pour les tâches d'administration.

#### Avant de commencer

Vous devez être dans le rôle `root`.

- **Ajoutez le profil de droits Stop (arrêt) comme dernier profil dans la liste des profils que vous affectez.**

Par exemple, vous pouvez limiter le rôle `auditrev` pour effectuer uniquement des révisions d'audit.

```
# rolemod -P "Audit Review,Stop" auditrev
```

Etant donné que le rôle `auditrev` ne dispose pas du profil de droits Console User (utilisateur de la console), l'auditeur ne peut pas arrêter le système. Etant donné que ce rôle ne dispose pas de l'autorisation `solaris.device.cdrw`, l'auditeur ne peut pas lire ou écrire sur l'unité de CD-ROM. Etant donné que ce rôle ne dispose pas du profil de droits Basic Solaris User (utilisateur Solaris de base), aucune autre commande que les commandes dans le profil de droits Audit Review (vérification de l'audit) ne peut être exécutée dans ce rôle. Par exemple, la commande `ls` ne sera pas exécutée. Le rôle utilise le navigateur de fichiers pour afficher les fichiers d'audit.

Pour plus d'informations, reportez-vous aux sections “[Profils de droits](#)” à la page 215 et “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la page 217.

La commande `rolemod` modifie les attributs d'un rôle défini dans le service de noms local ou le LDAP. La page de manuel [rolemod\(1M\)](#) contient les arguments associés à cette commande. La liste des arguments RBAC est similaire à la liste pour la commande `roleadd`, comme décrit dans la section “[Procédure de création d'un rôle](#)” à la page 181

### Exemple 9–25 Modification d'un système pour limiter les droits disponibles pour ses utilisateurs

Dans cet exemple, l'administrateur crée un système qui n'est utile que pour administrer le réseau. L'administrateur supprime le profil de droits Basic Solaris User (utilisateur Solaris de base) et l'autorisation `solaris.device.cdrw` du fichier `policy.conf`. Le profil de droits Console User (utilisateur de la console) n'est pas supprimé. Les lignes concernées dans le fichier `policy.conf` résultant sont les suivantes :

```
...
#AUTHS_GRANTED=solaris.device.cdrw
#PROFS_GRANTED=Basic Solaris User
CONSOLE_USER=Console User
...
```



Seul un utilisateur auquel des autorisations, commandes ou profils de droits sont explicitement affectés est capable d'utiliser ce système. Après la connexion, l'utilisateur autorisé peut effectuer des tâches d'administration. Si l'utilisateur autorisé se trouve devant le système, il a les droits de l'utilisateur de la console.

## ▼ Procédure d'octroi à un utilisateur de l'autorisation d'utiliser son propre mot de passe pour endosser un rôle

Par défaut, les utilisateurs doivent entrer le mot de passe du rôle pour endosser un rôle. Effectuez cette procédure pour que l'endossement d'un rôle dans Oracle Solaris soit identique à celui dans un environnement Linux.

### Avant de commencer

Vous devez avoir assumé un rôle qui inclut le profil de droits User Security (sécurité des utilisateurs). Ce rôle ne peut pas être le rôle dont vous souhaitez modifier la valeur `roleauth`.

### ● Activez un mot de passe utilisateur pour authentifier un rôle.

```
$ rolemod -K roleauth=user rolename
```

Pour endosser ce rôle, les utilisateurs affectés peuvent désormais utiliser leur propre mot de passe et pas le mot de passe qui a été spécifiquement créé pour le rôle.

### Exemple 9–26 Activation d'un rôle pour utiliser le mot de passe utilisateur affecté lors de l'utilisation d'un profil de droits

Dans cet exemple, le rôle `root` modifie la valeur de `roleauth` pour le rôle `secadmin` sur le système local.

```
# profiles -K roleauth=user "System Administrator"
```

Lorsqu'un utilisateur bénéficiant du profil de droits Security Administrator (administrateur de sécurité) veut endosser le rôle, l'utilisateur est invité à saisir un mot de passe. Dans la séquence suivante, le nom de rôle est `secadmin` :

```
% su - secadmin
Password:      Type user password
$             /** You are now in a profile shell with administrative rights**/
```

Si d'autres rôles ont été affectés à l'utilisateur, celui-ci utilise son propre mot de passe pour ces rôles également.

**Exemple 9–27** Modification de la valeur roleauth pour un rôle dans le référentiel LDAP

Dans cet exemple, le rôle root permet à tous les utilisateurs pouvant endosser le rôle secadmin d'utiliser leur propre mot de passe lorsqu'ils endossent un rôle. Cette capacité est accordée à ces utilisateurs pour tous les systèmes qui sont gérés par le serveur LDAP.

```
# rolemod -S ldap -K roleauth=user secadmin
# profiles -S ldap -K roleauth=user "Security Administrator"
```

**Erreurs fréquentes**

Si roleauth=user est défini pour le rôle, le mot de passe utilisateur permet au rôle authentifié d'accéder à tous les droits affectés à ce rôle. Ce mot-clé dépend de la recherche. Pour plus d'informations, reportez-vous à la section [“Ordre de recherche pour les attributs de sécurité affectés” à la page 217](#).

**▼ Procédure de modification du rôle root en utilisateur**

Un administrateur peut être amené à changer root en utilisateur lors de la mise hors service d'un système qui a été supprimé du réseau. Dans ce cas, la connexion au système en tant que root simplifie le nettoyage.

**Avant de commencer**

Vous devez vous connecter en tant qu'administrateur disposant des profils de droits User Management (gestion des utilisateurs) et User Security (sécurité des utilisateurs).

**1 Supprimez l'affectation du rôle root des utilisateurs locaux.**

Par exemple, supprimez l'affectation du rôle de deux utilisateurs.

```
% su - root
Password: a!2@3#4$5%6^7
# roles jdoe
root
# roles kdoe
root
# roles ldoe
secadmin
# usermod -R "" jdoe
# usermod -R "" kdoe
#
```

**2 Modifiez le rôle root en utilisateur.**

```
# rolemod -K type=normal root
```

Les utilisateurs qui sont actuellement dans le rôle root restent dans le rôle. Les autres utilisateurs disposant d'un accès root peuvent utiliser la commande su pour accéder à root ou se connecter au système en tant qu'utilisateur root.

**3 Vérifiez la modification.**

Vous pouvez utiliser l'une des commandes suivantes.

```
# getent user_attr root
root:::auths=solaris.*;profiles=All;audit_flags=lo\:no;lock_after_retries=no;
min_label=admin_low;clearance=admin_high
```

Si le mot-clé `type` n'est pas présent dans la sortie ou s'il est égal à `normal`, le compte n'est pas un rôle.

```
# userattr type root
```

Si la sortie est vide ou si elle répertorie `normal`, le compte n'est pas un rôle.

**Exemple 9–28 Interdiction de l'utilisation du rôle root pour configurer un système**

Dans cet exemple, la stratégie de sécurité du site requiert que le compte `root` ne puisse pas effectuer la maintenance du système. L'administrateur a créé et testé les rôles qui mettent à jour le système. Ces rôles incluent tous les profils de sécurité et le profil de droits `System Administrator` (administrateur système). Un rôle pouvant restaurer une sauvegarde a été affecté à un utilisateur de confiance. Aucun rôle ne peut modifier les indicateurs d'audit pour le système, un utilisateur ou un profil de droits.

Pour empêcher que le compte `root` soit utilisé pour effectuer la maintenance du système, l'administrateur de sécurité supprime l'affectation du rôle `root`. Dans la mesure où le compte `root` doit être en mesure de se connecter au système en mode monoutilisateur, le compte conserve un mot de passe.

```
# rolemod -K roles= jdoe
# userattr roles jdoe
```

**Exemple 9–29 Transformation de l'utilisateur root en rôle root**

Dans cet exemple, l'utilisateur `root` transforme à nouveau l'utilisateur `root` en un rôle.

Tout d'abord, `root` transforme le compte `root` en un rôle et vérifie la modification.

```
# rolemod -K type=role root
# getent user_attr root
root:::type=role;auths=solaris.*;profiles=All;audit_flags=lo\:no;
lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

Ensuite, `root` affecte le rôle `root` à un utilisateur local.

```
# usermod -R root jdoe
```

**Erreurs  
fréquentes**

Dans un environnement de bureau, vous ne pouvez pas directement vous connecter en tant que root lorsque root est un rôle. Un message de diagnostic indique que root est un rôle sur votre système.

Si vous ne disposez pas d'un compte local pouvant endosser le rôle root, créez-en un. En tant que root, connectez-vous au système en mode monutilisateur, créez un compte utilisateur local et un mot de passe et attribuez le rôle root au nouveau compte. Ensuite, connectez-vous en tant que nouvel utilisateur et endossez le rôle root.

# Utilisation des privilèges (tâches)

Les listes des tâches suivantes dirigent vers des instructions détaillées pour gérer les privilèges et les utiliser sur votre système.

| Tâche                                                         | Description                                                                                                         | Voir                                                                            |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Utilisation de privilèges lors de l'exécution d'une commande. | Implique de dresser la liste des privilèges qui vous ont été affectés et des privilèges disponibles sur le système. | <a href="#">“Détermination des privilèges (liste des tâches)” à la page 204</a> |
| Utilisation de privilèges sur votre site.                     | Comprend l'attribution, la suppression, l'ajout et le débogage de l'utilisation de privilèges.                      | <a href="#">“Gestion des privilèges (liste des tâches)” à la page 209</a>       |

## Détermination des privilèges (liste des tâches)

Lorsqu'un utilisateur se voit affecter directement des privilèges, ces derniers sont appliqués dans chaque shell. Lorsque les privilèges ne lui sont pas directement attribués, l'utilisateur doit ouvrir un shell de profil. Par exemple, lorsque les commandes ayant des privilèges attribués se trouvent dans un profil de droits répertorié dans la liste de profils de droits de l'utilisateur, l'utilisateur doit exécuter la commande dans un shell de profil.

La liste des tâches suivante vous dirige vers les procédures liées à l'affichage des privilèges qui vous ont été attribués.

| Tâche                                                                         | Description                                                                                                     | Voir                                                                                                          |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Affichage des privilèges définis.                                             | Répertoriez les privilèges Oracle Solaris et leurs définitions.                                                 | <a href="#">“Procédure de création d'une liste des privilèges sur le système” à la page 205</a>               |
| Affichage de vos privilèges en tant qu'utilisateur dans n'importe quel shell. | Affichez les privilèges qui vous sont affectés directement. Tous les processus s'exécutent avec ces privilèges. | <a href="#">“Procédure de détermination des privilèges qui vous sont attribués directement” à la page 206</a> |

| Tâche                                                                   | Description                                                                                                           | Voir                                                                                                           |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Affichage de vos commandes privilégiées dans un shell de profil.        | Affichez les commandes privilégiées que vous pouvez exécuter par l'intermédiaire d'un profil de droits affectés.      | <a href="#">“Procédure de détermination des commandes privilégiées que vous pouvez exécuter” à la page 207</a> |
| Affichage de vos privilèges en tant que rôle dans n'importe quel shell. | Affichez les commandes de privilèges que votre rôle peut exécuter par l'intermédiaire d'un profil de droits affectés. | <a href="#">“Procédure de détermination des commandes privilégiées que vous pouvez exécuter” à la page 207</a> |

## ▼ Procédure de création d'une liste des privilèges sur le système

La procédure suivante décrit la procédure d'affichage des noms et définitions de privilèges.

- Dans une fenêtre de terminal, vous pouvez afficher les privilèges en ligne.
  - Création d'une liste des privilèges en affichant la page de manuel [privileges\(5\)](#).

```
% man privileges
Standards, Environments, and Macros           privileges(5)

NAME
    privileges - process privilege model
...
    The defined privileges are:

    PRIV_CONTRACT_EVENT

        Allow a process to request reliable delivery of events
        to an event endpoint.

        Allow a process to include events in the critical event
        set term of a template which could be generated in
        volume by the user.
...

```

Ce format de privilège est utilisé par les développeurs.

- Création d'une liste des privilèges à l'aide de la commande `ppriv`.

```
% ppriv -lv | more
contract_event
    Allows a process to request critical events without limitation.
    Allows a process to request reliable delivery of all events on
    any event queue.
...
win_upgrade_sl
    Allows a process to set the sensitivity label of a window
    resource to a sensitivity label that dominates the existing
    sensitivity label.
    This privilege is interpreted only if the system is configured
    with Trusted Extensions.

```

Ce format de privilège est utilisé pour affecter des privilèges à des utilisateurs et des rôles à l'aide des commandes `useradd`, `roleadd`, `usermod` et `rolemod`, et des profils de droits à l'aide de la commande `profiles`.

## ▼ Procédure de détermination des privilèges qui vous sont attribués directement

La procédure suivante montre comment déterminer si des privilèges vous ont été directement attribués.



**Attention** – L'utilisation inappropriée de privilèges attribués directement peut entraîner des violations involontaires de sécurité. Pour plus de détails, reportez-vous à la section [“Considérations relatives à la sécurité lors de l'affectation directe d'attributs de sécurité”](#) à la page 157.

### 1 Répertoriez les privilèges pouvant être utilisés par vos processus.

Reportez-vous à la section [“Procédure de détermination de privilèges sur un processus”](#) à la page 209 pour connaître la procédure.

### 2 Appelez des actions et exécutez des commandes dans un shell.

Les privilèges répertoriés dans le jeu effectif sont en vigueur dans l'ensemble de votre session. Si des privilèges vous ont été directement attribués en plus du jeu de base, ceux-ci sont répertoriés dans le jeu effectif.

## Exemple 9–30 Détermination des privilèges qui vous sont directement attribués

Si des privilèges vous ont été attribués directement, votre jeu de base contient plus que le jeu de base par défaut. Dans cet exemple, l'utilisateur a toujours accès au privilège `proc_clock_highres`.

```
% /usr/bin/whoami
jdoe
% ppriv -v $$
1800:   pfksh
flags = <none>
E: file_link_any,...,proc_clock_highres,proc_session
I: file_link_any,...,proc_clock_highres,proc_session
P: file_link_any,...,proc_clock_highres,proc_session
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
% ppriv -vl proc_clock_highres
Allows a process to use high resolution timers.
```

**Exemple 9–31 Détermination des privilèges qui sont directement attribués à un rôle**

Les rôles utilisent un shell d'administration ou un shell de profil. Les utilisateurs endossant un rôle peuvent utiliser son shell pour répertorier les privilèges qui lui ont été directement attribués. Dans l'exemple suivant, des privilèges ont été directement attribués au rôle `realtime` pour gérer les programmes de date et d'heure.

```
% su - realtime
Password: <Type realtime password>
$ /usr/bin/whoami
realtime
$ ppriv -v $$
1600: pfksh
flags = <none>
E: file_link_any,...,proc_clock_highres,proc_session,sys_time
I: file_link_any,...,proc_clock_highres,proc_session,sys_time
P: file_link_any,...,proc_clock_highres,proc_session,sys_time
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

## ▼ Procédure de détermination des commandes privilégiées que vous pouvez exécuter

Lorsque les privilèges ne sont pas attribués directement à un utilisateur, celui-ci a accès aux commandes privilégiées par l'intermédiaire d'un profil de droits. Les commandes d'un profil de droits doivent être exécutées dans un shell de profil.

### 1 Déterminez les profils de droits qui vous ont été attribués.

```
% profiles
Audit Review
Console User
Suspend To RAM
Suspend To Disk
Brightness
CPU Power Management
Network Autoconf
Desktop Print Management
Network Wifi Info
Desktop Removable Media User
Basic Solaris User
All
```

### 2 Déterminez vos droits à partir du profil Audit Review (vérification d'audit).

```
profiles -l
Audit Review

solaris.audit.read

/usr/sbin/auditreduce euid=0
```

```
/usr/sbin/auditstat    euid=0
/usr/sbin/praudit      euid=0
```

Le profil de droits Audit Review (vérification d'audit) vous permet d'exécuter les commandes `auditreduce`, `auditstat` et `praudit` avec l'ID utilisateur effectif de 0 et vous attribue l'autorisation `solaris.audit.read`.

### Exemple 9-32 Détermination des commandes privilégiées d'un rôle

Dans cet exemple, un utilisateur endosse un rôle affecté et répertorie les commandes comprises dans l'un des profils de droits.

```
% roles
devadmin
% su - devadmin
Password:      Type devadmin password
$ profiles -l
Device Security
    /usr/bin/kbd          uid=0;gid=sys
    /usr/sbin/add_allocatable euid=0
    /usr/sbin/add_drv      uid=0
    /usr/sbin/devfsadm     uid=0
    /usr/sbin/eeprom       uid=0
    /usr/sbin/list_devices euid=0
    /usr/sbin/rem_drv      uid=0
    /usr/sbin/remove_allocatable euid=0
    /usr/sbin/strace       euid=0
    /usr/sbin/update_drv   uid=0
```

### Exemple 9-33 Exécution de commandes privilégiées dans votre rôle

Dans l'exemple suivant, le rôle `admin` peut modifier les autorisations pour le fichier `useful.script`.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script
chgrp admin useful.script
chgrp: useful.script: Not owner
% su - admin
Password:      <Type admin password>
$ /usr/bin/whoami
admin
$ chgrp admin useful.script
$ chown admin useful.script
$ ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script
```



## Gestion des privilèges (liste des tâches)

Le moyen le plus sûr de gérer les privilèges pour les utilisateurs et les rôles est de limiter leur utilisation aux commandes comprises dans un profil de droits. Le profil de droits est ensuite inclus dans un rôle. Le rôle est attribué à un utilisateur. Lorsque l'utilisateur endosse le rôle affecté, les commandes privilégiées peuvent être exécutées dans un shell de profil. Les procédures ci-dessous décrivent l'attribution des privilèges, la suppression des privilèges et le débogage de l'utilisation de privilèges.

La liste des tâches suivante décrit les procédures pour affecter, supprimer et déboguer des privilèges, et pour exécuter un script contenant des commandes privilégiées.

| Tâche                                                     | Description                                                                                                                                                                                                                                         | Voir                                                                                                    |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Détermination des privilèges dans un processus.           | Dresse la liste des jeux de privilèges effectifs, héréditaires, autorisés et limite pour un processus.                                                                                                                                              | <a href="#">“Procédure de détermination de privilèges sur un processus” à la page 209</a>               |
| Détermination des privilèges manquants dans un processus. | Dresse la liste des privilèges requis par un processus ayant échoué pour s'exécuter correctement.                                                                                                                                                   | <a href="#">“Procédure de détermination des privilèges requis par un programme” à la page 211</a>       |
| Ajout de privilèges à une commande.                       | Ajoute des privilèges à une commande dans un profil de droits. Le profil de droits peut être attribué à des utilisateurs ou des rôles. Les utilisateurs peuvent ensuite exécuter la commande avec les privilèges attribués dans un shell de profil. | <a href="#">Exemple 9–14</a>                                                                            |
| Affectation de privilèges à un utilisateur ou à un rôle.  | Développe le jeu de privilèges héréditaires d'un utilisateur ou d'un rôle. Utilisez cette procédure avec précaution.                                                                                                                                | <a href="#">Exemple 9–24</a>                                                                            |
| Limitation des privilèges d'un utilisateur.               | Limite le jeu de privilèges de base d'un utilisateur. Utilisez cette procédure avec précaution.                                                                                                                                                     | <a href="#">Exemple 9–12</a>                                                                            |
| Exécution d'un script shell privilégié.                   | Ajoute un privilège à un script shell et aux commandes du script shell. Exécute ensuite le script dans un shell de profil.                                                                                                                          | <a href="#">“Procédure d'exécution d'un script shell avec des commandes privilégiées” à la page 213</a> |

### ▼ Procédure de détermination de privilèges sur un processus

Cette procédure présente la détermination des privilèges disponibles pour vos processus. La liste n'inclut pas les privilèges attribués à des commandes particulières.

- **Dresse la liste des privilèges disponibles pour le processus de votre shell.**

```
% ppriv pid
$ ppriv -v pid
```

*pid*      Numéro du processus. Utilisez le symbole double dollar (\$\$) pour transmettre le numéro de processus du shell parent à la commande.

-v      Fournit une liste détaillée des noms des privilèges.

### Exemple 9–34 Détermination des privilèges dans votre shell actuel

Dans l'exemple ci-dessous, les privilèges dans le processus parent du processus de shell de l'utilisateur sont répertoriés. Dans le deuxième exemple, les noms complets des privilèges sont répertoriés. Les lettres dans la sortie font référence aux jeux de privilèges suivants :

E      Jeu de privilèges effectif.  
 I      Jeu de privilèges héritable.  
 P      Jeu de privilèges autorisé.  
 L      Jeu de privilèges de limite.

```
% ppriv $$
1200:  -csh
flags = <none>
      E: basic
      I: basic
      P: basic
      L: all

% ppriv -v $$
1200:  -csh
flags = <none>
      E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

### Exemple 9–35 Détermination des privilèges d'un rôle que vous pouvez prendre

Les rôles utilisent un shell d'administration ou un shell de profil. Vous devez endosser un rôle et utiliser son shell pour répertorier les privilèges qui lui ont été directement attribués. Dans l'exemple suivant, le rôle `sysadmin` n'a pas de privilèges attribués directement.

```
% su - sysadmin
Password:  <Type sysadmin password>
$ /usr/bin/whoami
sysadmin
$ ppriv -v $$
1400:  pfksh
flags = <none>
```

```

E: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
   proc_info,proc_session
I: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
   proc_info,proc_session
P: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
   proc_info,proc_session
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,win_upgrade_sl

```

## ▼ Procédure de détermination des privilèges requis par un programme

Cette procédure détermine les privilèges nécessaires à l'exécution correcte d'une commande ou d'un processus.

### Avant de commencer

La commande ou le processus doit échouer pour que cette procédure de débogage fonctionne.

#### 1 Saisissez la commande ayant échoué en tant qu'argument de la commande de débogage `ppriv`.

```

% ppriv -eD touch /etc/acct/yearly
touch[5245]: missing privilege "file_dac_write"
           (euid = 130, syscall = 224) needed at zfs_zaccess+0x258
touch: cannot create /etc/acct/yearly: Permission denied

```

#### 2 Déterminez l'appel système défaillant en recherchant le numéro `syscall` dans le fichier `/etc/name_to_sysnum`.

```

% grep 224 /etc/name_to_sysnum
creat64                224

```

### Exemple 9–36 Utilisation de la commande `truss` pour examiner l'utilisation des privilèges

La commande `truss` peut déboguer l'utilisation des privilèges dans un shell standard. Par exemple, la commande suivante débogue le processus `touch` défaillant :

```

% truss -t creat touch /etc/acct/yearly
creat64("/etc/acct/yearly", 0666)
           Err#13 EACCES [file_dac_write]
touch: /etc/acct/yearly cannot create

```

Les interfaces `/proc` étendues signalent les privilèges manquants après le code d'erreur dans la sortie `truss`.

**Exemple 9–37** Utilisation de la commande ppriv pour l'examen de l'utilisation des privilèges dans un shell de profil

La commande ppriv peut déboguer l'utilisation des privilèges dans un shell de profil. Si vous attribuez un profil de droits à un utilisateur et que ce profil comprend des commandes avec des privilèges, les commandes doivent être saisies dans un shell de profil. Lorsque les commandes privilégiées sont saisies dans un shell standard, les commandes ne sont pas exécutées avec les privilèges.

Dans cet exemple, l'utilisateur jdoe peut endosser le rôle objadmin. Le rôle objadmin comprend le profil de droits Object Access Management (gestion de l'accès aux objets). Ce profil de droits permet au rôle objadmin de modifier les autorisations pour les fichiers dont objadmin n'est pas propriétaire.

Dans l'exemple ci-dessous, jdoe ne parvient pas à changer les autorisations pour le fichier `useful.script` :

```
jdoe% ls -l useful.script
-rw-r--r-- 1 alooe staff 2303 Apr 10 10:10 useful.script
jdoe% chown objadmin useful.script
chown: useful.script: Not owner
jdoe% ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
(euid = 130, syscall = 16) needed at zfs_zaccess+0x258
chown: useful.script: Not owner
```

Lorsque jdoe endosse le rôle objadmin, les autorisations pour le fichier sont modifiées :

```
jdoe% su - objadmin
Password: <Type objadmin password>
$ ls -l useful.script
-rw-r--r-- 1 alooe staff 2303 Apr 10 10:10 useful.script
$ chown objadmin useful.script
$ ls -l useful.script
-rw-r--r-- 1 objadmin staff 2303 Apr 10 10:10 useful.script
$ chgrp admin useful.script
$ ls -l objadmin.script
-rw-r--r-- 1 objadmin admin 2303 Apr 10 10:11 useful.script
```

**Exemple 9–38** Modification d'un fichier appartenant à l'utilisateur root

Cet exemple illustre les protections contre l'escalade des privilèges. Pour plus de détails, reportez-vous à la section [“Prévention de l'escalade de privilèges” à la page 227](#). Le fichier appartient à l'utilisateur root. Le rôle le moins puissant, objadmin, a besoin de tous les privilèges pour modifier la propriété du fichier, de sorte que l'opération échoue.

```
jdoe% su - objadmin
Password: <Type objadmin password>
```

```
$ cd /etc; ls -l system
-rw-r--r-- 1 root sys 1883 Oct 10 10:20 system
$ chown objadmin system
chown: system: Not owner
$ ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
(euid = 101, syscall = 16) needed at zfs_zaccess+0x258
chown: system: Not owner
```

## ▼ Procédure d'exécution d'un script shell avec des commandes privilégiées

**Remarque** – Lorsque vous créez un script shell exécutant des commandes requérant des privilèges, le profil de droits approprié doit contenir les commandes avec les privilèges qui leur sont attribués.

### Avant de commencer

Vous devez être dans le rôle root.

#### 1 Commencez le script avec `/bin/pfsh`, ou tout autre shell de profil, sur la première ligne.

```
#!/bin/pfsh
# Copyright (c) 2011 by Oracle
```

#### 2 Déterminez les privilèges requis par les commandes du script.

```
% ppriv -eD script-full-path
```

#### 3 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 4 Créez ou modifiez un profil de droits pour le script.

Vous avez besoin d'ajouter le script de shell et les commandes dans le script de shell, avec les attributs de sécurité requis au profil de droits. Pour plus d'informations sur les étapes à suivre, reportez-vous à la section [“Procédure de création ou de modification d'un profil de droits”](#) à la page 186.

#### 5 Ajoutez le profil de droits à un rôle et attribuez le rôle à un utilisateur.

Pour exécuter le script, l'utilisateur endosse le rôle et exécute le script dans le shell de profil du rôle.

- Pour ajouter un profil de droits à un rôle, reportez-vous à la section [“Procédure de modification des attributs de sécurité d'un rôle”](#) à la page 194.

- Pour affecter le rôle à un utilisateur, reportez-vous à l'[Exemple 9–20](#).

## Attributs de sécurité dans Oracle Solaris (référence)

---

Ce chapitre fournit des informations de référence sur le RBAC et les privilèges. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre :

- “Profils de droits” à la page 215
- “Ordre de recherche pour les attributs de sécurité affectés” à la page 217
- “Autorisations” à la page 218
- “Bases de données RBAC” à la page 220
- “Commandes RBAC” à la page 223
- “Commandes d'administration pour la gestion des privilèges” à la page 225
- “Fichiers disposant d'informations sur les privilèges” à la page 226
- “Privilèges et audit” à la page 227
- “Prévention de l'escalade de privilèges” à la page 227
- “Anciennes applications et modèle de privilège” à la page 228

Pour plus d'informations sur l'utilisation de RBAC, reportez-vous au [Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles \(tâches\)”](#). Pour obtenir des informations de présentation, reportez-vous à la section [“Contrôle d'accès basé sur les rôles \(présentation\)”](#) à la page 145.

Pour utiliser les privilèges, reportez-vous à la section [“Utilisation des privilèges \(tâches\)”](#) à la page 204. Pour obtenir des informations sur la présentation, reportez-vous à la section [“Privilèges \(présentation\)”](#) à la page 158.

### Profils de droits

Cette section décrit des profils de droits typiques. Les profils de droits sont des ensembles pratiques comprenant des autorisations et d'autres attributs de sécurité, des commandes avec des attributs de sécurité, et des profils droits supplémentaires. Oracle Solaris fournit de nombreux profils de droits. S'ils ne répondent pas à vos besoins, vous pouvez modifier des profils existants et en créer de nouveaux.

Les profils de droits doivent être affectés dans l'ordre du plus puissant au moins puissant. Pour plus d'informations, reportez-vous à la section [“Ordre de recherche pour les attributs de sécurité affectés”](#) à la page 217.

- **Profil de droits System Administrator (administrateur système)** : fournit un profil pouvant effectuer la plupart des tâches qui ne sont pas en rapport avec la sécurité. Ce profil inclut plusieurs autres profils permettant de créer un rôle puissant. Notez que le profil de droits All (tous) est attribué à la fin de la liste des profils de droits supplémentaires. La commande `profiles` affiche le contenu du profil.

```
% profiles -p "System Administrator" info
```

- **Profil de droits Operator (opérateur)** : fournit des capacités limitées pour gérer des fichiers et des médias hors ligne. Ce profil inclut des profils de droits supplémentaires pour créer un rôle simple. La commande `profiles` affiche le contenu du profil.

```
% profiles -p Operator info
```

- **Profil de droits Printer Management (gestion des imprimantes)** : fournit un nombre limité de commandes et d'autorisations pour la gestion de l'impression. Ce profil est l'un des nombreux profils couvrant une seule partie de l'administration. La commande `profiles` affiche le contenu du profil.

```
% profiles -p "Printer Management" info
```

- **Profil de droits Basic Solaris User (utilisateur Solaris de base)** : permet aux utilisateurs d'utiliser le système dans les limites de la stratégie de sécurité. Ce profil est répertorié par défaut dans le fichier `policy.conf`. Notez que les avantages proposés par le profil de droits de l'utilisateur Solaris de base doivent être contrebalancés avec les exigences en matière de sécurité du site. Les sites nécessitant une sécurité plus stricte préféreront peut-être supprimer ce profil du fichier `policy.conf` ou affecter le profil de droits Stop (arrêt). La commande `profiles` affiche le contenu du profil.

```
% profiles -p "Basic Solaris User" info
```

- **Profil de droits Console User (utilisateur de la console)** : pour les propriétaires de station de travail, ce profil fournit l'accès aux autorisations, commandes et actions à la personne placée devant l'ordinateur. La commande `profiles` affiche le contenu du profil.

```
% profiles -p "Console User" info
```

- **Profil de droits All (tous)** : permet aux rôles d'accéder aux commandes n'ayant pas d'attribut de sécurité. Ce profil peut être approprié pour les utilisateurs ayant des droits limités. La commande `profiles` affiche le contenu du profil.

```
% profiles -p All info
```

- **Profil de droits Stop (arrêt)** : profil de droits spécial qui arrête l'évaluation d'autres profils. Ce profil empêche l'évaluation des variables `AUTHS_GRANTED`, `PROFS_GRANTED` et `CONSOLE_USER` dans le fichier `policy.conf`. Avec ce profil, vous pouvez fournir aux rôles et aux utilisateurs un shell de profil limité.



---

**Remarque** – Le profil de droits Stop affecte de manière indirecte l'affectation de privilèges. Les profils de droits indiqués après le profil de droits Stop (arrêt) ne sont pas évalués. Par conséquent, les commandes avec des privilèges dans ces profils ne sont pas prises en compte. Pour utiliser ce profil, reportez-vous à la section [“Procédure de limitation d'un administrateur aux droits affectés de manière explicite”](#) à la page 199.

---

La commande `profiles` affiche le contenu du profil.

**% profiles -p Stop info**

Chaque profil de droits est associé à un fichier d'aide. Les fichiers d'aide sont au format HTML et sont personnalisables. Les fichiers sont stockés dans le répertoire `/usr/lib/help/profiles/locale/C`.

## Affichage du contenu des profils de droits

Vous disposez de trois vues dans le contenu des profils de droits.

- La commande `getent` vous permet de consulter le contenu de tous les profils de droits sur le système. Pour un exemple de sortie, reportez-vous à la section [“Procédure d'affichage de tous les attributs de sécurité définis”](#) à la page 170.
- La commande `profiles -p "Profile Name" info` vous permet d'afficher le contenu d'un profil de droits spécifique.
- La commande `profiles -l account-name` vous permet de visualiser le contenu des profils de droits qui sont affectés à un utilisateur ou rôle spécifique.

Pour plus d'informations, reportez-vous aux pages de manuel [getent\(1M\)](#) et [profiles\(1\)](#).

## Ordre de recherche pour les attributs de sécurité affectés

Un utilisateur ou un rôle peut se voir affecter des attributs de sécurité directement ou par le biais d'un profil de droits. L'ordre de recherche a une incidence sur la valeur d'attribut de sécurité utilisée. La valeur de la première instance trouvée de l'attribut est utilisée.

---

**Remarque** – L'ordre des autorisations n'est pas important. Les autorisations sont cumulatives.

---

Lorsqu'un utilisateur se connecte, des attributs de sécurité sont affectés dans l'ordre de recherche suivant :

- **attributs de sécurité** affectés à l'utilisateur avec les commandes `useradd` et `usermod`. Pour obtenir la liste, reportez-vous à la section [“Base de données `user\_attr`” à la page 220](#).
- **profils de droits** affectés à l'utilisateur avec les commandes `useradd` et `usermod`. Ces affectations sont recherchées dans l'ordre.

L'ordre est le suivant : premier profil de la liste, puis sa liste de profils de droits, et deuxième profil dans la liste, puis sa liste de profils, et ainsi de suite. La première instance d'une valeur est celle que le système utilise, à l'exception des valeurs `auths` qui sont cumulatives. Les attributs dans des profils de droits incluent tous les attributs de sécurité des utilisateurs, plus les profils supplémentaires. Pour obtenir la liste, reportez-vous à la section [“Base de données `user\_attr`” à la page 220](#).

- Valeur **profil de droits Console User (utilisateur de la console)**. Pour obtenir une description, reportez-vous à la section [“Profils de droits” à la page 215](#).
- Si le **profil de droits Stop (arrêt)** est affecté, l'évaluation des attributs de sécurité s'arrête. Aucun attribut n'est affecté après l'affectation du profil Stop (arrêt). Le profil Stop est évalué après le profil de droits Console User (utilisateur de la console) et avant les autres attributs de sécurité dans le fichier `policy.conf`, y compris `AUTHS_GRANTED`. Pour obtenir une description, reportez-vous à la section [“Profils de droits” à la page 215](#).
- Valeur **Profil de droits Basic Solaris User (utilisateur Solaris de base)** dans le fichier `policy.conf`.
- Valeur `AUTHS_GRANTED` dans le fichier `policy.conf`.
- Valeur `PROFS_GRANTED` dans le fichier `policy.conf`.
- Valeur `PRIV_DEFAULT` dans le fichier `policy.conf`.
- Valeur `PRIV_LIMIT` dans le fichier `policy.conf`.

## Autorisations

Une *autorisation* RBAC est un droit discret qui peut être accordé à un rôle ou à un utilisateur. Les autorisations sont vérifiées par les applications conformes aux normes RBAC avant qu'un utilisateur n'ait accès à l'application ou aux opérations spécifiques au sein de l'application.

Les autorisations sont au niveau de l'utilisateur et sont par conséquent extensibles. Vous pouvez écrire un programme qui requiert une autorisation, ajouter les autorisations à votre système, créer un profil de droits pour ces autorisations et affecter le profil de droits aux rôles ou utilisateurs autorisés à utiliser le programme.

## Conventions de nommage des autorisations

Une autorisation a un nom qui est utilisé en interne. Par exemple, `solaris.system.date` est le nom d'une autorisation. Une autorisation est accompagnée d'une description courte, qui s'affiche dans les interfaces graphiques. Par exemple, `Set Date & Time` est la description de l'autorisation `solaris.system.date`.

Par convention, les noms d'autorisations sont construits dans l'ordre inverse suivant : nom du fournisseur Internet, partie de l'objet, toutes sous-parties et fonction. Les parties du nom d'autorisation sont séparées par des points. Un exemple serait `com.xyzcorp.device.access`. Les exceptions à cette convention sont les autorisations d'Oracle Solaris, lesquelles utilisent le préfixe `solaris` au lieu d'un nom Internet. La convention de nommage permet aux administrateurs d'appliquer des autorisations de manière hiérarchique. Un caractère générique (\*) peut représenter des chaînes à droite d'un point.

## Exemple de granularité d'autorisation

Exemple d'utilisation des autorisations : un utilisateur dans le rôle de sécurité liaison réseau sera limité à l'autorisation `solaris.network.link.security`, tandis que le rôle de sécurité réseau dispose du profil de droits Network Link Security (sécurité liaison réseau) comme profil supplémentaire et des autorisations `solaris.network.*` et `solaris.smf.manage.ssh`.

## Pouvoir de délégation dans les autorisations

Une autorisation se terminant par le suffixe `delegate` permet à un utilisateur ou à un rôle de déléguer à d'autres utilisateurs des autorisations attribuées commençant par le même préfixe.

L'autorisation `solaris.auth.delegate` permet à un utilisateur ou un rôle de déléguer à d'autres utilisateurs des autorisations affectés à ce même utilisateur ou rôle.

Par exemple, un rôle avec les autorisations `solaris.auth.delegate` et `solaris.network.wifi.wep` peut déléguer l'autorisation `solaris.network.wifi.wep` à un autre utilisateur ou rôle. De la même façon, un rôle avec les autorisations `solaris.auth.delegate` et `solaris.network.wifi.wep` peut déléguer l'autorisation `solaris.network.wifi.wep` à un autre utilisateur ou rôle.

## Bases de données RBAC

Les bases de données suivantes stockent les données pour les éléments RBAC :

- **Base de données d'attributs utilisateur étendus** (`user_attr`) : associe des utilisateurs et des rôles à des autorisations, des privilèges, des mots-clés et des profils de droits.
- **Base de données d'attributs de profils de droits** (`prof_attr`) : définit les profils de droits, répertorie les autorisations, privilèges et mots-clés affectés aux profils et identifie le fichier d'aide associé.
- **Base de données d'attributs d'autorisations** (`auth_attr`) : définit les autorisations et leurs attributs, et identifie le fichier d'aide associé.
- **Base de données d'attributs d'exécution** (`exec_attr`) : identifie les commandes portant des attributs de sécurité attribués à des profils de droits spécifiques.

La base de données `policy.conf` contient des autorisations, des privilèges et des profils de droits appliqués à tous les utilisateurs. Pour plus d'informations, reportez-vous à la section [“Fichier `policy.conf`” à la page 222](#).

## Bases de données RBAC et services de noms

Le champ d'application du service de noms des bases de données RBAC est défini dans le service SMF pour le commutateur du service de noms, `svc:/system/name-service/switch`. Les propriétés de ce service pour les bases de données RBAC sont `auth_attr`, `password` et `prof_attr`. La propriété `password` définit la priorité d'un service de noms pour les bases de données `passwd` et `user_attr`. La propriété `prof_attr` définit la priorité d'un service de noms pour les bases de données `prof_attr` et `exec_attr`.

Dans la sortie suivante, les entrées `auth_attr`, `password` et `prof_attr` ne sont pas répertoriées. Par conséquent, les bases de données RBAC utilisent le service de noms `files`.

```
# svccfg -s name-service/switch listprop config
config                                application
config/value_authorization           astring      solaris.smf.value.name-service.switch
config/default                       astring      files
config/host                          astring      "files ldap dns"
config/printer                       astring      "user files ldap"
```

## Base de données `user_attr`

La base de données `user_attr` contient des informations sur l'utilisateur et le rôle qui complètent les bases de données `passwd` et `shadow`.

Les attributs de sécurité suivants peuvent être définis à l'aide des commandes `roleadd`, `rolemod`, `useradd`, `usermod` et `profiles` :

- Dans le cas d'un utilisateur, le mot-clé `roles` affecte un ou plusieurs rôles définis.
- Pour un rôle, la valeur `user` du mot-clé `roleauth` permet au rôle de s'authentifier avec le mot de passe utilisateur plutôt qu'avec le mot de passe du rôle. Par défaut, la valeur est `role`.
- Pour un utilisateur ou un rôle, les attributs suivants peuvent être définis :
  - mot-clé `audit_flags` : modifie le masque d'audit. Pour des références, reportez-vous à la page de manuel [audit\\_flags\(5\)](#).
  - mot-clé `auths` : affecte des autorisations. Pour des références, reportez-vous à la page de manuel [auths\(1\)](#).
  - mot-clé `defaultpriv` : ajoute des privilèges ou en supprime du jeu de privilèges de base par défaut. Pour des références, reportez-vous à la section “[Mise en oeuvre des privilèges](#)” à la page 162.
  - mot-clé `limitpriv` : ajoute des privilèges ou en supprime du jeu limite de privilèges par défaut. Pour des références, reportez-vous à la section “[Mise en oeuvre des privilèges](#)” à la page 162.

Ces privilèges sont toujours en vigueur, ils ne sont pas des attributs d'une commande. Pour des références, reportez-vous à la page de manuel [privileges\(5\)](#) et à la section “[Mise en oeuvre des privilèges](#)” à la page 162.

  - mot-clé `projects` : ajoute un projet par défaut. Pour des références, reportez-vous à la page de manuel [project\(4\)](#).
  - mot-clé `lock_after_retries` : si la valeur est `yes`, le système est verrouillé une fois que le nombre de tentatives a atteint le nombre autorisé dans le fichier `/etc/default/login`.
  - mot-clé `profiles` : affecte des profils de droits.

Pour plus d'informations, reportez-vous à la page de manuel [user\\_attr\(4\)](#). Pour afficher le contenu de cette base de données, utilisez la commande `getent user_attr`. Pour plus d'informations, reportez-vous à la page de manuel [getent\(1M\)](#) et à la section “[Procédure d'affichage de tous les attributs de sécurité définis](#)” à la page 170.

## Base de données `auth_attr`

Toutes les autorisations sont stockées dans la base de données `auth_attr`. Les autorisations peuvent être affectées à des utilisateurs, des rôles ou aux profils de droits. La meilleure méthode consiste à placer les autorisations dans un profil de droits, afin d'inclure le profil dans la liste des profils d'un rôle, puis d'affecter le rôle à un utilisateur.

Pour visualiser le contenu de cette base de données, utilisez la commande `getent prof_attr`. Pour en savoir plus, reportez-vous à la page de manuel [getent\(1M\)](#) et à la section “[Procédure d'affichage de tous les attributs de sécurité définis](#)” à la page 170.

## Base de données `prof_attr`

La base de données `prof_attr` contient le nom, la description, l'emplacement du fichier d'aide, les privilèges et les autorisations qui sont affectés à des profils de droits. Les commandes et les attributs de sécurité qui sont affectés à des profils de droits sont stockés dans la base de données `exec_attr`. Pour plus d'informations, reportez-vous à la section “[Base de données `exec\_attr`](#)” à la page 222.

Pour plus d'informations, reportez-vous à la page de manuel [`prof\_attr\(4\)`](#). Pour visualiser le contenu de cette base de données, utilisez la commande `getent exec_attr`. Pour plus d'informations, reportez-vous à la page de manuel [`getent\(1M\)`](#) et à la section “[Procédure d'affichage de tous les attributs de sécurité définis](#)” à la page 170.

## Base de données `exec_attr`

La base de données `exec_attr` définit les commandes nécessitant des attributs de sécurité pour la réussite de l'opération. Les commandes font partie d'un profil de droits. Une commande avec ses attributs de sécurité peut être exécutée par les rôles ou utilisateurs auxquels le profil est attribué.

Pour plus d'informations, reportez-vous à la page de manuel [`exec\_attr\(4\)`](#). Pour visualiser le contenu de cette base de données, utilisez la commande `getent`. Pour plus d'informations, reportez-vous à la page de manuel [`getent\(1M\)`](#) et à la section “[Procédure d'affichage de tous les attributs de sécurité définis](#)” à la page 170.

## Fichier `policy.conf`

Le fichier `policy.conf` fournit un moyen d'accorder des profils de droits, des autorisations et des privilèges spécifiques à tous les utilisateurs. Les entrées correspondantes dans le fichier sont constitués de paires *key=value* :

- `AUTHS_GRANTED=authorizations` : fait référence à une ou plusieurs autorisations.
- `PROFS_GRANTED=rights profiles` : fait référence à un ou plusieurs profils de droits.
- `CONSOLE_USER=Console User` : fait référence au profil de droits Console User (utilisateur de la console). Ce profil est fourni avec un ensemble pratique d'autorisations pour l'utilisateur de la console. Vous pouvez personnaliser ce profil. Pour afficher le contenu d'un profil, reportez-vous à la section “[Profils de droits](#)” à la page 215.
- `PRIV_DEFAULT=privileges` : fait référence à un ou plusieurs privilèges.
- `PRIV_LIMIT=privileges` : fait référence à tous les privilèges.

L'exemple suivant illustre certaines valeurs typiques issues de la base de données `policy.conf` :

```
# grep AUTHS /etc/security/policy
AUTHS_GRANTED=solaris.device.cdrw

# grep PROFS /etc/security/policy
PROFS_GRANTED=Basic Solaris User

# grep PRIV /etc/security/policy

#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
```

Pour plus d'informations sur les privilèges, reportez-vous à la section “[Privilèges \(présentation\)](#)” à la page 158.

# Commandes RBAC

Cette section répertorie les commandes utilisées pour administrer RBAC. Elle fournit également un tableau des commandes dont l'accès peut être contrôlé par des autorisations.

## Commandes pour la gestion de RBAC

Les commandes suivantes récupèrent et définissent les informations RBAC.

TABLEAU 10–1 Commandes d'administration RBAC

| Page de manuel pour les commandes | Description                                                                                                                                                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">auths(1)</a>          | Affiche les autorisations d'un utilisateur.                                                                                                                                                                   |
| <a href="#">getent(1M)</a>        | Interface pour répertorier le contenu des bases de données user_attr, prof_attr et exec_attr.                                                                                                                 |
| <a href="#">nscd(1M)</a>          | Name Service Cache Daemon (démon cache de service de noms), utile pour la mise en mémoire cache des bases de données user_attr, prof_attr et exec_attr. Utilisez la commande svcadm pour redémarrer le démon. |
| <a href="#">pam_roles(5)</a>      | Module de gestion des comptes pour les rôles de PAM. Vérifie la présence de l'autorisation pour endosser un rôle.                                                                                             |
| <a href="#">pfexec(1)</a>         | Utilisé par des shells de profil pour exécuter des commandes avec les attributs de sécurité spécifiés dans la base de données exec_attr.                                                                      |
| <a href="#">policy.conf(4)</a>    | Fichier de configuration des stratégies de sécurité du système. Répertorie les autorisations accordées, les privilèges accordés et d'autres informations de sécurité.                                         |
| <a href="#">profiles(1)</a>       | Affiche les profils de droits d'un utilisateur spécifié. Permet de créer ou de modifier un profil de droits sur un système local ou un réseau LDAP.                                                           |
| <a href="#">roles(1)</a>          | Affiche les rôles qu'un utilisateur spécifique peut endosser.                                                                                                                                                 |

TABLEAU 10-1 Commandes d'administration RBAC (Suite)

| Page de manuel pour les commandes | Description                                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>roleadd(1M)</code>          | Ajoute un rôle à un système local ou à un réseau LDAP.                                                                             |
| <code>roleadd(1M)</code>          | Ajoute un rôle à un système local ou à un réseau LDAP.                                                                             |
| <code>rolemod(1M)</code>          | Modifie les propriétés d'un rôle sur un système local ou sur un réseau LDAP.                                                       |
| <code>userattr(1)</code>          | Affiche la valeur d'un droit spécifique qui est affecté à un utilisateur ou à un compte de rôle.                                   |
| <code>useradd(1M)</code>          | Ajoute un compte utilisateur au système ou à un réseau LDAP. L'option <code>-R</code> attribue un rôle au compte d'un utilisateur. |
| <code>userdel(1M)</code>          | Supprime une connexion d'utilisateur du système ou d'un réseau LDAP.                                                               |
| <code>usermod(1M)</code>          | Modifie les propriétés du compte d'un utilisateur sur le système.                                                                  |

## Commandes sélectionnées nécessitant des autorisations

Le tableau suivant fournit des exemples de la façon dont les autorisations sont utilisées pour limiter les options de commande sur un système Oracle Solaris. Pour plus d'informations sur les autorisations, reportez-vous à la section “Autorisations” à la page 218.

TABLEAU 10-2 Commandes et autorisations associées

| Page de manuel pour les commandes | Autorisations requises                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>at(1)</code>                | <code>solaris.jobs.user</code> requise pour toutes les options (lorsque ni les fichiers <code>at.allow</code> ni les fichiers <code>at.deny</code> n'existent)                                                                                                                                                                                                                          |
| <code>atq(1)</code>               | <code>solaris.jobs.admin</code> requise pour toutes les options                                                                                                                                                                                                                                                                                                                         |
| <code>cdwr(1)</code>              | <code>solaris.device.cdwr</code> requise pour toutes les options et accordée par défaut dans le fichier <code>policy.conf</code>                                                                                                                                                                                                                                                        |
| <code>crontab(1)</code>           | <code>solaris.jobs.user</code> requise pour l'option permettant de soumettre une tâche (lorsque ni les fichiers <code>crontab.allow</code> ni les fichiers <code>crontab.deny</code> n'existent)<br><br><code>solaris.jobs.admin</code> requise pour les options permettant de répertorier ou de modifier les fichiers <code>crontab</code> d'autres utilisateurs                       |
| <code>allocate(1)</code>          | <code>solaris.device.allocate</code> (ou toute autre autorisation spécifiée dans le fichier <code>device_allocate</code> ) requise pour attribuer un périphérique<br><br><code>solaris.device.revoke</code> (ou toute autre autorisation spécifiée dans le fichier <code>device_allocate</code> ) requise pour allouer un périphérique à un autre utilisateur (option <code>-F</code> ) |



TABLEAU 10-2 Commandes et autorisations associées (Suite)

| Page de manuel pour les commandes | Autorisations requises                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>deallocate(1)</code>        | <code>solaris.device.allocate</code> (ou toute autre autorisation spécifiée dans le fichier <code>device_allocate</code> ) requise pour libérer un périphérique d'un autre utilisateur<br><br><code>solaris.device.revoke</code> (ou toute autre autorisation spécifiée dans <code>device_allocate</code> ) requise pour forcer la libération du périphérique spécifié (option <code>-F</code> ) ou de tous les périphériques (option <code>-I</code> ) |
| <code>list_devices(1)</code>      | <code>solaris.device.revoke</code> requise pour répertorier les périphériques d'un autre utilisateur (option <code>-U</code> )                                                                                                                                                                                                                                                                                                                          |
| <code>roleadd(1M)</code>          | <code>solaris.user.manage</code> requis pour créer un rôle. <code>solaris.account.activate</code> requis pour définir le mot de passe initial. <code>solaris.account.setpolicy</code> requis pour définir une stratégie de mot de passe, comme le verrouillage de compte et le vieillissement du mot de passe.                                                                                                                                          |
| <code>roledel(1M)</code>          | Autorisation <code>solaris.passwd.assign</code> nécessaire pour supprimer le mot de passe.                                                                                                                                                                                                                                                                                                                                                              |
| <code>rolemod(1M)</code>          | Autorisation <code>solaris.passwd.assign</code> nécessaire pour modifier le mot de passe. <code>solaris.account.setpolicy</code> requis pour modifier une stratégie de mot de passe, comme le verrouillage de compte et le vieillissement du mot de passe.                                                                                                                                                                                              |
| <code>sendmail(1M)</code>         | <code>solaris.mail</code> requise pour accéder aux fonctions de sous-système de messagerie ; <code>solaris.mail.mailq</code> requise pour afficher la file d'attente du courrier                                                                                                                                                                                                                                                                        |
| <code>useradd(1M)</code>          | <code>solaris.user.manage</code> requis pour créer un utilisateur. <code>solaris.account.activate</code> requis pour définir le mot de passe initial. <code>solaris.account.setpolicy</code> requis pour définir une stratégie de mot de passe, comme le verrouillage de compte et le vieillissement du mot de passe.                                                                                                                                   |
| <code>userdel(1M)</code>          | Autorisation <code>solaris.passwd.assign</code> nécessaire pour supprimer le mot de passe.                                                                                                                                                                                                                                                                                                                                                              |
| <code>usermod(1M)</code>          | Autorisation <code>solaris.passwd.assign</code> nécessaire pour modifier le mot de passe. <code>solaris.account.setpolicy</code> requis pour modifier une stratégie de mot de passe, comme le verrouillage de compte et le vieillissement du mot de passe.                                                                                                                                                                                              |

## Privileges

Des privilèges limitant les processus sont mis en oeuvre dans le noyau et peuvent limiter les processus au niveau des commandes, des utilisateurs, des rôles ou du système.

## Commandes d'administration pour la gestion des privilèges

Le tableau suivant répertorie les commandes disponibles pour gérer les privilèges.

TABLEAU 10-3 Commandes pour la gestion des privilèges

| Objectif                                                      | Commande                                 | Page de manuel                   |
|---------------------------------------------------------------|------------------------------------------|----------------------------------|
| Examiner les privilèges de processus                          | <code>ppriv -v pid</code>                | <a href="#">ppriv(1)</a>         |
| Définir les privilèges de processus                           | <code>ppriv -s spec</code>               |                                  |
| Dresser la liste des privilèges du système                    | <code>ppriv -l</code>                    |                                  |
| Répertorier un privilège et sa description                    | <code>ppriv -lv priv</code>              |                                  |
| Déboguer les échecs liés aux privilèges                       | <code>ppriv -eD failed-operation</code>  |                                  |
| Attribuer des privilèges à un nouvel utilisateur              | <code>useradd</code>                     | <a href="#">useradd(1M)</a>      |
| Ajouter des privilèges à un utilisateur existant              | <code>usermod</code>                     | <a href="#">usermod(1M)</a>      |
| Affecter des privilèges à un profil de droits                 | <code>profiles</code>                    | <a href="#">profiles(1)</a>      |
| Affecter des privilèges à un nouveau rôle                     | <code>roleadd</code>                     | <a href="#">roleadd(1M)</a>      |
| Ajouter des privilèges à un rôle existant                     | <code>rolemod</code>                     | <a href="#">rolemod(1M)</a>      |
| Afficher la stratégie de périphériques                        | <code>getdevpolicy</code>                | <a href="#">getdevpolicy(1M)</a> |
| Définir la stratégie de périphériques                         | <code>devfsadm</code>                    | <a href="#">devfsadm(1M)</a>     |
| Mettre à jour la stratégie relative aux périphériques ouverts | <code>update_drv -p policy driver</code> | <a href="#">update_drv(1M)</a>   |
| Ajouter la stratégie de périphériques pour un périphérique    | <code>add_drv -p policy driver</code>    | <a href="#">add_drv(1M)</a>      |

## Fichiers disposant d'informations sur les privilèges

Les fichiers suivants contiennent des informations sur les privilèges.

TABLEAU 10-4 Fichiers contenant des informations sur les privilèges

| Fichier et page de manuel                                                   | Informations sur les privilèges                          | Description                                 |
|-----------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------|
| <a href="#">/etc/security/policy.conf</a><br><a href="#">policy.conf(4)</a> | <code>PRIV_DEFAULT</code>                                | Jeu de privilèges héritable pour le système |
|                                                                             | <code>PRIV_LIMIT</code>                                  | Jeu de privilèges de limite pour le système |
| <a href="#">syslog.conf</a><br><a href="#">syslog.conf(4)</a>               | Fichier journal du système pour les messages de débogage | Journal de débogage des privilèges          |
|                                                                             | Chemin défini dans l'entrée <code>priv.debug</code>      |                                             |

## Privilèges et audit

L'utilisation des privilèges peut être auditée. A chaque fois qu'un processus utilise un privilège, l'utilisation du privilège est enregistrée dans la piste d'audit du jeton d'audit `upriv`. Lorsque les noms de privilèges font partie de l'enregistrement, leur représentation textuelle est utilisée. Les événements d'audit suivants enregistrent l'utilisation de privilèges :

- **AUE\_SETPPRIV (événement d'audit)** : l'événement génère un enregistrement d'audit lorsqu'un jeu de privilèges est modifié. L'événement d'audit `AUE_SETPPRIV` se trouve dans la classe `pm`.
- **AUE\_MODALLOCPRIV (événement d'audit)** : l'événement d'audit génère un enregistrement d'audit lorsqu'un privilège est ajouté depuis l'extérieur du noyau. L'événement d'audit `AUE_MODALLOCPRIV` se trouve dans la classe `ad`.
- **AUE\_MODDEVPLCY (événement d'audit)** : l'événement d'audit génère un enregistrement d'audit lorsque la stratégie liée au périphérique est modifiée. L'événement d'audit `AUE_MODDEVPLCY` se trouve dans la classe `ad`.
- **AUE\_PFEXEC audit event** : l'événement d'audit génère un enregistrement d'audit lorsqu'un appel est effectué à `execve()` avec `pfexec()` activé. L'événement d'audit `AUE_PFEXEC` se trouve dans les classes d'audit `as`, `ex`, `ps` et `ua`. Les noms des privilèges sont inclus dans l'enregistrement d'audit.

L'utilisation réussie de privilèges inclus dans le jeu de base n'est pas auditée. La tentative d'utilisation d'un privilège de base qui a été supprimé du jeu de base d'un utilisateur fait l'objet d'un audit.

## Prévention de l'escalade de privilèges

Le noyau empêche l'*escalade de privilèges*. Une escalade de privilèges se produit lorsqu'un privilège permet à un processus de faire plus que ce à quoi il est autorisé. Pour empêcher qu'un processus acquière plus de privilèges que ceux qui lui sont accordés normalement, les modifications de système vulnérable exigent le jeu complet de privilèges. Par exemple, un fichier ou un processus détenu par `root` (`UID=0`) ne peut être modifié que par un processus ayant le jeu complet de privilèges. Le compte `root` n'a pas besoin de privilèges pour modifier un fichier appartenant à `root`. Toutefois, un utilisateur non `root` doit avoir tous les privilèges pour modifier un fichier appartenant à `root`.

De même, les opérations permettant d'accéder aux périphériques requièrent tous les privilèges du jeu effectif.

Les privilèges `file_chown_self` et `proc_owner` sont soumis à l'escalade de privilèges. Le privilège `file_chown_self` permet à un processus d'abandonner ses fichiers. Le privilège `proc_owner` permet à un processus d'examiner des processus dont il n'est pas propriétaire.

Le privilège `file_chown_self` est limité par la variable système `rstchown`. Lorsque la variable `rstchown` est définie sur zéro, le privilège `file_chown_self` est supprimé du jeu héritable initial du système et de tous les utilisateurs. Pour plus d'informations sur la variable système `rstchown`, reportez-vous à la page de manuel [chown\(1\)](#).

Le privilège `file_chown_self` est attribué, pour des raisons de sécurité, à une commande particulière, placée dans un profil et affectée à un rôle pour l'utiliser dans un shell de profil.

Le privilège `proc_owner` n'est pas suffisant pour définir un processus UID sur 0. Basculer d'un processus de n'importe quel UID à `UID=0` exige tous les privilèges. Etant donné que le privilège `proc_owner` donne un accès illimité en lecture à tous les fichiers sur le système, le privilège est attribué, pour des raisons de sécurité, à une commande particulière, placée dans un profil et affectée à un rôle pour l'utiliser dans un shell de profil.



---

**Attention** – Le compte d'un utilisateur peut être modifié afin d'inclure le privilège `file_chown_self` ou `proc_owner` dans le jeu héritable initial de l'utilisateur. Vous devez avoir des raisons de sécurité de poids pour placer ces privilèges puissants dans le jeu de privilèges héritable pour n'importe quel utilisateur, rôle ou système.

---

Pour plus de détails sur la manière d'empêcher l'escalade de privilèges pour des périphériques, reportez-vous à la section "[Privilèges et périphériques](#)" à la page 166.

## Anciennes applications et modèle de privilège

Pour s'adapter aux anciennes applications, l'implémentation de privilèges fonctionne à la fois avec le superutilisateur et les modèles de privilège. Le noyau suit automatiquement l'indicateur `PRIV_AWARE`, qui indique qu'un programme a été conçu pour fonctionner avec des privilèges. Prenons un processus fils qui n'est pas conscient des privilèges. Les privilèges hérités du processus parent sont disponibles dans les jeux effectif et autorisé de l'enfant. Si le processus fils définit un UID sur 0, le processus fils n'a peut-être pas toutes les capacités de superutilisateur. Les jeux effectif et autorisé du processus sont limités aux privilèges dans le jeu limite de l'enfant. Par conséquent, le jeu limite d'un processus conscient des privilèges restreint les privilèges root des processus fils qui ne sont pas conscients des privilèges.

## PARTIE IV

# Services cryptographiques

Cette section décrit les fonctions centralisées de cryptographie et de technologie à clé publique fournies par Oracle Solaris

- [Chapitre 11, “Structure cryptographique \(présentation\)”](#)
- [Chapitre 12, “Structure cryptographique \(tâches\)”](#)
- [Chapitre 13, “Structure de gestion des clés”](#)



## Structure cryptographique (présentation)

---

Ce chapitre décrit la fonction de structure cryptographique d'Oracle Solaris. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

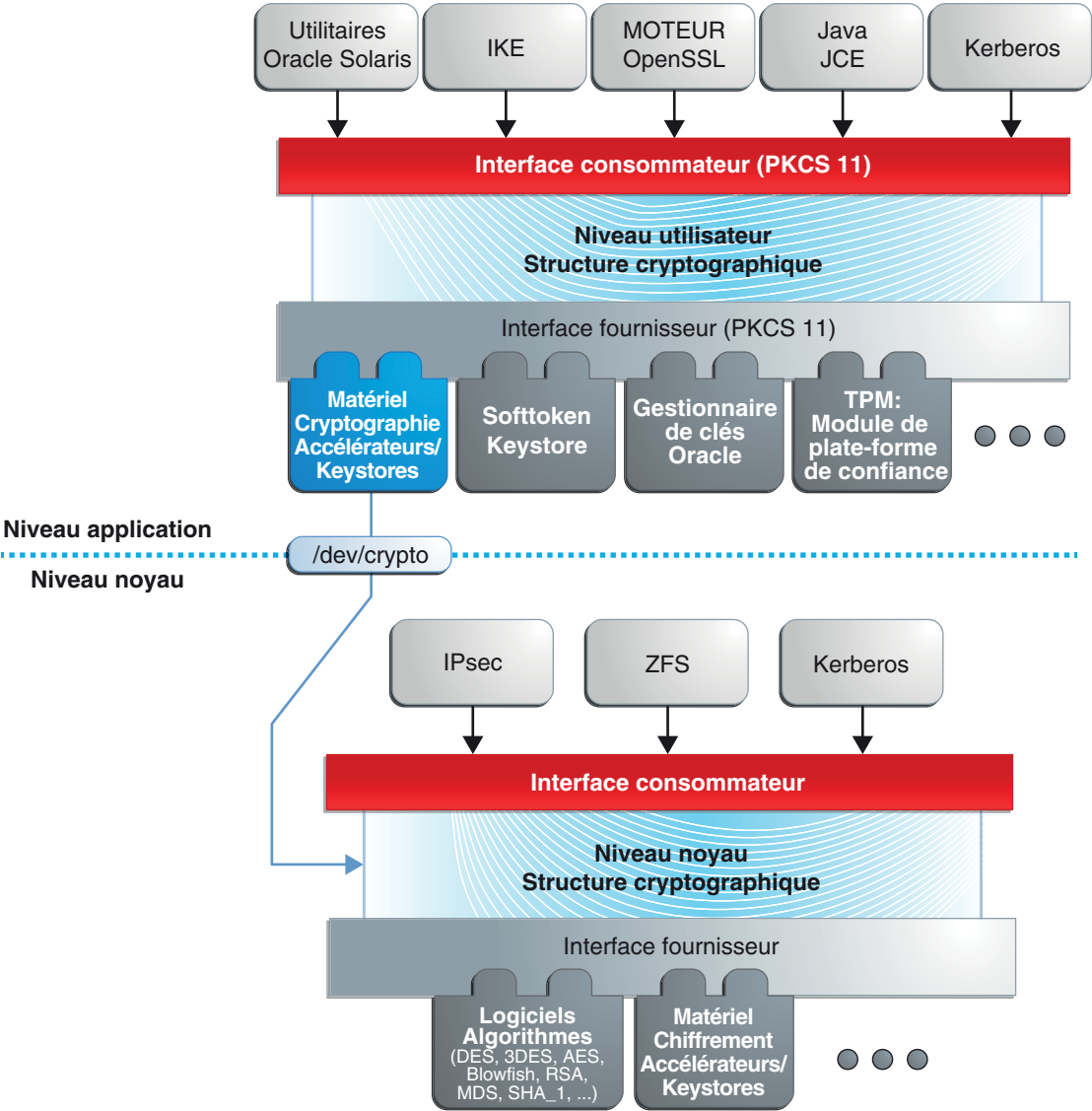
- “Introduction à la structure cryptographique” à la page 231
- “Terminologie utilisée dans la structure cryptographique” à la page 233
- “Champ d'application de la structure cryptographique” à la page 235
- “Commandes d'administration dans la structure cryptographique” à la page 235
- “Commandes au niveau de l'utilisateur dans la structure cryptographique” à la page 236
- “Plug-ins de la structure cryptographique” à la page 237
- “Services cryptographiques et zones” à la page 237

Pour administrer et utiliser la structure cryptographique, reportez-vous au [Chapitre 12](#), “Structure cryptographique (tâches)”.

### Introduction à la structure cryptographique

La structure cryptographique fournit un magasin d'algorithmes et de bibliothèques PKCS #11 commun pour traiter les exigences en matière de cryptographie. Les bibliothèques PKCS #11 sont implémentées conformément au standard suivant : Cryptoki (Cryptographic Token Interface, interface de jetons cryptographiques) pour la bibliothèque PKCS #11 de RSA Security Inc.

FIGURE 11-1 Niveaux de structure cryptographique



Au niveau du noyau, la structure gère actuellement les exigences en matière de cryptographie pour Kerberos et IPsec. Les consommateurs au niveau utilisateur incluent `libsasl` et IKE. Le proxy SSL du noyau (`kssl`) utilise la structure cryptographique. Pour plus d'informations, reportez-vous à la section “Serveurs Web utilisant le protocole SSL (Secure Sockets Layer)” du manuel *Administration d'Oracle Solaris : Services réseau* et à la page de manuel `ksslcfg(1M)`.



La loi sur les exportations aux Etats-Unis exige que l'utilisation des interfaces cryptographiques ouvertes soit restreinte. La structure cryptographique est conforme à la loi en vigueur en exigeant que les fournisseurs cryptographiques du noyau et PKCS 11 s'identifient. Pour plus d'informations, reportez-vous à la section “[Signatures binaires pour les logiciels tiers](#)” à la page 236.

La structure permet aux *fournisseurs* de services cryptographiques de voir leurs services utilisés par de nombreux *consommateurs* dans Oracle Solaris. Les fournisseurs sont également appelés des *plug-ins*. La structure autorise trois types de plug-ins :

- **Plug-ins au niveau de l'utilisateur** : objets partagés qui fournissent des services en utilisant les bibliothèques PKCS #11, telles que `pkcs11_softtoken.so.1`.
- **Plug-ins au niveau du noyau** : modules de noyau qui fournissent l'implémentation d'algorithmes cryptographiques dans les logiciels, tels que [AES](#).

De nombreux algorithmes de la structure sont optimisés pour les architectures x86 avec le jeu d'instructions SSE2 et pour le matériel SPARC.

- **Plug-ins matériels** : pilotes de périphériques et leurs accélérateurs matériels associés. Les puces Niagara, les pilotes de périphériques NCP et N2CP, en sont des exemples. Un accélérateur matériel décharge le système d'exploitation de fonctions cryptographiques coûteuses. La carte Sun Crypto Accelerator 6000 est un exemple.

La structure implémente une interface standard, la bibliothèque PKCS #11, v2.11, pour les fournisseurs au niveau de l'utilisateur. La bibliothèque peut être utilisée par des applications tierces pour atteindre les fournisseurs. Des tiers peuvent également ajouter à la structure des bibliothèques signées, des modules d'algorithme de noyau signés et des pilotes de périphériques signés. Ces plug-ins sont ajoutés lorsque l'utilitaire `pkgadd` installe le logiciel tiers. Pour visualiser un diagramme des principaux composants de la structure, reportez-vous au [Chapitre 8, “Introduction to the Oracle Solaris Cryptographic Framework”](#) du manuel *Developer's Guide to Oracle Solaris 11 Security*.

## Terminologie utilisée dans la structure cryptographique

La liste suivante de définitions et d'exemples est utile lorsque vous utilisez la structure cryptographique.

- **Algorithmes** : algorithmes cryptographiques. Il s'agit de procédures de calcul récursives établies qui chiffrent ou hachent une entrée. Les algorithmes de chiffrement peuvent être symétriques ou asymétriques. Les algorithmes symétriques utilisent la même clé pour le chiffrement et le déchiffrement. Les algorithmes asymétriques, qui sont utilisés dans la cryptographie par clé publique, nécessitent deux clés. Les fonctions de hachage sont également des algorithmes.

Quelques exemples d'algorithmes :

- Algorithmes symétriques, comme AES et ARCFOUR
- Algorithmes asymétriques, comme Diffie-Hellman et RSA
- Fonctions de hachage, comme MD5
- **Consommateurs** : utilisateurs des services cryptographiques provenant de fournisseurs. Les consommateurs peuvent être des applications, des utilisateurs finaux ou des opérations de noyau.

Quelques exemples de consommateurs :

- Applications, comme IKE
- Utilisateurs finaux, comme un utilisateur standard exécutant la commande encrypt
- Opérations de noyau, comme IPsec
- **Mécanisme** : application d'un mode d'algorithme pour un objectif particulier.

Par exemple, un mécanisme DES appliqué à l'authentification, tel que CKM\_DES\_MAC, est un mécanisme distinct d'un mécanisme DES appliqué au chiffrement, CKM\_DES\_CBC\_PAD.

- **Metaslot** : connecteur réunissant les capacités d'autres connecteurs chargés dans la structure. Le metaslot facilite le travail de gestion de toutes les capacités des fournisseurs disponibles par le biais de la structure. Lorsqu'une application utilisant le metaslot demande une opération, le metaslot détermine quel connecteur réel doit effectuer l'opération. Les capacités du metaslot sont configurables, mais la configuration n'est pas nécessaire. Le metaslot est activé par défaut. Pour configurer le metaslot, reportez-vous à la page de manuel [cryptoadm\(1M\)](#).
- **Mode** : version d'un algorithme cryptographique. Par exemple, CBC (Cipher block Chaining, enchaînement des blocs de chiffrement) est un autre mode d'ECB (Electronic Code Book, bloc de contrôle d'événement). L'algorithme AES possède deux modes, CKM\_AES\_ECB et CKM\_AES\_CBC.
- **Stratégie** : choix effectué par un administrateur de rendre des mécanismes disponibles pour l'utilisation. Par défaut, tous les fournisseurs et tous les mécanismes sont disponibles pour l'utilisation. La désactivation de tout mécanisme serait une application de la stratégie. L'activation d'un mécanisme désactivé serait également une application de la stratégie.
- **Fournisseurs** : services cryptographiques utilisés par les consommateurs. Etant donné que les fournisseurs se connectent à la structure, ils sont également qualifiés de *plug-ins*.

Quelques exemples de fournisseurs :

- Bibliothèques PKCS 11, comme pkcs11\_softtoken.so
- Modules d'algorithmes cryptographiques, comme aes et arc four
- Pilotes de périphériques et leurs accélérateurs matériels associés, comme le pilote mca pour la Sun Crypto Accelerator 6000

- **Emplacement** : interface vers un ou plusieurs périphériques cryptographiques. Chaque emplacement, qui correspond à un lecteur physique ou à une autre interface de périphérique, peut contenir un jeton. Un jeton fournit une vue logique d'un périphérique cryptographique dans la structure.
- **Jeton** : dans un connecteur, un jeton fournit une vue logique d'un périphérique cryptographique dans la structure.

## Champ d'application de la structure cryptographique

La structure offre des commandes aux administrateurs, utilisateurs et développeurs qui approvisionnent les fournisseurs :

- **Commandes d'administration** : la commande `cryptoadm` fournit une sous-commande `list` pour répertorier les fournisseurs disponibles et leurs capacités. Les utilisateurs standard peuvent exécuter les commandes `cryptoadm list` et `cryptoadm --help`.

Toutes les autres sous-commandes `cryptoadm` exigent que vous endossiez un rôle incluant le profil de droits Crypto Management (gestion de la cryptographie) ou que vous vous connectiez en tant que superutilisateur. Les sous-commandes telles que `disable`, `install` et `uninstall` sont disponibles pour l'administration de la structure. Pour plus d'informations, reportez-vous à la page de manuel [cryptoadm\(1M\)](#).

La commande `svcadm` est utilisée pour gérer le démon `kcfd` et actualiser la stratégie cryptographique dans le noyau. Pour plus d'informations, reportez-vous à la page de manuel [svcadm\(1M\)](#).

- **Commandes au niveau de l'utilisateur** : les commandes `digest` et `mac` fournissent des services d'intégrité des fichiers. Les commandes `encrypt` et `decrypt` protègent les fichiers des risques d'écoute informatique. Pour utiliser ces commandes, reportez-vous à la section “Protection de fichiers avec la structure cryptographique (liste des tâches)” à la page 240.

## Commandes d'administration dans la structure cryptographique

La commande `cryptoadm` administre une structure cryptographique en cours d'exécution. La commande fait partie du profil de droits Crypto Management (gestion de la cryptographie). Ce profil peut être attribué à un rôle pour l'administration sécurisée de la structure cryptographique. La commande `cryptoadm` gère ce qui suit :

- Affichage des informations du fournisseur cryptographique
- Désactivation ou activation de mécanismes du fournisseur
- Désactivation ou activation du metaslot

La commande `svcadm` est utilisée pour activer, actualiser et désactiver le démon des services cryptographiques, `kcfd`. Cette commande fait partie de l'utilitaire de gestion des services (SMF)

d'Oracle Solaris. `svc:/system/cryptosvcs` est l'instance de service pour la structure cryptographique. Pour plus d'informations, reportez-vous aux pages de manuel [smf\(5\)](#) et [svcadm\(1M\)](#).

## Commandes au niveau de l'utilisateur dans la structure cryptographique

La structure cryptographique fournit des commandes au niveau de l'utilisateur pour vérifier l'intégrité des fichiers et les chiffrer/déchiffrer. Une commande distincte, `elfsign`, permet aux fournisseurs de signer les binaires pour les utiliser avec la structure.

- **digest (commande)** : calcule une [synthèse de message](#) pour un ou plusieurs fichiers ou pour `stdin`. Une synthèse permet de vérifier l'intégrité d'un fichier. [SHA1](#) et [MD5](#) sont des exemples de fonctions digest.
- **mac (commande)** : calcule un [MAC](#) pour un ou plusieurs fichiers ou pour `stdin`. Un code MAC associe des données à un message authentifié. Un MAC permet à un destinataire de vérifier que le message provient de l'expéditeur et qu'il n'a pas été altéré. Les mécanismes `sha1_mac` et `md5_hmac` peuvent calculer un MAC.
- **encrypt (commande)** : chiffre des fichiers ou `stdin` avec un chiffrement symétrique. La commande `encrypt -l` répertorie les algorithmes disponibles. Les mécanismes répertoriés dans une bibliothèque au niveau de l'utilisateur sont disponibles pour la commande `encrypt`. La structure offre les mécanismes AES, DES, 3DES (triple DES) et ARCFOUR pour le chiffrement utilisateur.
- **decrypt (commande)** : déchiffre des fichiers ou `stdin` qui ont été chiffrés avec la commande `encrypt`. La commande `decrypt` utilise les mêmes clé et même mécanisme que ceux utilisés pour chiffrer le fichier d'origine.

## Signatures binaires pour les logiciels tiers

La commande `elfsign` fournit un moyen de signer les fournisseurs à utiliser avec la structure cryptographique. En règle générale, cette commande est exécutée par le développeur d'un fournisseur.

La commande `elfsign` possède des sous-commandes permettant de demander un certificat, signer des binaires et vérifier la signature d'un binaire. Les binaires non signés ne peuvent pas être utilisés par la structure cryptographique. Les fournisseurs qui disposent de binaires signés vérifiables peuvent utiliser la structure.

## Plug-ins de la structure cryptographique

Des tiers peuvent inclure leurs fournisseurs dans la structure cryptographique. Un fournisseur tiers peut être l'un des objets suivants :

- Bibliothèque partagée PKCS #11
- Module de logiciel noyau chargeable, comme un algorithme de chiffrement, la fonction MAC ou la fonction digest
- Pilote de périphérique de noyau pour un accélérateur matériel

Les objets d'un fournisseur doivent être signés avec un certificat d'Oracle. La demande de certificat se base sur une clé privée sélectionnée par le tiers et un certificat fourni par Oracle. La demande de certificat est envoyée à Oracle, qui enregistre le tiers, puis émet le certificat. Le tiers signe ensuite son objet fournisseur à l'aide du certificat Oracle.

Les modules de logiciels noyau chargeables et les pilotes de périphériques de noyau pour les accélérateurs matériels doivent également s'enregistrer dans le noyau. L'enregistrement s'effectue par l'intermédiaire de l'interface du fournisseur de services (SPI) de la structure cryptographique.

## Services cryptographiques et zones

La zone globale et chaque zone non globale possèdent leur propre service `/system/cryptosvc`. Lorsque le service cryptographique est activé ou actualisé dans la zone globale, le démon `kcfd` démarre dans la zone globale, et la stratégie au niveau de l'utilisateur pour la zone globale et la stratégie du noyau pour le système sont définies. Lorsque le service est activé ou actualisé dans une zone non globale, le démon `kcfd` démarre dans la zone et la stratégie au niveau de l'utilisateur pour la zone est définie. La stratégie du noyau a été définie par la zone globale.

Pour plus d'informations sur les zones, reportez-vous à la [Partie II, “Oracle Solaris Zones”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*. Pour plus d'informations sur le SMF qui gère les applications persistantes, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes* et à la page de manuel `smf(5)`.



## Structure cryptographique (tâches)

---

Ce chapitre décrit l'utilisation de la structure cryptographique. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

- [“Utilisation de la structure cryptographique \(liste des tâches\)”](#) à la page 239
- [“Protection des fichiers avec la structure cryptographique \(tâches\)”](#) à la page 240
- [“Administration de la structure cryptographique \(tâches\)”](#) à la page 254

### Utilisation de la structure cryptographique (liste des tâches)

La liste des tâches suivante fait référence à des tâches liées à l'utilisation de la structure cryptographique.

| Tâche                                                      | Description                                                                                                                                                                             | Voir                                                                                                        |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Protection de fichiers individuels ou de jeux de fichiers. | Permet de s'assurer que le contenu du fichier n'a pas été altéré. Empêche les fichiers d'être lus par des intrus. Ces procédures peuvent être effectuées par des utilisateurs standard. | <a href="#">“Protection de fichiers avec la structure cryptographique (liste des tâches)”</a> à la page 240 |
| Administration de la structure.                            | Ajoute, configure et supprime des fournisseurs de logiciels. Désactive et active des mécanismes du fournisseur de matériel. Ces procédures constituent des procédures d'administration. | <a href="#">“Administration de la structure cryptographique (liste des tâches)”</a> à la page 254           |

# Protection des fichiers avec la structure cryptographique (tâches)

Cette section décrit la génération des clés symétriques, la création des sommes de contrôle pour l'intégrité des fichiers et la protection des fichiers contre les risques d'écoute informatique. Les commandes de cette section peuvent être exécutées par des utilisateurs standard. Les développeurs peuvent écrire des scripts qui utilisent ces commandes.

## Protection de fichiers avec la structure cryptographique (liste des tâches)

La structure cryptographique peut vous aider à protéger vos fichiers. La liste des tâches suivante présente les procédures permettant de dresser la liste des algorithmes disponibles et de protéger des fichiers par cryptographie.

| Tâche                                                                       | Description                                                                                                                                     | Voir                                                                                                        |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Génération d'une clé symétrique                                             | Génère une clé aléatoire à utiliser avec des algorithmes spécifiés par l'utilisateur.                                                           | <a href="#">"Procédure de génération d'une clé symétrique à l'aide de la commande dd" à la page 240</a>     |
|                                                                             | Génère une clé de la longueur définie par l'utilisateur. Stocke éventuellement la clé dans un fichier, un keystore PKCS #11 ou un keystore NSS. | <a href="#">"Procédure de génération d'une clé symétrique à l'aide de la commande pktool" à la page 243</a> |
| Calcul d'une somme de contrôle assurant l'intégrité d'un fichier.           | Vérifie que l'exemplaire d'un fichier reçu par le destinataire est identique au fichier qui a été envoyé.                                       | <a href="#">"Procédure de calcul d'une synthèse d'un fichier" à la page 247</a>                             |
| Protection d'un fichier avec un code d'authentification des messages (MAC). | Atteste au destinataire de votre message que vous en êtes l'expéditeur.                                                                         | <a href="#">"Procédure de calcul du code MAC d'un fichier" à la page 248</a>                                |
| Chiffrement d'un fichier, puis déchiffrement du fichier chiffré.            | Protège le contenu d'un fichier en chiffrant le fichier. Fournit les paramètres de chiffrement pour déchiffrer le fichier.                      | <a href="#">"Procédure de chiffrement et déchiffrement d'un fichier" à la page 250</a>                      |

### ▼ Procédure de génération d'une clé symétrique à l'aide de la commande dd

Une clé est nécessaire pour chiffrer les fichiers et générer le MAC d'un fichier. La clé doit provenir d'un pool de nombres aléatoires.



Pour créer la clé, vous avez le choix entre trois options :

- Si votre site possède un générateur de nombres aléatoires, utilisez-le.
- Si vous voulez générer la clé et l'enregistrer, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande `pktool`](#)” à la page 243.
- Dans le cas contraire, utilisez cette procédure. Cette procédure requiert que vous fournissiez la taille de clé en bits. En revanche, la commande `pktool` détermine la taille de la clé appropriée en fonction de l'algorithme que vous indiquez.

## 1 Déterminez la longueur de clé requise par votre algorithme.

### a. Répertoirez les algorithmes disponibles.

```
% encrypt -l
Algorithm      Keysize:  Min   Max (bits)
-----
aes            128    128
arcfour        8      128
des            64     64
3des           192    192

% mac -l
Algorithm      Keysize:  Min   Max (bits)
-----
des_mac        64     64
sha1_hmac      8      512
md5_hmac       8      512
sha256_hmac    8      512
sha384_hmac    8     1024
sha512_hmac    8     1024
```

### b. Déterminez la longueur de clé en octets à transmettre à la commande `dd`.

Divisez les tailles de clé minimale et maximale par 8. Lorsque les tailles de clé minimale et maximale sont différentes, des tailles de clé intermédiaire sont possibles. Par exemple, la valeur 8, 16 ou 64 peut être transmise à la commande `dd` pour les fonctions `sha1_hmac` et `md5_hmac`.

## 2 Générez la clé symétrique.

```
% dd if=/dev/urandom of=keyfile bs=n count=n
```

`if=file`      Fichier d'entrée. Pour une clé aléatoire, utilisez le fichier `/dev/urandom`.

`of=keyfile`    Fichier de sortie contenant la clé générée.

`bs=n`          Taille de clé en octets. Pour obtenir la longueur en octets, divisez la longueur de clé en bits par 8.

`count=n`      Nombre de blocs d'entrée. Le nombre pour `n` doit être 1.

**3 Stockez votre clé dans un répertoire protégé.**

Le fichier de clés ne doit être lisible que par l'utilisateur.

```
% chmod 400 keyfile
```

**Exemple 12-1** Création d'une clé pour l'algorithme AES

Dans l'exemple suivant, une clé secrète pour l'algorithme AES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes AES utilisent une clé de 128 bits. La clé est exprimée en tant que clé de 16 octets dans la commande dd.

```
% ls -al ~/keyf
drwx----- 2 jdoe staff      512 May 3 11:32 ./
% dd if=/dev/urandom of=$HOME/keyf/05.07.aes16 bs=16 count=1
% chmod 400 ~/keyf/05.07.aes16
```

**Exemple 12-2** Création d'une clé pour l'algorithme DES

Dans l'exemple suivant, une clé secrète pour l'algorithme DES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes DES utilisent une clé de 64 bits. La clé est exprimée en tant que clé de 8 octets dans la commande dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.des8 bs=8 count=1
% chmod 400 ~/keyf/05.07.des8
```

**Exemple 12-3** Création d'une clé pour l'algorithme 3DES

Dans l'exemple suivant, une clé secrète pour l'algorithme 3DES est créée. La clé est également stockée pour un déchiffrement ultérieur. Les mécanismes 3DES utilisent une clé de 192 bits. La clé est exprimée en tant que clé de 24 octets dans la commande dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.3des.24 bs=24 count=1
% chmod 400 ~/keyf/05.07.3des.24
```

**Exemple 12-4** Création d'une clé pour l'algorithme MD5

Dans l'exemple suivant, une clé secrète pour l'algorithme MD5 est créée. La clé est également stockée pour un déchiffrement ultérieur. La clé est exprimée en tant que clé de 64 octets dans la commande dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.mack64 bs=64 count=1
% chmod 400 ~/keyf/05.07.mack64
```

## ▼ Procédure de génération d'une clé symétrique à l'aide de la commande `pktool`

Certaines applications exigent une clé symétrique pour le chiffrement et le déchiffrement des communications. Dans cette procédure, vous créez une clé symétrique et la stockez.

- Si votre site dispose d'un générateur de nombres aléatoires, vous pouvez l'utiliser pour créer un nombre aléatoire pour la clé. Cette procédure n'utilise pas le générateur de nombres aléatoires de votre site Web.
- Vous pouvez également utiliser la commande `dd` avec le périphérique `/dev/urandom` en entrée. La commande `dd` ne stocke pas la clé. Pour plus d'informations sur cette procédure, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande `dd`](#)” à la page 240.

### 1 (Facultatif) Si vous prévoyez d'utiliser un keystore, créez-le.

- Pour créer et initialiser un keystore PKCS #11, reportez-vous à la section “[Procédure de génération d'une phrase de passe à l'aide de la commande `pktool setpin`](#)” à la page 277.
- Pour créer et initialiser une base de données NSS, reportez-vous à l'[Exemple 13–5](#).

### 2 Générez un nombre aléatoire pour l'utiliser comme clé symétrique.

Choisissez l'une des méthodes suivantes.

- **Générez une clé et stockez-la dans un fichier.**

L'avantage d'une clé stockée dans un fichier est que vous pouvez extraire la clé de ce fichier pour l'utiliser dans le fichier de clés d'une application, tel que le fichier `/etc/inet/secret/ipseckeys` ou IPsec.

```
% pktool genkey keystore=file outkey=key-fn \
[keytype=generic|specific-symmetric-algorithm] [keylen=size-in-bits] \
[dir=directory] [print=n]
```

**keystore**

La valeur `file` spécifie le type de fichier dans l'emplacement de stockage de la clé.

**outkey=key-fn**

Nom de fichier lorsque `keystore=file`.

**keytype=specific-symmetric-algorithm**

Pour une clé symétrique de n'importe quelle longueur, la valeur est `generic`. Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

**keylen=size-in-bits**

Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour des ou `3des`.

`dir=directory`

Chemin d'accès au répertoire de *key-fn*. Par défaut, *directory* est le répertoire courant.

`print=n`

Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

- **Générez une clé et stockez-la dans un keystore PKCS #11.**

L'avantage du keystore PKCS #11 est que vous pouvez extraire la clé par son étiquette. Cette méthode est utile pour les clés qui chiffrent et déchiffrent des fichiers. Vous devez effectuer l'[Étape 1](#) avant d'utiliser cette méthode.

```
% pktool genkey label=key-label \
[keytype=generic|specific-symmetric-algorithm] [keylen=size-in-bits] \
[token=token] [sensitive=n] [extractable=y] [print=n]
```

`label=key-label`

Étiquette spécifiée par l'utilisateur pour la clé. La clé peut être récupérée à partir du keystore par son étiquette.

`keytype=specific-symmetric-algorithm`

Pour une clé symétrique de n'importe quelle longueur, la valeur est `generic`. Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

`keylen=size-in-bits`

Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour des ou 3des.

`token=token`

Nom du jeton. Par défaut, le jeton est Sun Software PKCS#11 softtoken.

`sensitive=n`

Détermine la sensibilité de la clé. Lorsque la valeur est `y`, la clé ne peut pas être imprimée à l'aide de l'argument `print=y`. Par défaut, la valeur de `sensitive` est `n`.

`extractable=y`

Indique que la clé peut être extraite du keystore. Spécifiez `n` afin d'empêcher l'extraction de la clé.

`print=n`

Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

- **Générez une clé et stockez-la dans un keystore NSS.**

Vous devez effectuer l'[Étape 1](#) avant d'utiliser cette méthode.

```
% pktool keystore=nss genkey label=key-label \
[keytype=[keytype=generic|specific-symmetric-algorithm] [keylen=size-in-bits] [token=token] \
[dir=directory-path] [prefix=database-prefix]
```

`keystore`

La valeur `nss` spécifie le type NSS de l'emplacement de stockage de la clé.

`label=key-label`

Étiquette spécifiée par l'utilisateur pour la clé. La clé peut être récupérée à partir du keystore par son étiquette.

`keytype=specific-symmetric-algorithm`

Pour une clé symétrique de n'importe quelle longueur, la valeur est `generic`. Pour un algorithme particulier, spécifiez `aes`, `arcfour`, `des` ou `3des`.

`keylen=size-in-bits`

Longueur de la clé en bits. Le nombre doit être divisible par 8. *Ne spécifiez rien* pour des ou `3des`.

`token=token`

Nom du jeton. Par défaut, le jeton est le jeton interne NSS.

`dir=directory`

Chemin d'accès au répertoire de la base de données NSS. Par défaut, *directory* est le répertoire courant.

`prefix=directory`

Préfixe de la base de données NSS. Par défaut, le champ de préfixe est vide.

`print=n`

Imprime la clé de la fenêtre de terminal. Par défaut, la valeur de `print` est `n`.

### 3 (Facultatif) Vérifiez que la clé existe.

Utilisez l'une des commandes suivantes, en fonction de l'endroit où vous avez stocké la clé.

- **Vérifiez la clé dans le fichier *key-fn*.**

```
% pktool list keystore=file objtype=key infile=key-fn
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Vérifiez la clé dans le keystore PKCS #11 ou NSS.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

## Exemple 12-5 Création d'une clé symétrique à l'aide de la commande pktool

Dans l'exemple suivant, un utilisateur crée un keystore PKCS#11 pour la première fois, puis génère une longue clé symétrique pour une application. Enfin, l'utilisateur vérifie que la clé se trouve dans le keystore.

```
# pktool setpin
Create new passphrase:    easily-remembered-hard-to-detect-password
Re-enter new passphrase:  Retype password
Passphrase changed.
```

```
% pktool genkey label=specialappkey keytype=generic keylen=1024
Enter PIN for Sun Software PKCS#11 softtoken : Type password

% pktool list objtype=key
Enter PIN for Sun Software PKCS#11 softtoken : Type password

Found 1 keys.
Key #1 - symmetric: specialappkey (1024 bits)
```

### Exemple 12-6 Création d'une clé DES à l'aide de la commande pktool

Dans l'exemple suivant, une clé secrète pour l'algorithme DES est créée. La clé est stockée dans un fichier local pour un déchiffrement ultérieur. La commande protège le fichier avec 400 autorisations. Si la clé est créée, l'option `print=y` affiche la clé générée dans la fenêtre de terminal.

Les mécanismes DES utilisent une clé de 64 bits. L'utilisateur propriétaire du fichier de clés récupère la clé à l'aide de la commande `od`.

```
% pktool genkey keystore=file outkey=64bit.file1 keytype=des print=y
Key Value ="a3237b2c0a8ff9b3"
% od -x 64bit.file1
00000000 a323 7b2c 0a8f f9b3
```

### Exemple 12-7 Création d'une clé symétrique pour les associations de sécurité (SA) IPsec

Dans l'exemple suivant, l'administrateur crée manuellement les numéros de clé pour les SA IPsec et les stocke dans des fichiers. Ensuite, l'administrateur copie les clés pour le fichier `/etc/inet/secret/ipseckeys` et détruit les fichiers d'origine.

- Tout d'abord, l'administrateur crée et affiche les clés requises par la stratégie IPsec :
 

```
# pktool genkey keystore=file outkey=ipencrin1 keytype=generic keylen=192 print=y
Key Value ="294979e512cb8e79370dabecadc3fcb849e78d2d6bd2049"
# pktool genkey keystore=file outkey=ipencrout1 keytype=generic keylen=192 print=y
Key Value ="9678f80e33406c86e3d1686e50406bd0434819c20d09d204"
# pktool genkey keystore=file outkey=ipspi1 keytype=generic keylen=32 print=y
Key Value ="acbeaa20"
# pktool genkey keystore=file outkey=ipspi2 keytype=generic keylen=32 print=y
Key Value ="19174215"
# pktool genkey keystore=file outkey=ipsha21 keytype=generic keylen=256 print=y
Key Value ="659c20f2d6c3f9570bcee93e96d95e2263aca4eeb3369f72c5c786af4177fe9e"
# pktool genkey keystore=file outkey=ipsha22 keytype=generic keylen=256 print=y
Key Value ="b041975a0e1fce0503665c3966684d731fa3dbb12fcf87b0a837b2da5d82c810"
```
- Ensuite, l'administrateur crée le fichier suivant `/etc/inet/secret/ipseckeys` :
 

```
## SPI values require a leading 0x.
## Backslashes indicate command continuation.
##
## for outbound packets on this system
add esp spi 0xacbeaa20 \
```

```

src 192.168.1.1 dst 192.168.2.1 \
encr_alg aes auth_alg sha256 \
encrkey 294979e512cb8e79370dabecadc3fcbb849e78d2d6bd2049 \
authkey 659c20f2d6c3f9570bcee93e96d95e2263aca4eeb3369f72c5c786af4177fe9e
##
## for inbound packets
add esp spi 0x19174215 \
src 192.168.2.1 dst 192.168.1.1 \
encr_alg aes auth_alg sha256 \
encrkey 9678f80e33406c86e3d1686e50406bd0434819c20d09d204 \
authkey b041975a0e1fce0503665c3966684d731fa3dbb12fcf87b0a837b2da5d82c810

```

- Après avoir vérifié que la syntaxe du fichier `ipseckeys` est valide, l'administrateur détruit les fichiers clé d'origine.

```

# ipseckey -c /etc/inet/secret/ipseckeys
# rm ipencrin1 ipencrout1 ipspi1 ipspi2 ipsha21 ipsha22

```

- L'administrateur copie le fichier `ipseckeys` au système de communication en utilisant la commande `ssh` ou un autre mécanisme sécurisé. Sur le système de communication, les protections sont inversées. La première entrée dans le fichier `ipseckeys` protège les paquets entrants, et la seconde entrée protège les paquets sortants. Aucune clé n'est générée sur le système de communication.

## ▼ Procédure de calcul d'une synthèse d'un fichier

Lorsque vous calculez la synthèse d'un fichier, vous pouvez vérifier que le fichier n'a pas été altéré en comparant les résultats de la synthèse. Une synthèse n'altère pas le fichier d'origine.

### 1 Répertoriez les algorithmes de synthèse disponibles.

```

% digest -l
md5
sha1
sha256
sha384
sha512

```

### 2 Calculez la synthèse du fichier et enregistrez la liste des synthèses.

Fournissez un algorithme avec la commande `digest`.

```
% digest -v -a algorithm input-file > digest-listing
```

-v Affiche la sortie au format suivant :

```
algorithm (input-file) = digest
```

-a *algorithm* Algorithme à utiliser pour calculer une synthèse du fichier. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de l'[Étape 1](#).

*input-file* Fichier d'entrée pour la commande `digest`.

*digest-listing* Fichier de sortie pour la commande `digest`.

**Exemple 12-8** Calcul d'une synthèse avec le mécanisme MD5

Dans l'exemple suivant, la commande `digest` utilise le mécanisme MD5 pour calculer la synthèse pour une pièce jointe d'un e-mail.

```
% digest -v -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
md5 (email.attach) = 85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Lorsque l'option `-v` n'est pas utilisée, la synthèse est enregistrée sans informations complémentaires :

```
% digest -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
85c0a53d1a5cc71ea34d9ee7b1b28b01
```

**Exemple 12-9** Calcul d'une synthèse avec le mécanisme SHA1

Dans l'exemple suivant, la commande `digest` utilise le mécanisme SHA1 pour fournir une liste des répertoires. Les résultats sont placés dans un fichier.

```
% digest -v -a sha1 docs/* > $HOME/digest.docs.legal.05.07
% more ~/digest.docs.legal.05.07
sha1 (docs/legal1) = 1df50e8ad219e34f0b911e097b7b588e31f9b435
sha1 (docs/legal2) = 68efa5a636291bde8f33e046eb33508c94842c38
sha1 (docs/legal3) = 085d991238d61bd0cfa2946c183be8e32cccf6c9
sha1 (docs/legal4) = f3085eae7e2c8d008816564fdf28027d10e1d983
```

▼ **Procédure de calcul du code MAC d'un fichier**

Un code d'authentification des messages, ou MAC, calcule la synthèse pour le fichier et utilise une clé secrète pour protéger davantage cette synthèse. Un code MAC n'altère pas le fichier d'origine.

**1** Répertoriez les mécanismes disponibles.

```
% mac -l
Algorithm      Keysize:  Min    Max
-----
des_mac                64     64
sha1_hmac              8    512
md5_hmac               8    512
sha256_hmac            8    512
sha384_hmac            8   1024
sha512_hmac            8   1024
```

**2** Générez une clé symétrique de la longueur appropriée.

Deux options s'offrent à vous : Vous pouvez fournir une [phrase de passe](#) à partir de laquelle une clé sera générée. Ou vous pouvez fournir une clé.



- Si vous fournissez une phrase de passe, vous devez la stocker ou la mémoriser. Si vous la stockez en ligne, le fichier de la phrase de passe ne doit être lisible que par vous.
- Si vous fournissez une clé, elle doit avoir la taille correcte pour le mécanisme. Pour plus d'informations sur cette procédure, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande dd](#)” à la page 240. Vous pouvez également exécuter la commande `pktool`. Pour plus d'informations sur cette procédure et des exemples, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande pktool](#)” à la page 243.

### 3 Créez un MAC pour un fichier.

Fournissez une clé et utilisez un algorithme de clé symétrique avec la commande `mac`.

```
% mac [-v] -a algorithm [-k keyfile | -K key-label [-T token]] input-file
```

-v Affiche la sortie au format suivant :

```
algorithm (input-file) = mac
```

-a *algorithm* Algorithme à utiliser pour calculer le code MAC. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de la commande `mac -l`.

-k *keyfile* Fichier contenant une clé de longueur spécifiée par algorithme.

-K *key-label* Est l'étiquette d'une clé dans le keystore PKCS #11.

-T *token* Est le nom du jeton. Par défaut, le jeton est Sun Software PKCS#11 soft token. Est utilisé uniquement lorsque l'option -K *key-label* est utilisée.

*input-file* Fichier d'entrée pour le MAC.

#### Exemple 12-10 Calcul d'un MAC avec DES\_MAC et une phrase de passe

Dans l'exemple suivant, la pièce jointe d'e-mail est authentifiée avec le mécanisme DES\_MAC et une clé dérivée d'une phrase de passe. La liste MAC est enregistrée dans un fichier. Si la phrase de passe est stockée dans un fichier, celui-ci doit être lisible uniquement par l'utilisateur.

```
% mac -v -a des_mac email.attach
Enter passphrase: <Type passphrase>
des_mac (email.attach) = dd27870a
% echo "des_mac (email.attach) = dd27870a" >> ~/desmac.daily.05.07
```

#### Exemple 12-11 Calcul d'un MAC avec MD5\_HMAC et un fichier de clés

Dans l'exemple suivant, la pièce jointe d'e-mail est authentifiée avec le mécanisme MD5\_HMAC et une clé secrète. La liste MAC est enregistrée dans un fichier.

```
% mac -v -a md5_hmac -k $HOME/keyf/05.07.mack64 email.attach
md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c
```

```
% echo "md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c" \
>> ~/mac.daily.05.07
```

### Exemple 12-12 Calcul d'un MAC avec SHA1\_HMAC et un fichier de clés

Dans l'exemple suivant, le manifeste de répertoire est authentifié avec le mécanisme SHA1\_HMAC et une clé secrète. Les résultats sont placés dans un fichier.

```
% mac -v -a sha1_hmac \
-k $HOME/keyf/05.07.mack64 docs/* > $HOME/mac.docs.legal.05.07
% more ~/mac.docs.legal.05.07
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

### Exemple 12-13 Calcul d'un MAC avec SHA1\_HMAC et une étiquette de clés

Dans l'exemple suivant, le manifeste de répertoire est authentifié avec le mécanisme SHA1\_HMAC et une clé secrète. Les résultats sont placés dans le keystore PKCS #11 de l'utilisateur. L'utilisateur a initialement créé le keystore et le mot de passe pour le keystore à l'aide de la commande `pktool setpin`.

```
% mac -a sha1_hmac -K legaldocs0507 docs/*
Enter pin for Sun Software PKCS#11 softtoken: Type password
```

Pour récupérer le MAC à partir du keystore, l'utilisateur se sert des informations détaillées et fournit l'étiquette clé et le nom du répertoire qui a été authentifié.

```
% mac -v -a sha1_hmac -K legaldocs0507 docs/*
Enter pin for Sun Software PKCS#11 softtoken: Type password
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

## ▼ Procédure de chiffrement et déchiffrement d'un fichier

Lorsque vous chiffrez un fichier, le fichier d'origine n'est ni supprimé, ni modifié. Le fichier de sortie est chiffré.

Pour trouver des solutions aux erreurs courantes générées par la commande `encrypt`, reportez-vous à la section suivant les exemples.

## 1 Créez une clé symétrique de la longueur appropriée.

Deux options s'offrent à vous. Vous pouvez fournir une [phrase de passe](#) à partir de laquelle une clé sera générée. Ou vous pouvez fournir une clé.

- Si vous fournissez une phrase de passe, vous devez stocker ou mémoriser la phrase de passe. Si vous la stockez en ligne, le fichier de la phrase de passe ne doit être lisible que par vous.
- Si vous fournissez une clé, elle doit avoir la taille correcte pour le mécanisme. Pour plus d'informations sur cette procédure, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande dd](#)” à la page 240. Vous pouvez également exécuter la commande `pktool`. Pour plus d'informations sur cette procédure et des exemples, reportez-vous à la section “[Procédure de génération d'une clé symétrique à l'aide de la commande pktool](#)” à la page 243.

## 2 Chiffrez un fichier.

Fournissez une clé et utilisez un algorithme de clé symétrique avec la commande `encrypt`.

```
% encrypt -a algorithm [-v] \
[-k keyfile | -K key-label [-T token]] [-i input-file] [-o output-file]
```

- |                              |                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-a <i>algorithm</i></b>   | Algorithme à utiliser pour chiffrer le fichier. Saisissez l'algorithme lorsqu'il s'affiche dans la sortie de la commande <code>encrypt -l</code> .                                             |
| <b>-k <i>keyfile</i></b>     | Fichier contenant une clé de longueur spécifiée par algorithme. La longueur de la clé pour chaque algorithme est répertoriée, en bits, dans la sortie de la commande <code>encrypt -l</code> . |
| <b>-K <i>key-label</i></b>   | Etiquette d'une clé dans le keystore PKCS #11.                                                                                                                                                 |
| <b>-T <i>token</i></b>       | Nom du jeton. Par défaut, le jeton est <code>Sun Software PKCS#11 softtoken</code> . Est utilisé uniquement lorsque l'option <code>-K <i>key-label</i></code> est utilisée.                    |
| <b>-i <i>input-file</i></b>  | Fichier d'entrée que vous voulez chiffrer. Ce fichier n'est pas modifié par la commande.                                                                                                       |
| <b>-o <i>output-file</i></b> | Fichier de sortie correspondant à la forme chiffrée du fichier d'entrée.                                                                                                                       |

### Exemple 12–14 Création d'une clé AES pour le chiffrement de vos fichiers

Dans l'exemple suivant, un utilisateur crée et stocke une clé AES dans keystore PKCS #11 existant pour l'utilisation lors du chiffrement et du déchiffrement. L'utilisateur peut vérifier que la clé existe et l'utiliser, mais il ne peut pas l'afficher.

```
% pktool genkey label=MyAESkeynumber1 keytype=aes keylen=256
Enter PIN for Sun Software PKCS#11 softtoken :    Type password

% pktool list objtype=key
Enter PIN for Sun Software PKCS#11 softtoken :<Type password>
Found 1 key
```

Key #1 - Sun Software PKCS#11 softtoken: MyAESkeynumber1 (256)

Pour utiliser la clé pour chiffrer un fichier, l'utilisateur le récupère la clé par son étiquette.

```
% encrypt -a aes -K MyAESkeynumber1 -i encryptthisfile -o encryptedthisfile
```

Pour déchiffrer le encryptedthisfile, l'utilisateur récupère la clé par son étiquette.

```
% decrypt -a aes -K MyAESkeynumber1 -i encryptedthisfile -o sameasencryptthisfile
```

### Exemple 12-15 Chiffrement et déchiffrement avec AES et une phrase de passe

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme AES. La clé est générée à partir de la phrase de passe. Si la phrase de passe est stockée dans un fichier, celui-ci doit être lisible uniquement par l'utilisateur.

```
% encrypt -a aes -i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

Enter passphrase: *<Type passphrase>*

Re-enter passphrase: *Type passphrase again*

Le fichier d'entrée, ticket.to.ride, existe toujours sous sa forme d'origine.

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même phrase de passe et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement du fichier.

```
% decrypt -a aes -i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

Enter passphrase: *<Type passphrase>*

### Exemple 12-16 Chiffrement et déchiffrement avec AES et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme AES. Les mécanismes AES utilisent une clé de 128 bits, ou 16 octets.

```
% encrypt -a aes -k ~/keyf/05.07.aes16 \  
-i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

Le fichier d'entrée, ticket.to.ride, existe toujours sous sa forme d'origine.

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a aes -k ~/keyf/05.07.aes16 \  
-i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

**Exemple 12-17** Chiffrement et déchiffrement avec ARCFOUR et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme ARCFOUR. L'algorithme ARCFOUR accepte une clé de 8 bits (1 octet), 64 bits (8 octets) ou 128 bits (16 octets).

```
% encrypt -a arcfour -i personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/enc/e.personal.txt
```

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a arcfour -i ~/enc/e.personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/personal.txt
```

**Exemple 12-18** Chiffrement et déchiffrement avec 3DES et un fichier de clés

Dans l'exemple suivant, un fichier est chiffré avec l'algorithme 3DES. L'algorithme 3DES requiert une clé de 192 bits, ou 24 octets.

```
% encrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/personal2.txt -o ~/enc/e.personal2.txt
```

Pour déchiffrer le fichier de sortie, l'utilisateur utilise la même clé et le même mécanisme de chiffrement que ceux utilisés pour le chiffrement.

```
% decrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/enc/e.personal2.txt -o ~/personal2.txt
```

**Erreurs fréquentes**

Les messages suivants indiquent que la clé que vous avez fournie à la commande `encrypt` n'est pas autorisée par l'algorithme utilisé.

- `encrypt: unable to create key for crypto operation: CKR_ATTRIBUTE_VALUE_INVALID`
- `encrypt: failed to initialize crypto operation: CKR_KEY_SIZE_RANGE`

Si vous transmettez une clé ne répondant pas aux exigences de l'algorithme, vous devez fournir une meilleure clé.

- La première option consiste à utiliser une phrase de passe. La structure fournit ensuite une clé qui remplit les conditions requises.
- La deuxième option consiste à transmettre une taille de clé acceptée par l'algorithme. Par exemple, l'algorithme DES requiert une clé de 64 bits. L'algorithme 3DES requiert une clé de 192 bits.

# Administration de la structure cryptographique (tâches)

Cette section explique l'administration des fournisseurs de logiciels et des fournisseurs de matériel dans la structure cryptographique. L'utilisation de ces fournisseurs peut être empêchée lorsque cela est souhaitable. Par exemple, vous pouvez désactiver l'implémentation d'un algorithme d'un seul fournisseur de logiciels. Ensuite, vous pouvez forcer le système à utiliser l'algorithme d'un autre fournisseur de logiciels.

## Administration de la structure cryptographique (liste des tâches)

La liste des tâches suivante présente les procédures permettant d'administrer les fournisseurs de logiciels et matériels dans la structure cryptographique.

| Tâche                                                                        | Description                                                                                                                                   | Voir                                                                                                                |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Etablissement de la liste des fournisseurs dans la structure cryptographique | Répertoire les algorithmes, les bibliothèques et les périphériques matériels disponibles pour l'utilisation dans la structure cryptographique | <a href="#">“Procédure d’établissement de la liste des fournisseurs disponibles” à la page 255</a>                  |
| Ajout d'un fournisseur de logiciels.                                         | Ajoute une bibliothèque PKCS #11 ou un module de noyau à la structure cryptographique. Le fournisseur doit être signé.                        | <a href="#">“Procédure d'ajout d'un fournisseur de logiciels” à la page 258</a>                                     |
| Interdiction d'utilisation d'un mécanisme au niveau de l'utilisateur.        | Empêche l'utilisation d'un mécanisme logiciel. Le mécanisme peut être activé à nouveau.                                                       | <a href="#">“Procédure d'interdiction de l'utilisation d'un mécanisme au niveau de l'utilisateur” à la page 260</a> |
| Désactivation temporaire des mécanismes d'un module de noyau.                | Empêche temporairement l'utilisation d'un mécanisme. Généralement utilisée à des fins de test.                                                | <a href="#">“Procédure d'interdiction de l'utilisation d'un fournisseur de logiciels noyau” à la page 262</a>       |
| Désinstallation d'un fournisseur.                                            | Empêche l'utilisation d'un fournisseur de logiciels noyau.                                                                                    | <a href="#">Exemple 12–27</a>                                                                                       |
| Etablissement de la liste des fournisseurs de matériel disponibles.          | Affiche le matériel connecté, les mécanismes que le matériel fournit et les mécanismes activés pour utilisation.                              | <a href="#">“Procédure d’établissement de la liste des fournisseurs de matériel” à la page 264</a>                  |
| Désactivation de mécanismes d'un fournisseur de matériel.                    | Permet de s'assurer que les mécanismes sélectionnés sur un accélérateur matériel ne sont pas utilisés.                                        | <a href="#">“Procédure de désactivation des mécanismes et fonctions d'un fournisseur de matériel” à la page 265</a> |
| Redémarrage ou actualisation des services cryptographiques.                  | Permet de s'assurer que les services cryptographiques sont disponibles.                                                                       | <a href="#">“Procédure d'actualisation ou de redémarrage de tous les services cryptographiques” à la page 267</a>   |

## ▼ Procédure d'établissement de la liste des fournisseurs disponibles

La structure cryptographique fournit des algorithmes pour plusieurs types de consommateurs :

- Les fournisseurs au niveau de l'utilisateur offrent une interface de chiffrement PKCS #11 aux applications liées à la bibliothèque `libpkcs11`.
- Les fournisseurs de logiciels noyau offrent des algorithmes pour IPsec, Kerberos et d'autres composants de noyau Oracle Solaris
- Les fournisseurs de matériel noyau offrent des algorithmes disponibles pour les consommateurs de noyau et les applications via la bibliothèque `pkcs11_kernel`.

### 1 Répertoriez les fournisseurs dans un format court.

---

**Remarque** – Le contenu et le format de la liste de fournisseurs varient selon les versions d'Oracle Solaris. Exécutez la commande `cryptoadm list` sur votre système pour afficher les fournisseurs que votre système prend en charge.

---

Seuls les mécanismes au niveau de l'utilisateur sont disponibles pour les utilisateurs standard.

```
% cryptoadm list
User-level providers:
Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
Provider: /usr/lib/security/$ISA/pkcs11_tpm.so
```

```
Kernel software providers:
  des
  aes
  arcfour
  blowfish
  ecc
  sha1
  sha2
  md4
  md5
  rsa
  swrand
```

```
Kernel hardware providers:
  ncp/0
```

### 2 Répertoriez les fournisseurs et leurs mécanismes dans la structure cryptographique.

Tous les mécanismes sont répertoriés dans la sortie suivante. Cependant, certains de ces mécanismes peuvent ne pas être disponibles pour l'utilisation. Pour répertorier uniquement les mécanismes approuvés pour l'utilisation par l'administrateur, reportez-vous à l'[Exemple 12-20](#).

La sortie est tronquée à des fins d'affichage.

```
% cryptoadm list -m
User-level providers:
=====

Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
/usr/lib/security/$ISA/pkcs11_kernel.so: no slots presented.

Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC
CKM_DES_CBC_PAD
CKM_DES_ECB
CKM_DES_KEY_GEN
CKM_DES_MAC_GENERAL
...
CKM_ECDSA_SHA1
CKM_ECDH1_DERIVE

Provider: /usr/lib/security/$ISA/pkcs11_tpm.so
/usr/lib/security/$ISA/pkcs11_tpm.so: no slots presented.

Kernel software providers:
=====
des: CKM_DES_ECB,CKM_DES_CBC,CKM_DES3_ECB,CKM_DES3_CBC
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC
arcfour: CKM_RC4
blowfish: CKM_BLOWFISH_ECB,CKM_BLOWFISH_CBC
ecc: CKM_EC_KEY_PAIR_GEN,CKM_ECDH1_DERIVE,CKM_ECDSA,CKM_ECDSA_SHA1
sha1: CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL
sha2: CKM_SHA256,CKM_SHA256_HMAC,CKM_SHA256_HMAC_GENERAL,CKM_SHA384,CKM_SHA384_HMAC,
CKM_SHA384_HMAC_GENERAL,CKM_SHA512,CKM_SHA512_HMAC,CKM_SHA512_HMAC_GENERAL
md4: CKM_MD4
md5: CKM_MD5,CKM_MD5_HMAC,CKM_MD5_HMAC_GENERAL
rsa: CKM_RSA_PKCS,CKM_RSA_X_509,CKM_MD5_RSA_PKCS,CKM_SHA1_RSA_PKCS,
CKM_SHA256_RSA_PKCS,CKM_SHA384_RSA_PKCS,CKM_SHA512_RSA_PKCS
swrand: No mechanisms presented.

Kernel hardware providers:
=====
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

## Exemple 12-19 Recherche de mécanismes cryptographiques existants

Dans l'exemple suivant, tous les mécanismes offerts par la bibliothèque au niveau de l'utilisateur, `pkcs11_softtoken`, sont répertoriés.

```
% cryptoadm list -m provider=/usr/lib/security/$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC
CKM_DES_CBC_PAD
CKM_DES_ECB
CKM_DES_KEY_GEN
CKM_DES_MAC_GENERAL
```



```
CKM_DES_MAC
...
CKM_ECDSA
CKM_ECDSA_SHA1
CKM_ECDH1_DERIVE
```

### Exemple 12-20 Recherche de mécanismes cryptographiques disponibles

La stratégie détermine les mécanismes utilisables. L'administrateur définit la stratégie. Un administrateur peut choisir de désactiver des mécanismes à partir d'un fournisseur particulier. L'option -p affiche la liste des mécanismes autorisés par la stratégie définie par l'administrateur.

```
% cryptoadm list -p
User-level providers:
=====
/usr/lib/security/$ISA/pkcs11_kernel.so: all mechanisms are enabled.
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_MD5. random is enabled.
/usr/lib/security/$ISA/pkcs11_tpm.so: all mechanisms are enabled.

Kernel software providers:
=====
des: all mechanisms are enabled.
aes: all mechanisms are enabled.
arcfour: all mechanisms are enabled.
blowfish: all mechanisms are enabled.
ecc: all mechanisms are enabled.
sha1: all mechanisms are enabled.
sha2: all mechanisms are enabled.
md4: all mechanisms are enabled.
md5: all mechanisms are enabled.
rsa: all mechanisms are enabled.
swrand: random is enabled.

Kernel hardware providers:
=====
ncp/0: all mechanisms are enabled. random is enabled.
```

### Exemple 12-21 Détermination des fonctions exécutées par les différents mécanismes cryptographiques

Les mécanismes exécutent des fonctions cryptographiques spécifiques, telles que la signature ou la génération de clé. Les options -v -m affichent tous les mécanismes et leurs fonctions.

Dans cet exemple, l'administrateur souhaite déterminer les fonctions pour lesquelles le mécanisme CKM\_ECDSA\* peut être utilisé.

```
% cryptoadm list -vm
User-level providers:
=====

Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
/usr/lib/security/$ISA/pkcs11_kernel.so: no slots presented.
```

```
Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
...
CKM_ECDSA      112 571 . . . . X . X . . . . .
CKM_ECDSA_SHA1 112 571 . . . . X . X . . . . .
...
```

La liste indique que ces mécanismes au niveau de l'utilisateur sont disponibles à partir de la bibliothèque `/usr/lib/security/$ISA/pkcs11_softtoken.so`.

Chaque élément dans une entrée représente un élément d'information sur le mécanisme. Pour ces mécanismes ECC, la liste indique les éléments suivants :

- Longueur minimale : 112 octets
- Longueur maximale : 571 octets
- Matériel : n'est pas disponible sur le matériel.
- Chiffrer : n'est pas utilisé pour chiffrer les données.
- Déchiffrer : n'est pas utilisé pour déchiffrer les données.
- Résumé : n'est pas utilisé pour créer des résumés de message.
- Signer : est utilisé pour signer les données.
- Signer + récupérer : n'est pas utilisé pour signer les données, lorsque les données peuvent être récupérées à partir de la signature.
- Vérifier : est utilisé pour vérifier les données signées.
- Vérifier + récupérer : n'est pas utilisé pour vérifier les données qui peuvent être récupérées à partir de la signature.
- Génération de clé : n'est pas utilisé pour générer une clé privée.
- Génération de paire : n'est pas utilisé pour générer une paire de clés.
- Encapsuler : n'est pas utilisé pour encapsuler c'est-à-dire, chiffrer, une clé existante.
- Désencapsuler : n'est pas utilisé pour désencapsuler une clé encapsulée.
- Dériver : n'est pas utilisé pour dériver une nouvelle clé à partir d'une clé de base.

## ▼ Procédure d'ajout d'un fournisseur de logiciels

### Avant de commencer

Le profil de droits Crypto Management (gestion de la cryptographie) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

**2 Répertoriez les fournisseurs de logiciels disponibles sur le système.**

```
% cryptoadm list
User-level providers:
Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_tpm.so: all mechanisms are enabled.

Kernel software providers:
  des
  aes
  arcfour
  blowfish
  sha1
  sha2
  md4
  md5
  rsa
  swrand

Kernel hardware providers:
  ncp/0
```

**3 Ajoutez le fournisseur à partir d'un référentiel.**

Le logiciel du fournisseur existant a reçu un certificat émis par Oracle.

**4 Actualisez les fournisseurs.**

Vous devez actualiser les fournisseurs si vous avez ajouté un fournisseur de logiciels ou si vous avez ajouté un matériel et spécifié une stratégie pour ce matériel.

```
# svcadm refresh svc:/system/cryptosvc
```

**5 Localisez le nouveau fournisseur dans la liste.**

Dans ce cas, un nouveau fournisseur de logiciels noyau a été installé.

```
# cryptoadm list
...
Kernel software providers:
  des
  aes
  arcfour
  blowfish
  ecc
  sha1
  sha2
  md4
  md5
  rsa
  swrand
  sha3      <-- added provider
...
```

**Exemple 12-22 Ajout d'un fournisseur de logiciels au niveau de l'utilisateur**

Dans l'exemple suivant, une bibliothèque PKCS 11 signée est installée.

```
# pkgadd -d /cdrom/cdrom0/SolarisNew
  Answer the prompts
# svcadm refresh system/cryptosvc
# cryptoadm list
user-level providers:
=====
/usr/lib/security/$ISA/pkcs11_kernel.so
/usr/lib/security/$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_tpm.so
/opt/lib/$ISA/libpkcs11.so.1      <-- added provider
```

Les développeurs qui testent une bibliothèque avec la structure cryptographique peuvent installer la bibliothèque manuellement.

```
# cryptoadm install provider=/opt/lib/$ISA/libpkcs11.so.1
```

## ▼ Procédure d'interdiction de l'utilisation d'un mécanisme au niveau de l'utilisateur

Si certains des mécanismes cryptographiques provenant d'un fournisseur de bibliothèques ne doivent pas être utilisés, vous pouvez supprimer les mécanismes sélectionnés. Cette procédure utilise les mécanismes DES de la bibliothèque `pkcs11_softtoken` comme un exemple.

### Avant de commencer

Le profil de droits Crypto Management (gestion de la cryptographie) doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).
- 2 **Répertoriez les mécanismes offerts par un fournisseur de logiciels particulier au niveau de l'utilisateur.**

```
% cryptoadm list -m provider=/usr/lib/security/$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
```

- 3 **Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p
user-level providers:
=====
...
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
...
```

**4 Désactivez les mécanismes qui ne doivent pas être utilisés.**

```
$ cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB
```

**5 Répertoriez les mécanismes disponibles pour l'utilisation.**

```
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

**Exemple 12–23** Activation d'un mécanisme d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, un mécanisme DES désactivé est de nouveau rendu disponible pour l'utilisation.

```
$ cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_ECB
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_CBC_PAD,CKM_DES_ECB. random is enabled.
```

**Exemple 12–24** Activation de tous les mécanismes d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, tous les mécanismes de la bibliothèque au niveau de l'utilisateur sont activés.

```
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so all
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
```

**Exemple 12–25** Suppression définitive de la disponibilité d'un fournisseur de logiciels au niveau de l'utilisateur

Dans l'exemple suivant, la bibliothèque libpkcs11.so.1 est supprimée.

```
$ cryptoadm uninstall provider=/opt/lib/\$ISA/libpkcs11.so.1
$ cryptoadm list
user-level providers:
  /usr/lib/security/\$ISA/pkcs11_kernel.so
  /usr/lib/security/\$ISA/pkcs11_softtoken.so
  /usr/lib/security/\$ISA/pkcs11_tpm.so
```

```
kernel software providers:
...
```

## ▼ Procédure d'interdiction de l'utilisation d'un fournisseur de logiciels noyau

Si la structure cryptographique fournit plusieurs modes d'un fournisseur tel que AES, vous pouvez supprimer un mécanisme lent ou corrompu. Cette procédure utilise l'algorithme AES comme exemple.

### Avant de commencer

Le profil de droits Crypto Management (gestion de la cryptographie) doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175.](#)
- 2 **Répertoriez les mécanismes qui sont offerts par un fournisseur de logiciels noyau particulier.**  

```
$ cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC
```
- 3 **Répertoriez les mécanismes disponibles pour l'utilisation.**  

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```
- 4 **Désactivez le mécanisme qui ne doit pas être utilisé.**  

```
$ cryptoadm disable provider=aes mechanism=CKM_AES_ECB
```
- 5 **Répertoriez les mécanismes disponibles pour l'utilisation.**  

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
```

### Exemple 12–26 Activation d'un mécanisme d'un fournisseur de logiciels noyau

Dans l'exemple suivant, un mécanisme AES désactivé est de nouveau rendu disponible pour l'utilisation.

```
cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
$ cryptoadm enable provider=aes mechanism=CKM_AES_ECB
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

**Exemple 12–27** Suppression temporaire de la disponibilité d'un fournisseur de logiciels noyau

Dans l'exemple suivant, l'utilisation du fournisseur AES est temporairement rendue impossible. La sous-commande `unload` est utile pour empêcher le chargement automatique d'un fournisseur pendant que le fournisseur est en cours de désinstallation. Par exemple, la sous-commande `unload` peut être utilisée lors de l'installation d'un patch qui affecte le fournisseur.

```
$ cryptoadm unload provider=aes
```

```
$ cryptoadm list
...
Kernel software providers:
  des
  aes (inactive)
  arcfour
  blowfish
  ecc
  sha1
  sha2
  md4
  md5
  rsa
  swrand
```

Le fournisseur AES reste indisponible jusqu'à l'actualisation de la structure cryptographique.

```
$ svcadm refresh system/cryptosvc
```

```
$ cryptoadm list
...
Kernel software providers:
  des
  aes
  arcfour
  blowfish
  ecc
  sha1
  sha2
  md4
  md5
  rsa
  swrand
```

Si un consommateur de noyau utilise le fournisseur de logiciels noyau, le logiciel n'est pas déchargé. Un message d'erreur s'affiche et le fournisseur continue d'être disponible pour l'utilisation.

**Exemple 12–28** Suppression définitive de la disponibilité du fournisseur de logiciels

Dans l'exemple suivant, l'utilisation du fournisseur AES est définitivement rendue impossible. Une fois supprimé, le fournisseur AES n'apparaît plus dans la liste des stratégies des fournisseurs de logiciels noyau.

```
$ cryptoadm uninstall provider=aes
```

```
$ cryptoadm list
```

```
...
```

```
Kernel software providers:
```

```
des
arcfour
blowfish
ecc
sha1
sha2
md4
md5
rsa
swrand
```

Si un consommateur de noyau utilise ce fournisseur de logiciels noyau, un message d'erreur s'affiche et le fournisseur continue d'être disponible pour l'utilisation.

### Exemple 12–29 Réinstallation d'un fournisseur de logiciels noyau supprimé

Dans l'exemple suivant, le fournisseur de logiciels noyau AES est réinstallé.

```
$ cryptoadm install provider=aes \
mechanism=CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC
```

```
$ cryptoadm list
```

```
...
```

```
Kernel software providers:
```

```
des
aes
arcfour
blowfish
ecc
sha1
sha2
md4
md5
rsa
swrand
```

## ▼ Procédure d'établissement de la liste des fournisseurs de matériel

Les fournisseurs de matériel sont automatiquement détectés et chargés. Pour plus d'informations, reportez-vous à la page de manuel [driver.conf\(4\)](#).

### Avant de commencer

Lorsque du matériel doit être utilisé au sein de la structure cryptographique, le matériel s'enregistre sur la SPI dans le noyau. La structure vérifie que le pilote matériel est signé. Plus précisément, la structure vérifie que le fichier d'objet du pilote est signé au moyen d'un certificat émis par Sun.



Par exemple, la carte Sun Crypto Accelerator 6000 (mca), le pilote NCP pour l'accélérateur cryptographique sur les processeurs UltraSPARC T1 et T2 (ncp) et le pilote n2cp pour les processeurs UltraSPARC T2 (n2cp) connectent les mécanismes matériels à la structure.

Pour plus d'informations sur l'obtention de la signature pour votre fournisseur, reportez-vous à la section “[Signatures binaires pour les logiciels tiers](#)” à la page 236.

### 1 Répertoriez les fournisseurs de matériel disponibles sur le système.

```
% cryptoadm list
...
kernel hardware providers:
  ncp/0
```

### 2 Répertoriez les mécanismes fournis par la puce ou la carte.

```
% cryptoadm list -m provider=ncp/0
ncp/0:
CKM_DSA
CKM_RSA_X_509
...
CKM_ECDH1_DERIVE
CKM_ECDSA
```

### 3 Répertoriez les mécanismes disponibles pour l'utilisation sur la puce ou la carte.

```
% cryptoadm list -p provider=ncp/0
ncp/0: all mechanisms are enabled.
```

## ▼ Procédure de désactivation des mécanismes et fonctions d'un fournisseur de matériel

Vous pouvez désactiver de façon sélective des mécanismes et la fonction de nombres aléatoires à partir d'un fournisseur de matériel. Pour les réactiver, reportez-vous à l'[Exemple 12–30](#). Le matériel de cet exemple, la carte Sun Crypto Accelerator 1000, fournit un générateur de nombres aléatoires.

#### Avant de commencer

Le profil de droits Crypto Management (gestion de la cryptographie) doit vous avoir été attribué.

### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

### 2 Choisissez les mécanismes ou la fonction à désactiver.

Répertoriez le fournisseur de matériel.

```
# cryptoadm list
...
```

Kernel hardware providers:  
dca/0

- **Désactivez les mécanismes sélectionnés.**

```
# cryptoadm list -m provider=dca/0
dca/0: CKM_RSA_PKCS, CKM_RSA_X_509, CKM_DSA, CKM_DES_CBC, CKM_DES3_CBC
random is enabled.
# cryptoadm disable provider=dca/0 mechanism=CKM_DES_CBC,CKM_DES3_CBC
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_CBC,CKM_DES3_CBC.
random is enabled.
```

- **Désactivez le générateur de nombres aléatoires.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

- **Désactivez tous les mécanismes. Ne désactivez pas le générateur de nombres aléatoires.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is enabled.
```

- **Désactivez toutes les fonctions et tous les mécanismes sur le matériel.**

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is disabled.
```

### Exemple 12-30 Activation des mécanismes et fonctions sur un fournisseur de matériel

Dans les exemples suivants, les mécanismes désactivés sur un élément matériel sont activés individuellement.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB,CKM_DES3_ECB
.
random is enabled.
# cryptoadm enable provider=dca/0 mechanism=CKM_DES3_ECB
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB.
random is enabled.
```

Dans l'exemple ci-dessous, seul le générateur aléatoire est activé.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
```

```
# cryptoadm enable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is enabled.
```

Dans l'exemple ci-dessous, seuls les mécanismes sont activés. Le générateur aléatoire reste désactivé.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
# cryptoadm enable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

Dans l'exemple suivant, toutes les fonctions et tous les mécanismes de la carte sont activés.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_DES_ECB,CKM_DES3_ECB.
random is disabled.
# cryptoadm enable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
```

## ▼ Procédure d'actualisation ou de redémarrage de tous les services cryptographiques

Par défaut, la structure cryptographique est activée. Lorsque le démon `kcfd` échoue pour une raison quelconque, l'utilitaire de gestion des services peut être utilisé pour redémarrer les services cryptographiques. Pour plus d'informations, reportez-vous aux pages de manuel [smf\(5\)](#) et [svcadm\(1M\)](#). Pour connaître l'effet du redémarrage des services cryptographiques sur les zones, reportez-vous à la section “[Services cryptographiques et zones](#)” à la page 237.

### Avant de commencer

Le profil de droits Crypto Management (gestion de la cryptographie) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Vérifiez l'état des services cryptographiques.

```
% svcs cryptosvc
STATE          STIME    FMRI
offline        Dec_09   svc:/system/cryptosvc:default
```

#### 3 Activez les services cryptographiques.

```
# svcadm enable svc:/system/cryptosvc
```

### **Exemple 12-31** Actualisation des services cryptographiques

Dans l'exemple suivant, les services cryptographiques sont actualisés dans la zone globale. Par conséquent, la stratégie de cryptographie au niveau du noyau dans chaque zone non globale est également actualisée.

```
# svcadm refresh system/cryptosvc
```

## Structure de gestion des clés

---

La fonction KMF (Key Management Framework, structure de gestion clé) fournit des outils et interfaces de programmation pour gérer les objets de clé publique. Les objets de clé publique comprennent les certificats X.509 et les paires de clés publiques et privées. Les formats de stockage de ces objets peuvent varier. KMF offre également un outil de gestion des stratégies qui définissent l'utilisation de certificats X.509 par des applications. KMF prend en charge des plug-ins de fournisseurs tiers.

- [“Gestion des technologies à clé publique” à la page 269](#)
- [“Utilitaires de la structure de gestion des clés” à la page 270](#)
- [“Utilisation de la structure de gestion des clés \(tâches\)” à la page 272](#)

### Gestion des technologies à clé publique

La structure de gestion des clés (KMF) fournit une approche unifiée à la gestion des technologies à clé publique (PKI). Oracle Solaris dispose de différentes applications qui utilisent des technologies PKI. Chaque application fournit ses propres interfaces de programmation, mécanismes de stockage des clés et utilitaires d'administration. Si une application offre un mécanisme d'application de stratégie, ce mécanisme s'applique uniquement à l'application correspondante. Avec KMF, les applications utilisent un ensemble unifié d'outils d'administration, un ensemble d'interfaces de programmation et un mécanisme d'application de stratégie. Ces fonctions gèrent les besoins en PKI de toutes les applications adoptant ces interfaces.

KMF unifie la gestion des technologies à clé publique avec les interfaces suivantes :

- **Commande pktool** : cette commande gère les objets PKI, tels que les certificats, dans une variété de keystores.
- **Commande kmfcfg** : cette commande gère la base de données de stratégie PKI et les plug-ins tiers.

Les décisions de stratégie PKI comprennent des opérations telles que la méthode de validation d'une opération. En outre, la stratégie PKI peut limiter l'étendue d'un certificat. Par exemple, la stratégie PKI peut affirmer qu'un certificat peut être utilisé uniquement à des fins spécifiques. Une telle stratégie peut empêcher qu'un certificat soit utilisé pour d'autres demandes.

- **Bibliothèque KMF** : cette bibliothèque contient des interfaces de programmation qui extraient le mécanisme keystore sous-jacent.

Les applications n'ont pas à choisir un mécanisme de keystore spécifique, ils peuvent migrer d'un seul mécanisme à un autre. Les fichiers keystore pris en charge sont PKCS #11, NSS et OpenSSL. La bibliothèque comprend une structure modulaire permettant l'ajout de nouveaux mécanismes keystore. Par conséquent, les applications qui utilisent les nouveaux mécanismes ne nécessitent que des modifications mineures pour utiliser un nouveau keystore.

---

**Remarque** – Pour déterminer la version de OpenSSL qui est en cours d'exécution, tapez `openssl version`. La sortie se présente de la manière suivante :

OpenSSL 1.0.0d 8 Feb 2011

---

## Utilitaires de la structure de gestion des clés

KMF offre des méthodes pour la gestion du stockage des clés et fournit la stratégie globale concernant l'utilisation de ces clés. KMF gère la stratégie, les clés et les certificats pour les trois technologies à clé publique suivantes :

- Fournisseurs de jetons de PKCS #11, c'est-à-dire provenant de la structure cryptographique
- NSS, c'est-à-dire les services de sécurité réseau (Network Security Services)
- OpenSSL, un keystore basé les fichiers

L'outil `kmfcfg` peut créer, modifier ou supprimer des entrées de stratégie KMF. L'outil gère également les plug-ins de la structure. KMF gère les keystores par le biais de la commande `pktool`. Pour plus d'informations, reportez-vous aux pages de manuel [kmfcfg\(1\)](#) et [pktool\(1\)](#) et aux sections suivantes.

## Gestion de la stratégie KMF

La stratégie KMF est enregistrée dans une base de données. Cette base de données de stratégie est accédée en interne par toutes les applications qui utilisent les interfaces de programmation KMF. La base de données peut limiter l'utilisation des clés et des certificats qui sont gérés par la bibliothèque KMF. Lorsqu'une application tente de vérifier un certificat, l'application vérifie la base de données de stratégies. La commande `kmfcfg` modifie la base de données de stratégies.

## Gestion de plug-in KMF

La commande `kmfcfg` fournit les sous-commandes suivantes pour les plug-ins :

- `list plugin` : répertorie les plug-ins gérés par KMF.
- `install plugin` : installe le plug-in par le nom de chemin d'accès du module et crée un keystore pour le plug-in. Pour supprimer le plug-in de KMF, supprimez le keystore.
- `uninstall plugin` : supprime le plug-in de KMF en supprimant son keystore.
- `modify plugin` : active le plug-in à exécuter avec une option définie dans le code du plug-in, comme `debug`.

Pour plus d'informations, reportez-vous à la page de manuel [kmfcfg\(1\)](#) Pour connaître la procédure, reportez-vous à la section “[Procédure de gestion des plug-ins tiers dans KMF](#)” à la page 283.

## Gestion de keystore KMF

KMF gère les keystores pour les trois technologies à clé publique, PKCS #11, NSS et OpenSSL. Pour l'ensemble de ces technologies, la commande `pktool` vous permet d'effectuer les opérations suivantes :

- Génération d'un certificat autosigné
- Génération d'une demande de certificat
- Génération d'une clé symétrique
- Génération d'une paire de clés publique/privée
- Génération d'une CSR (certificate signing request, demande de signature de certificat) PKCS #10 à envoyer à une autorité de certification externe (CA) pour signature
- Signature d'une CSR PKCS #10
- Importation d'objets dans le keystore
- Liste des objets dans le keystore
- Suppression d'objets du keystore

- Téléchargement d'une CRL.

Pour les technologies PKCS #11 et NSS, la commande `pktool` vous permet également de définir un code PIN en générant une phrase de passe :

- Génération d'une phrase de passe pour le keystore.
- Génération d'une phrase de passe pour un objet dans le keystore.

Pour consulter des exemples d'utilisation de l'utilitaire `pktool`, reportez-vous à la page de manuel `pktool(1)` et à la section “[Utilisation de la structure de gestion des clés \(liste des tâches\)](#)” à la page 272.

## Utilisation de la structure de gestion des clés (tâches)

Cette section décrit l'utilisation de la commande `pktool` pour gérer vos objets de clé publique, tels que des mots et phrases de passe, des fichiers, des keystores, des certificats et des CRL.

### Utilisation de la structure de gestion des clés (liste des tâches)

La structure de gestion des clés (KMF) vous permet de gérer de manière centralisée les technologies à clé publique.

| Tâche                            | Description                                                                                                                            | Voir                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Création d'un certificat         | Crée un certificat à utiliser par PKCS #11, NSS ou SSL.                                                                                | <a href="#">“Procédure de création d'un certificat à l'aide de la commande pktool gencert” à la page 273</a>        |
| Exportation d'un certificat      | Crée un fichier avec le certificat et ses clés de prise en charge. Le fichier peut être protégé par un mot de passe.                   | <a href="#">“Procédure d'exportation d'un certificat et de la clé privée au format PKCS #12” à la page 276</a>      |
| Importation d'un certificat      | Importe un certificat à partir d'un autre système.                                                                                     | <a href="#">“Procédure d'importation d'un certificat dans votre keystore” à la page 274</a>                         |
|                                  | Importe un certificat en format PKCS #12 à partir d'un autre système.                                                                  | <a href="#">Exemple 13–2</a>                                                                                        |
| Génération d'une phrase de passe | Génère une phrase de passe pour l'accès à un keystore PKCS #11 ou NSS.                                                                 | <a href="#">“Procédure de génération d'une phrase de passe à l'aide de la commande pktool setpin” à la page 277</a> |
| Génération d'une clé symétrique  | Génération des clés symétriques à utiliser dans les fichiers de chiffrement, pour créer le MAC d'un fichier, et pour les applications. | <a href="#">“Procédure de génération d'une clé symétrique à l'aide de la commande pktool” à la page 243</a>         |



| Tâche                          | Description                                                                                                                                                    | Voir                                                                                                                                   |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Génération d'une paire de clés | Génération d'une paire de clés publique/privée à utiliser avec des applications.                                                                               | <a href="#">“Procédure de génération d'une paire de clés à l'aide de la commande <code>pktool genkeypair</code>” à la page 278</a>     |
| Génération d'une CSR PKCS #10  | Génération d'une CSR (certificate signing request, demande de signature de certificat) PKCS #10 à faire signer par une autorité de certification externe (CA). | Page de manuel <code>pktool(1)</code>                                                                                                  |
| Signature d'une CSR PKCS #10   | Signe une CSR PKCS #10.                                                                                                                                        | <a href="#">“Procédure de signature d'une demande de certificat à l'aide de la commande <code>pktool signcsr</code>” à la page 282</a> |
| Ajout d'un plug-in à KMF       | Installe, modifie et répertorie un plug-in. En outre, supprime le plug-in dans la KMF.                                                                         | <a href="#">“Procédure de gestion des plug-ins tiers dans KMF” à la page 283</a>                                                       |

## ▼ Procédure de création d'un certificat à l'aide de la commande `pktool gencert`

Cette procédure crée un certificat autosigné et le stocke dans le keystore PKCS #11. Dans le cadre de cette opération, une paire de clés publique et privée RSA est également créée. La clé privée est stockée dans le keystore avec le certificat.

### 1 Génération d'un certificat autosigné

```
% pktool gencert [keystore=keystore] label=label-name \
subject=subject-DN serial=hex-serial-number
```

|                                       |                                                                                                                                                                         |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>keystore=keystore</code>        | Spécifie le keystore par type d'objet de clé publique. La valeur peut être <code>nss</code> , <code>pkcs11</code> ou <code>ssl</code> . Ce mot de passe est facultatif. |
| <code>label=label-name</code>         | Spécifie un nom unique donné au certificat par l'émetteur.                                                                                                              |
| <code>subject=subject-DN</code>       | Spécifie le nom distinctif du certificat.                                                                                                                               |
| <code>serial=hex-serial-number</code> | Spécifie le numéro de série au format hexadécimal. L'émetteur du certificat choisit ce nombre, comme par exemple <code>0x0102030405</code> .                            |

### 2 Vérifiez le contenu du keystore.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
   ID: Fingerprint that binds certificate to private key
   Subject: subject-DN
   Issuer: distinguished-name
   Serial: hex-serial-number
n. ...
```

Cette commande répertorie tous les certificats dans le keystore. Dans l'exemple suivant, le keystore ne contient qu'un seul certificat.

### Exemple 13-1 Création d'un certificat autosigné à l'aide de pktool

Dans l'exemple suivant, un utilisateur à My Company crée un certificat autosigné et le stocke dans un keystore pour les objets PKCS #11. Le keystore est initialement vide. Si le keystore n'a pas été initialisé, le code PIN pour le softtoken est changeme.

```
% pktool gencert keystore=pkcs11 label="My Cert" \
subject="C=US, O=My Company, OU=Security Engineering Group, CN=MyCA" \
serial=0x00000001
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token

% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: My Cert
   ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
   Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Serial: 0x01
```

## ▼ Procédure d'importation d'un certificat dans votre keystore

Cette procédure explique comment importer un fichier contenant des informations PKI codé avec PEM ou DER raw dans votre keystore. Pour connaître la procédure d'exportation, reportez-vous à l'[Exemple 13-4](#).

### 1 Importez le certificat.

```
% pktool import keystore=keystore infile=infile-name label=label-name
```

### 2 Si vous importez des objets PKI privés, entrez les mots de passe lorsque vous y êtes invité.

#### a. A l'invite, entrez le mot de passe pour le fichier.

Si vous importez des informations PKI privées, tels qu'un fichier d'exportation au format PKCS #12, le fichier nécessite un mot de passe. Le créateur du fichier que vous importez vous fournit le mot de passe PKCS #12.

```
Enter password to use for accessing the PKCS12 file:    Type PKCS #12 password
```

#### b. A l'invite, entrez le mot de passe pour le keystore.

```
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token
```

### 3 Vérifiez le contenu du keystore.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
   ID: Fingerprint that binds certificate to private key
   Subject: subject-DN
   Issuer: distinguished-name
   Serial: hex-serial-number
2. ...
```

#### Exemple 13-2 Importation d'un fichier PKCS #12 dans votre keystore

Dans l'exemple suivant, l'utilisateur importe un fichier PKCS #12 d'un tiers. La commande `pktool import` extrait la clé privée et le certificat du fichier `gracedata.p12` et les stocke dans le keystore préféré de l'utilisateur.

```
% pktool import keystore=pkcs11 infile=gracedata.p12 label=GraceCert
Enter password to use for accessing the PKCS12 file: Type PKCS #12 password
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token
Found 1 certificate(s) and 1 key(s) in gracedata.p12
% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: GraceCert
   ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
   Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Serial: 0x01
```

#### Exemple 13-3 Importation d'un certificat X.509 dans votre keystore

Dans l'exemple suivant, l'utilisateur importe un certificat X.509 au format PEM dans le keystore préféré de l'utilisateur. Ce certificat public n'est pas protégé par un mot de passe. Le keystore public de l'utilisateur n'est pas protégé par un mot de passe non plus.

```
% pktool import keystore=pkcs11 infile=somecert.pem label="TheirCompany Root Cert"
% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: TheirCompany Root Cert
   ID: 21:ae:83:98:24:d1:1f:cb:65:5b:48:75:d0:2:47:cf:98:1f:ec:a0
   Subject: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
   Issuer: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
   Serial: 0x01
```

## ▼ Procédure d'exportation d'un certificat et de la clé privée au format PKCS #12

Vous pouvez créer un fichier au format PKCS #12 afin d'exporter des clés privées et leur certificat X.509 associé vers d'autres systèmes. L'accès au fichier est protégé par un mot de passe.

### 1 Recherchez le certificat à exporter.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
   ID: Fingerprint that binds certificate to private key
   Subject: subject-DN
   Issuer: distinguished-name
   Serial: hex-serial-number
2. ...
```

### 2 Exportez les clés et le certificat.

Utilisez le keystore et l'étiquette de la commande `pktool list`. Donnez un nom au fichier d'exportation. Si le nom contient un espace, mettez le nom entre guillemets.

```
% pktool export keystore=keystore outfile=outfile-name label=label-name
```

### 3 Protégez le fichier d'exportation par un mot de passe.

A l'invite, entrez le mot de passe courant du keystore. A ce stade, vous créez un mot de passe pour le fichier d'exportation. Le destinataire doit fournir ce mot de passe lors de l'importation du fichier.

```
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token
Enter password to use for accessing the PKCS12 file:    Create PKCS #12 password
```

---

**Astuce** – Envoyez le mot de passe séparément du fichier d'exportation. Les pratiques recommandées suggèrent que vous fournissiez le mot de passe hors bande, par exemple lors d'un appel téléphonique.

---

### Exemple 13–4 Exportation d'un certificat et de la clé privée au format PKCS #12

Dans l'exemple suivant, un utilisateur exporte les clés privées avec leur certificat X.509 associé dans un fichier PKCS #12 normal. Ce fichier peut être importé dans d'autres keystores. Le mot de passe PKCS #11 protège le keystore source. Le mot de passe PKCS #12 est utilisé pour protéger des données privées dans le fichier PKCS #12. Ce mot de passe est requis pour importer le fichier.

```
% pktool list
Found 1 certificates.
1. (X.509 certificate)
```

```

Label: My Cert
ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
Serial: 0x01

```

```

% pktool export keystore=pkcs11 outfile=mydata.p12 label="My Cert"
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file:  Create PKCS #12 password

```

L'utilisateur appelle ensuite le destinataire par téléphone pour lui fournir le mot de passe PKCS #12.

## ▼ Procédure de génération d'une phrase de passe à l'aide de la commande `pktool setpin`

Vous pouvez générer une phrase de passe pour un objet dans un keystore et pour le keystore lui-même. La phrase de passe est nécessaire pour accéder à l'objet ou au keystore. Pour un exemple de génération d'une phrase de passe pour un objet dans un keystore, reportez-vous à l'[Exemple 13-4](#).

### 1 Générez une phrase de passe pour accéder à un keystore.

```
% pktool setpin keystore=nss|pkcs11 dir=directory
```

### 2 Répondez aux invites.

Si aucun mot de passe n'est encore défini pour le keystore, appuyez sur la touche Entrée pour créer le mot de passe.

```

Enter current token passphrase:      Press the Return key
Create new passphrase:               Type the passphrase that you want to use
Re-enter new passphrase:             Retype the passphrase
Passphrase changed.

```

Le keystore est maintenant protégé par une *passphrase*. Si vous perdez la phrase de passe, vous perdez l'accès aux objets dans le keystore.

### Exemple 13-5 Protection d'un keystore par une phrase de passe

L'exemple suivant montre comment définir la phrase de passe pour une base de données NSS. Comme aucune phrase de passe n'a été créée, l'utilisateur appuie sur la touche Entrée à la première invite.

```

% pktool setpin keystore=nss dir=/var/nss
Enter current token passphrase:      Press the Return key
Create new passphrase:               has8n0NdaH

```

Re-enter new passphrase: **has8n0NdaH**  
Passphrase changed.

## ▼ Procédure de génération d'une paire de clés à l'aide de la commande **pktool genkeypair**

Certaines applications exigent une paire de clés publique/privée. Dans cette procédure, vous créez ces paires de clés et les stockez.

### 1 (Facultatif) Si vous prévoyez d'utiliser un keystore, créez-le.

- Pour créer et initialiser un keystore PKCS #11, reportez-vous à la section [“Procédure de génération d'une phrase de passe à l'aide de la commande \*\*pktool setpin\*\*” à la page 277.](#)
- Pour créer et initialiser un keystore NSS, reportez-vous à l'[Exemple 13–5](#).

### 2 Créez la paire de clés.

Choisissez l'une des méthodes suivantes.

- **Créez la paire de clés et stockez-la dans un fichier.**

Les clés basées sur des fichiers sont créées pour les applications qui lisent les clés directement à partir de fichiers sur le disque. En règle générale, les applications qui utilisent directement les bibliothèques de chiffrement OpenSSL requièrent le stockage des clés et des certificats pour l'application dans des fichiers.

---

**Remarque** – Le keystore `file` ne prend pas en charge les clés et les certificats de courbes elliptiques (`ec`) .

---

```
% pktool genkeypair keystore=file outkey=key-filename \  
[format=der|pem] [keytype=rsa|dsa] [keylen=key-size]
```

`keystore=file`

La valeur `file` spécifie le type de fichier dans l'emplacement de stockage de la clé.

`outkey=key-filename`

Spécifie le nom du fichier de stockage de la paire de clés.

`format=der|pem`

Spécifie le format de codage de la paire de clés. La sortie `der` est binaire et la sortie `pem` est ASCII.

`keytype=rsa|dsa`

Spécifie le type de paire de clés qui peut être stockée dans un keystore file. Pour obtenir des définitions, reportez-vous à [DSA](#) et [RSA](#).

`keylen=key-size`

Spécifie la longueur de la clé en bits. Le nombre doit être divisible par 8. Pour déterminer les tailles de clés possibles, utilisez la commande `cryptoadm list -vm`.

#### ■ Créez la paire de clés et stockez-la dans un keystore PKCS #11.

Vous devez effectuer l'[Étape 1](#) avant d'utiliser cette méthode.

Le keystore PKCS #11 permet de stocker des objets sur un périphérique matériel. Le périphérique peut être une carte Sun Crypto Accelerator 6000, un périphérique TPM (Trusted Platform Module, module de plate-forme de confiance) ou une carte à puce branchée à la structure cryptographique. PKCS #11 peut également être utilisé pour stocker des objets dans le `softtoken`, ou jeton logiciel, qui stocke les objets dans un sous-répertoire privé sur le disque. Pour plus d'informations, reportez-vous à la page de manuel [pkcs11\\_softtoken\(5\)](#).

Vous pouvez récupérer la paire de clés dans le keystore par une étiquette que vous indiquez.

```
% pktool genkeypair label=key-label \
[token=token[:manuf[:serial]]] \
[keytype=rsa|dsa|ec] [curve=ECC-Curve-Name] \
[keylen=key-size] [listcurves]
```

`label=key-label`

Spécifie une étiquette pour la paire de clés. La paire de clés peut être récupérée à partir du keystore par son étiquette.

`token=token[:manuf[:serial]]`

Spécifie le nom du jeton. Par défaut, le nom du jeton est Sun Software PKCS#11 `softtoken`.

`keytype=rsa|dsa|ec` [curve=ECC-Curve-Name]

Spécifie le type de la paire de clés. Pour le type de courbe elliptique (ec), vous pouvez éventuellement spécifier le nom de la courbe. Les noms de courbes sont répertoriés en tant que sortie de l'option `listcurves`.

`keylen=key-size`

Spécifie la longueur de la clé en bits. Le nombre doit être divisible par 8.

`listcurves`

Répertorie les noms de courbes elliptiques qui peuvent être utilisés comme valeurs de l'option `curve=` pour un type de clé ec.

#### ■ Générez une paire de clés et stockez-la dans un keystore NSS.

Le keystore NSS est utilisé par les serveurs qui utilisent NSS comme interface de chiffrement principale. Par exemple, le Oracle iPlanet Web Server utilise les bases de données NSS pour stocker les objets.

Vous devez effectuer l'**Étape 1** avant d'utiliser cette méthode.

```
% pktool keystore=nss genkeypair label=key-nickname \
[token=token[:manuf[:serial]]] \
[dir=directory-path] [prefix=database-prefix] \
[keytype=rsa|dsa|ec] [curve=ECC-Curve-Name] \
[keylen=key-size] [listcurves]
```

**keystore=nss**

La valeur *nss* spécifie le type NSS de l'emplacement de stockage de la clé.

**label=nickname**

Spécifie une étiquette pour la paire de clés. La paire de clés peut être récupérée à partir du keystore par son étiquette.

**token=token[:manuf[:serial]]**

Spécifie le nom du jeton. Par défaut, le jeton est Sun Software PKCS#11 softtoken.

**dir=directory**

Spécifie le chemin d'accès au répertoire de la base de données NSS. Par défaut, *directory* est le répertoire courant.

**prefix=database-prefix**

Spécifie le préfixe de la base de données NSS. Par défaut, le champ de préfixe est vide.

**keytype=rsa|dsa|ec [curve=ECC-Curve-Name]**

Spécifie le type de la paire de clés. Pour le type de courbe elliptique, vous pouvez éventuellement spécifier le nom de la courbe. Les noms de courbes sont répertoriés en tant que sortie de l'option *listcurves*.

**keylen=key-size**

Spécifie la longueur de la clé en bits. Le nombre doit être divisible par 8.

**listcurves**

Répertorie les noms de courbes elliptiques qui peuvent être utilisés comme valeurs de l'option *curve=* pour un type de clé *ec*.

### 3 (Facultatif) Vérifiez que la clé existe.

Utilisez l'une des commandes suivantes, en fonction de l'emplacement où vous avez stocké la clé :

- **Vérifiez la clé dans le fichier *key-filename*.**

```
% pktool list keystore=file objtype=key infile=key-filename
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Vérifiez la clé dans le keystore PKCS #11.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```



- **Vérifiez la clé dans le keystore NSS.**

```
% pktool list keystore=nss dir=directory objtype=key
```

### Exemple 13–6 Création d'une paire de clés à l'aide de la commande pktool

Dans l'exemple ci-dessous, un utilisateur crée un keystore PKCS #11 pour la première fois. Après avoir déterminé les tailles de clé des paires de clés RSA, l'utilisateur génère une paire de clés pour une application. Enfin, l'utilisateur vérifie que la paire de clés figure dans le keystore. L'utilisateur constate que la seconde instance de la paire de clés RSA peut être stockée sur le matériel. Etant donné que l'utilisateur ne spécifie pas un argument token, la paire de clés est stockée sous forme d'un Sun Software PKCS#11 softtoken.

```
# pktool setpin
Create new passphrase:      Easily remembered, hard-to-detect password
Re-enter new passphrase:    Retype password
Passphrase changed.
% cryptoadm list -vm | grep PAIR
...
CKM_DSA_KEY_PAIR_GEN        512  1024 . . .
CKM_RSA_PKCS_KEY_PAIR_GEN   256  4096 . . .
...
CKM_RSA_PKCS_KEY_PAIR_GEN   512  2048 X . .
ecc: CKM_EC_KEY_PAIR_GEN,CKM_ECDH1_DERIVE,CKM_ECDSA,CKM_ECDSA_SHA1
% pktool genkeypair label=specialappkeypair keytype=rsa keylen=2048
Enter PIN for Sun Software PKCS#11 softtoken :    Type password

% pktool list
Enter PIN for Sun Software PKCS#11 softtoken :    Type password

Found 1 keys.
Key #1 - keypair:  specialappkeypair (2048 bits)
```

### Exemple 13–7 Création d'une paire de clés qui utilise l'algorithme de courbe elliptique

Dans l'exemple suivant, un utilisateur ajoute une paire de clés de courbe elliptique (ec) dans le keystore, spécifie un nom de courbe et vérifie que la paire de clés figure dans le keystore.

```
% pktool genkeypair listcurves
secp112r1, secp112r2, secp128r1, secp128r2, secp160k1
.
.
.
c2pnb304w1, c2tnb359v1, c2pnb368w1, c2tnb431r1, prime192v2
prime192v3
% pktool genkeypair label=eckeypair keytype=ec curves=c2tnb431r1
% pktool list
Enter PIN for Sun Software PKCS#11 softtoken :    Type password
```

Found 2 keys.

Key #1 - keypair: specialappkeypair (2048 bits)

Key #2 - keypair: eckeypair (c2tnb431r1)

## ▼ Procédure de signature d'une demande de certificat à l'aide de la commande `pktool signcsr`

Cette procédure est utilisée pour signer une CSR (demande de signature du certificat) PKCS #10. La CSR peut être au format PEM ou DER. Le processus de signature émet un certificat X.509 v3. Pour générer une CSR PKCS #10, reportez-vous à la page de manuel [pktool\(1\)](#).

### Avant de commencer

Vous êtes une autorité de certification (CA), vous avez reçu une CSR et elle est stockée dans un fichier.

#### 1 Recueillez les informations suivantes pour les arguments requis de la commande `pktool signcsr`:

**signkey** Si vous avez stocké la clé du signataire dans un keystore PKCS #11, **signkey** est l'*étiquette* qui récupère cette clé privée.

Si vous avez stocké la clé du signataire dans un keystore NSS, **signkey** est le nom du fichier qui contient cette clé privée.

**csr** Spécifie le nom de fichier de la CSR.

**serial** Spécifie le numéro de série du certificat signé.

**outcert** Spécifie le nom de fichier du certificat signé.

**issuer** Spécifie votre nom d'émetteur CA au format DN (nom distinctif).

Pour plus d'informations sur les arguments facultatifs de la sous-commande `signcsr`, reportez-vous à la page de manuel [pktool\(1\)](#).

#### 2 Signez la demande et émettez le certificat.

Par exemple, la commande suivante signe le certificat avec la clé du signataire figurant dans le référentiel PKCS #11 :

```
# pktool signcsr signkey=CASigningKey \  
csr=fromExampleCoCSR \  
serial=0x12345678 \  
outcert=ExampleCoCert2010 \  
issuer="O=Oracle Corporation, \  
OU=Oracle Solaris Security Technology, L=Redwood City, ST=CA, C=US, \  
CN=rootsign Oracle"
```

La commande suivante signe le certificat avec la clé du signataire figurant dans un fichier :

```
# pktool signcsr signkey=CASigningKey \
csr=fromExampleCoCSR \
serial=0x12345678 \
outcert=ExampleCoCert2010 \
issuer="O=Oracle Corporation, \
      OU=Oracle Solaris Security Technology, L=Redwood City, ST=CA, C=US, \
      CN=rootsign Oracle"
```

### 3 Envoyez le certificat au demandeur.

Vous pouvez utiliser des e-mails, un site web ou un autre mécanisme pour livrer le certificat au demandeur.

Par exemple, vous pouvez utiliser votre messagerie pour envoyer le fichier `ExampleCoCert2010` au demandeur.

## ▼ Procédure de gestion des plug-ins tiers dans KMF

Vous identifiez votre plug-in en lui attribuant un nom de keystore. Lorsque vous ajoutez le plug-in à la KMF, le logiciel l'identifie par son nom de keystore. Le plug-in peut être défini de manière à accepter une option. Cette procédure inclut la suppression du plug-in de la KMF.

### 1 Installez le plug-in.

```
% /usr/bin/kmfcfg install keystore=keystore-name \
modulepath=path-to-plugin [option="option-string"]
```

où

*keystore-name* : spécifie un nom unique pour le keystore que vous fournissez.

*path-to-plugin* : spécifie le chemin d'accès complet à l'objet de bibliothèque partagée pour le plug-in KMF.

*option-string* : spécifie un argument facultatif de l'objet de bibliothèque partagée.

### 2 Répertoriez les plug-ins.

```
% kmfcfg list plugin
keystore-name:path-to-plugin [(built-in)] | [;option=option-string]
```

### 3 Pour supprimer le plug-in, désinstallez-le et vérifiez sa suppression.

```
% kmfcfg uninstall keystore=keystore-name
% kmfcfg plugin list
```

**Exemple 13-8** Appel d'un plug-in KMF avec une option

Dans l'exemple suivant, l'administrateur stocke un plug-in KMF dans un répertoire spécifique au site. Le plug-in est défini pour accepter une option debug. L'administrateur ajoute le plug-in et vérifie qu'il est installé.

```
# /usr/bin/kmfcfg install keystore=mykmfplug \
modulepath=/lib/security/site-modules/mykmfplug.so
# kmfcfg list plugin
KMF plugin information:
-----
pkcs11:kmf_pkcs11.so.1 (built-in)
file:kmf_openssl.so.1 (built-in)
nss:kmf_nss.so.1 (built-in)
mykmfplug:/lib/security/site-modules/mykmfplug.so
# kmfcfg modify plugin keystore=mykmfplug option="debug"
# kmfcfg list plugin
KMF plugin information:
-----
...
mykmfplug:/lib/security/site-modules/mykmfplug.so;option=debug
```

Le plug-in s'exécute à présent en mode de débogage.

## PARTIE V

# Services d'authentification et communication sécurisée

Cette section décrit les services d'authentification pouvant être configurés sur un système autonome ou entre deux systèmes.

- [Chapitre 14, “Authentification des services réseau \(tâches\)”](#)
- [Chapitre 15, “Utilisation de PAM”](#)
- [Chapitre 16, “Utilisation de SASL”](#)
- [Chapitre 17, “Utilisation de Secure Shell \(tâches\)”](#)
- [Chapitre 18, “Secure Shell \(référence\)”](#)

Pour configurer un réseau d'utilisateurs et de systèmes authentifiés, reportez-vous à la section [Partie VI](#).



## Authentification des services réseau (tâches)

---

Ce chapitre fournit des informations sur la façon d'utiliser le RPC sécurisé pour authentifier un hôte et un utilisateur sur un montage NFS. Voici la liste des sujets abordés dans ce chapitre :

- [“Présentation du RPC sécurisé” à la page 287](#)
- [“Administration de l'authentification avec le RPC sécurisé \(tâches\)” à la page 292](#)

### Présentation du RPC sécurisé

Le RPC (Remote Procedure Call, appel de procédure à distance) sécurisé protège les procédures distantes par le biais d'un mécanisme d'authentification. Le mécanisme d'authentification Diffie-Hellman authentifie à la fois l'hôte et l'utilisateur à l'origine d'une demande de service. Le mécanisme d'authentification utilise le chiffrement Data Encryption Standard (DES). Les applications qui utilisent le RPC sécurisé incluent le service de noms NFS et NIS.

### Services NFS et RPC sécurisé

NFS permet à plusieurs hôtes de partager des fichiers sur le réseau. Dans le cadre du service NFS, un serveur contient les données et les ressources pour plusieurs clients. Les clients ont accès aux systèmes de fichiers que le serveur partage avec les clients. Les utilisateurs connectés aux systèmes client peuvent accéder aux systèmes de fichiers en montant les systèmes de fichiers à partir du serveur. Pour l'utilisateur sur le système client, il s'affiche comme si les fichiers étaient des fichiers locaux pour le client. L'une des utilisations les plus courantes de NFS permet aux systèmes d'être installés dans les bureaux, tout en stockant tous les fichiers utilisateur dans un emplacement central. Certaines fonctions du service NFS, telles que l'option `-nosuid` de la commande `mount` peuvent être utilisées pour interdire l'ouverture des périphériques et systèmes de fichiers par des utilisateurs non autorisés.

Le service NFS utilise le RPC sécurisé afin d'authentifier les utilisateurs adressant des demandes sur le réseau. Ce processus est appelé *NFS sécurisé*. Le mécanisme d'authentification Diffie-Hellman AUTH\_DH utilise des fonctions de chiffrement DES pour garantir un accès autorisé. Le mécanisme AUTH\_DH est également appelé AUTH\_DES. Pour plus d'informations, reportez-vous aux références suivantes :

- Pour configurer et administrer le service NFS sécurisé, reportez-vous à la section [“Administration du système NFS sécurisé” du manuel \*Administration d'Oracle Solaris : Services réseau\*](#).
- Pour une présentation des transactions impliquées dans l'authentification RPC, reportez-vous à la section [“Mise en oeuvre de l'authentification Diffie-Hellman” à la page 289](#).

## Chiffrement DES avec NFS sécurisé

Les fonctions de chiffrement Data Encryption Standard (DES) utilisent une clé 56 bits pour chiffrer les données. Si deux utilisateurs identifiés ou principaux disposent de la même clé DES, ils peuvent communiquer en privé à l'aide de la clé pour chiffrer et déchiffrer du texte. DES est un mécanisme de chiffrement relativement rapide.

Le risque lié à l'utilisation de la clé DES uniquement est qu'un intrus puisse recueillir suffisamment de messages texte chiffrés avec la même clé pour être en mesure de découvrir la clé et déchiffrer les messages. C'est pour cette raison que les systèmes de sécurité tels que NFS sécurisé doivent changer de clés fréquemment.

## Authentification Kerberos

Kerberos est un système d'authentification développé au MIT. Une partie du chiffrement dans Kerberos est basée sur DES. La prise en charge de Kerberos V4 n'est plus assurée dans le cadre du RPC sécurisé. Cependant, une mise en oeuvre côté client et côté serveur de Kerberos V5, qui utilise RPCSEC\_GSS, est incluse dans cette version. Pour plus d'informations, reportez-vous au [Chapitre 19, “Introduction au service Kerberos”](#).

## Authentification Diffie-Hellman et RPC sécurisé

La méthode Diffie-Hellman (DH) d'authentification des utilisateurs se révèle très difficile à déchiffrer pour un intrus. Le client et le serveur disposent chacun de leur clé privée, qu'ils utilisent avec la clé publique pour créer une clé commune. La clé privée est également appelée *clé secrète*. Le client et le serveur utilisent la clé commune pour communiquer l'un avec l'autre. La clé commune est chiffrée à l'aide d'une fonction de chiffrement convenue, comme par exemple la méthode DES.



L'authentification est basée sur la capacité du système émetteur à utiliser la clé commune pour chiffrer l'heure actuelle. Le système récepteur peut ensuite la déchiffrer et la vérifier par rapport à son heure actuelle. L'heure du client et l'heure du serveur doivent être synchronisées. Pour plus d'informations, reportez-vous à la section [“Gestion du protocole NTP \(tâches\)” du manuel \*Administration d'Oracle Solaris : Services réseau\*](#).

Les clés publiques et privées sont conservées dans une base de données NIS. NIS stocke les clés dans la carte `publickey`. Ce fichier contient la clé publique et la clé privée pour tous les utilisateurs potentiels.

L'administrateur système est responsable du paramétrage des cartes NIS, et de la génération d'une clé publique et d'une clé privée pour chaque utilisateur. La clé privée est stockée sous forme chiffrée avec le mot de passe de l'utilisateur. Du fait de ce processus, la clé privée n'est connue que de l'utilisateur.

## Mise en oeuvre de l'authentification Diffie-Hellman

Cette section décrit la série de transactions dans une session client-serveur utilisant la méthode d'authentification Diffie-Hellman (`AUTH__DH`).

### Génération de clés publiques et de clés secrètes pour le RPC sécurisé

Avant une transaction, l'administrateur exécute la commande `newkey` ou `nisaddcred` pour générer une clé publique et une clé secrète. Chaque utilisateur dispose de ses propres clé publique et clé secrète. La clé publique est stockée dans une base de données publique. La clé secrète est stockée sous forme chiffrée dans la même base de données. La commande `chkey` modifie la paire de clés.

### Exécution de la commande `keylogin` pour le RPC sécurisé

Normalement, le mot de passe de connexion est identique au mot de passe du RPC sécurisé. Dans ce cas, la commande `keylogin` n'est pas requise. Toutefois, si les mots de passe sont différents, les utilisateurs doivent se connecter, puis exécuter la commande `keylogin`.

La commande `keylogin` invite l'utilisateur à indiquer son mot de passe de RPC sécurisé. La commande utilise ensuite le mot de passe pour déchiffrer la clé secrète. La commande `keylogin` transmet ensuite la clé secrète déchiffrée au programme du *serveur de clés*. Le serveur de clés est un service RPC avec une instance locale sur chaque ordinateur. Le serveur de clés enregistre la clé secrète déchiffrée et attend que l'utilisateur lance une transaction de RPC sécurisé avec un serveur.

Si le mot de passe de connexion et le mot de passe RPC sont identiques, le processus de connexion transmet la clé secrète au serveur de clés. Si les mots de passe doivent être différents, l'utilisateur doit toujours exécuter la commande `keylogin`. Lorsque la commande `keylogin` est incluse dans le fichier de configuration d'environnement de l'utilisateur, tels que le fichier `~/.login`, `~/.cshrc` ou `~/.profile`, la commande `keylogin` s'exécute automatiquement chaque fois que l'utilisateur se connecte.

## Génération de la clé de conversation pour le RPC sécurisé

Lorsque l'utilisateur lance une transaction avec un serveur, les événements suivants se produisent :

1. Le serveur de clés génère une clé de conversation de manière aléatoire.
2. Le noyau utilise la clé de conversation, ainsi que d'autres matériaux, pour chiffrer l'horodatage du client.
3. Le serveur de clés recherche la clé publique du serveur dans la base de données des clés publiques. Pour plus d'informations, reportez-vous à la page de manuel [publickey\(4\)](#).
4. Le serveur de clés utilise la clé secrète du client et la clé publique du serveur pour générer une clé commune.
5. Le serveur de clés chiffre la clé de conversation avec la clé commune.

## Connexion initiale au serveur dans le RPC sécurisé

La transmission, qui inclut l'horodatage chiffré et la clé de conversation chiffrée, est ensuite envoyée au serveur. La transmission comprend également des informations d'identification et un vérificateur. L'information d'identification contient trois composants :

- Le nom de réseau du client
- La clé de conversation chiffrée à l'aide de la clé commune
- Une "fenêtre" chiffrée à l'aide de la clé de conversation

La fenêtre correspond à la différence de temps qui doit être autorisée selon le client entre l'horloge du serveur et l'horodatage du client. Si la différence entre l'horloge du serveur et l'horodatage est supérieure à la fenêtre, le serveur rejette la demande du client. Dans des circonstances normales, ce rejet ne se produit pas, car le client se synchronise d'abord avec le serveur avant de commencer la session RPC.

Le vérificateur du client contient les éléments suivants :

- L'horodatage chiffré
- Un vérificateur chiffré de la fenêtre spécifiée, décrémente de 1.

Le vérificateur de fenêtre est requis au cas où quelqu'un tenterait d'usurper l'identité d'un utilisateur. L'usurpateur peut écrire un programme qui, au lieu de remplir les champs chiffrés avec les informations d'identification et le vérificateur, insère simplement des bits aléatoires. Le serveur déchiffre la clé de conversation dans une clé aléatoire. Le serveur utilise ensuite la clé pour tenter de déchiffrer la fenêtre et l'horodatage. Il en résulte des nombres aléatoires. Cependant, après quelques milliers d'essais, la paire fenêtre/horodatage aléatoire est susceptible de passer le système d'authentification. Le vérificateur de fenêtre réduit les risques que des informations d'identification fausses puissent être authentifiées.

## Déchiffrement de la clé de conversation dans le RPC sécurisé

Lorsque le serveur reçoit la transmission du client, les événements suivants se produisent :

1. Le serveur de clés qui est local pour le serveur recherche la clé publique du client dans la base de données de clés publiques.
2. Le serveur de clés utilise la clé publique du client et la clé secrète du serveur pour en déduire la clé commune. La clé commune est identique à celle calculée par le client. Seul le serveur et le client peuvent calculer la clé commune car le calcul nécessite de connaître l'une des clés secrètes.
3. Le noyau utilise la clé commune pour déchiffrer la clé de conversation.
4. Le noyau appelle le serveur de clés pour déchiffrer l'horodatage du client à l'aide de la clé de conversation déchiffrée.

## Stockage d'informations sur le serveur dans le RPC sécurisé

Une fois l'horodatage du client déchiffré par le serveur, ce dernier enregistre quatre éléments d'informations dans une table des informations d'identification :

- Le nom d'ordinateur du client
- La clé de conversation
- La fenêtre
- L'horodatage du client

Le serveur enregistre les trois premiers éléments pour une utilisation ultérieure. Le serveur enregistre l'horodatage du client pour empêcher toute rediffusion. Le serveur accepte uniquement les horodatages qui sont postérieurs au dernier horodatage vu. Par conséquent, les transactions rediffusées sont garanties d'être rejetées.

---

**Remarque** – Dans ces transactions, le nom de l'appelant, qui doit être authentifié d'une manière ou d'une autre, est implicite. Le serveur de clés ne peut pas utiliser l'authentification DES afin d'authentifier l'appelant car l'utilisation de DES par le serveur de clés pourrait générer un interblocage. Pour éviter tout interblocage, le serveur de clés stocke les clés secrètes par ID utilisateur (UID) et attribue des requêtes uniquement aux processus root locaux.

---

## Renvoi du vérificateur au client dans le RPC sécurisé

Le serveur renvoie un vérificateur au client incluant les éléments suivants :

- L'ID d'index, qui est enregistré par le serveur dans son cache des informations d'identification
- L'horodatage du client moins 1, qui est chiffré à l'aide de la clé de conversation

La soustraction de 1 à l'horodatage du client permet de garantir que l'horodatage est obsolète. Un horodatage obsolète ne peut pas être réutilisé comme vérificateur de client.

### Authentification du serveur dans le RPC sécurisé

Le client reçoit le vérificateur et authentifie le serveur. Le client sait que seul le serveur peut avoir envoyé le vérificateur car le serveur est le seul à connaître l'horodatage envoyé par le client.

### Traitement des transactions dans le RPC sécurisé

Avec chaque transaction survenant après la première transaction, le client renvoie l'ID d'index au serveur dans sa prochaine transaction. Le client envoie également un autre horodatage chiffré. Le serveur renvoie l'horodatage du client moins 1, chiffré par la clé de conversation.

## Administration de l'authentification avec le RPC sécurisé (tâches)

En requérant l'authentification pour l'utilisation des systèmes de fichiers NFS montés, vous augmentez la sécurité de votre réseau.

### Administration du RPC sécurisé (liste des tâches)

La liste des tâches suivante indique les procédures de configuration du RPC sécurisé pour NIS et NFS.

| Tâche                                                            | Description                                                                                                             | Voir                                                                                                        |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1. Démarrage du serveur de clés.                                 | Permet de s'assurer que des clés peuvent être créées, de sorte que les utilisateurs peuvent être authentifiés.          | <a href="#">“Procédure de redémarrage du serveur de clé RPC sécurisé” à la page 293</a>                     |
| 2. Définition des informations d'identification sur un hôte NIS. | Permet de s'assurer que l'utilisateur root sur un hôte peut être authentifié dans un environnement NIS.                 | <a href="#">“Procédure de configuration d'une clé Diffie-Hellman pour un hôte NIS” à la page 293</a>        |
| 3. Attribution d'une clé à un utilisateur NIS.                   | Permet à un utilisateur d'être authentifié dans un environnement NIS.                                                   | <a href="#">“Procédure de configuration d'une clé Diffie-Hellman pour un utilisateur NIS” à la page 294</a> |
| 4. Partage de fichiers NFS avec authentification.                | Permet à un serveur NFS de protéger en toute sécurité des systèmes de fichiers partagés à l'aide de l'authentification. | <a href="#">“Procédure de partage de fichiers NFS avec l'authentification Diffie-Hellman” à la page 295</a> |

## ▼ Procédure de redémarrage du serveur de clé RPC sécurisé

### Avant de commencer

Vous devez être dans le rôle root.

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

```
# svcs \*keyserv\*
STATE      STIME      FMRI
disabled Dec_14   svc:/network/rpc/keyserv
```

- 2 Activez le service du serveur de clés si le service n'est pas en ligne.

```
# svcadm enable network/rpc/keyserv
```

## ▼ Procédure de configuration d'une clé Diffie-Hellman pour un hôte NIS

Cette procédure doit être effectuée sur chaque hôte du domaine NIS.

### Avant de commencer

Vous devez être dans le rôle root.

- 1 Si le service de noms par défaut n'est pas NIS, ajoutez-y la carte `publickey`.

- a. Vérifiez que la valeur de `config/default` pour le service de noms n'est pas `nis`.

```
# svccfg -s name-service/switch listprop config
config                                application
config/value_authorization           astring      solaris.smf.value.name-service.switch
config/default                        astring      files
config/host                           astring      "files nis dns"
config/printer                        astring      "user files nis"
```

Si la valeur de `config/default` est `nis`, vous pouvez arrêter ici.

- b. Définissez le service de noms pour `publickey` sur `nis`.

```
# svccfg
# svccfg -s name-service/switch setprop config/publickey = astring: "nis"
# svccfg -s name-service/switch:default refresh
```

- c. Confirmez la valeur de `publickey`.

```
# svccfg
# svccfg -s name-service/switch listprop
config                                application
config/value_authorization           astring      solaris.smf.value.name-service.switch
config/default                        astring      files
config/host                           astring      "files nis dns"
config/printer                        astring      "user files nis"
config/publickey                      astring      nis
```

Sur ce système, la valeur de `publickey` est répertoriée, car elle est différente de la valeur par défaut, `files`.

## 2 Créez une nouvelle paire de clés à l'aide de la commande `newkey`.

```
# newkey -h hostname
```

où *hostname* est le nom du client.

### Exemple 14–1 Configuration d'une nouvelle clé pour root sur un client NIS

Dans l'exemple ci-dessous, `earth` est configuré en tant que client NIS sécurisé. L'administrateur se voit attribuer le profil de droits Name Service Security (sécurité du service de noms).

```
# newkey -h earth
Adding new key for unix.earth@example.com
New Password:      <Type password>
Retype password:   <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

## ▼ Procédure de configuration d'une clé Diffie-Hellman pour un utilisateur NIS

Cette procédure doit être effectuée sur chaque utilisateur du domaine NIS.

### Avant de commencer

Seuls les administrateurs système, lorsqu'ils sont connectés au serveur maître NIS, peuvent générer une nouvelle clé pour un utilisateur. Le profil de droits Name Service Security (sécurité du service de noms) doit avoir été attribué aux administrateurs.

## 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

## 2 Créez une nouvelle clé pour un utilisateur.

```
# newkey -u username
```

où *username* correspond au nom de l'utilisateur. Le système vous invite à saisir un mot de passe. Vous pouvez saisir un mot de passe générique. La clé privée est stockée sous forme chiffrée à l'aide du mot de passe générique.

## 3 Indiquez à l'utilisateur de se connecter et de saisir la commande `chkey -p`.

Cette commande permet aux utilisateurs de re-chiffrer leurs clés privées avec un mot de passe uniquement connu de l'utilisateur.

---

**Remarque** – La commande `chkey` peut être utilisée pour créer une nouvelle paire de clés pour un utilisateur.

---

### Exemple 14–2 Configuration et chiffrement d'une nouvelle clé utilisateur dans NIS

Dans cet exemple, le superutilisateur définit la clé.

```
# newkey -u jdoe
Adding new key for unix.12345@example.com
New Password:      <Type password>
Retype password:   <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

L'utilisateur `jdoe` re-chiffre la clé à l'aide d'un mot de passe privé.

```
% chkey -p
Updating nis publickey database.
Reencrypting key for unix.12345@example.com
Please enter the Secure-RPC password for jdoe:  <Type password>
Please enter the login password for jdoe:      <Type password>
Sending key change request to centralexample...
```

## ▼ Procédure de partage de fichiers NFS avec l'authentification Diffie-Hellman

Cette procédure protège les systèmes de fichiers partagés sur un serveur NFS en requérant l'authentification pour l'accès.

#### Avant de commencer

L'authentification par clé publique Diffie-Hellman doit être activée sur le réseau. Pour activer l'authentification sur le réseau, effectuez la procédure [“Procédure de configuration d'une clé Diffie-Hellman pour un hôte NIS”](#) à la page 293.

Le profil de droits System Management (gestion du système) doit vous avoir été attribué pour effectuer cette tâche.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Sur le serveur NFS, partagez un système de fichiers avec l'authentification Diffie-Hellman.

```
# share -F nfs -o sec=dh /filesystem
```

où *filesystem* est le système de fichiers partagé.

L'option `-o sec=dh` signifie que l'authentification AUTH\_DH est désormais requise pour accéder au système de fichiers.

### 3 Sur un client NFS, montez un système de fichiers avec l'authentification Diffie-Hellman.

```
# mount -F nfs -o sec=dh server:filesystem mount-point
```

*server*                      Nom du système qui partage *filesystem*

*filesystem*                Nom du système de fichiers partagé, tel que `opt`

*mount-point*            Nom du point de montage, tel que `/opt`

L'option `-o sec=dh` permet de monter le système de fichiers avec l'authentification AUTH\_DH.



## Utilisation de PAM

---

Ce chapitre traite de la structure PAM (Pluggable Authentication Module, module d'authentification enfichable). PAM fournit une méthode pour "enficher" des services d'authentification dans le SE Oracle Solaris. PAM permet la prise en charge de plusieurs services d'authentification lors de l'accès à un système.

- "PAM (présentation)" à la page 297
- "PAM (tâches)" à la page 299
- "Configuration PAM (référence)" à la page 302

### PAM (présentation)

La structure PAM (Pluggable Authentication Module, module d'authentification enfichable) permet "d'enficher" de nouveaux services d'authentification sans modifier les services de saisie système tels que `login`, `ftp` et `telnet`. Vous pouvez également utiliser PAM pour intégrer la connexion UNIX à d'autres mécanismes de sécurité tels que Kerberos. Des mécanismes de compte, d'informations d'identification, de session et de gestion des mots de passe peuvent également être "enfichés" grâce à cette structure.

### Avantages de l'utilisation de PAM

La structure PAM permet de configurer l'utilisation des services de saisie système (tels que `ftp`, `login`, `telnet` ou `rsh`) pour authentifier l'utilisateur. La liste ci-dessous répertorie les avantages principaux de PAM :

- Flexibilité de la stratégie de configuration
  - Stratégie d'authentification par application
  - Possibilité de choisir un mécanisme d'authentification par défaut
  - Possibilité de demander plusieurs autorisations sur les systèmes haute sécurité
- Facilité d'utilisation pour l'utilisateur final

- Pas de nouvelle saisie des mots de passe s'ils ne varient pas d'un service d'authentification à l'autre
- Possibilité d'inviter l'utilisateur à saisir des mots de passe pour plusieurs services d'authentification sans qu'il ait à taper plusieurs commandes
- Possibilité de transmettre des options facultatives aux services d'authentification des utilisateurs
- Possibilité de mettre en place une stratégie de sécurité spécifique au site sans avoir à modifier les services de saisie système

## Présentation de la structure PAM

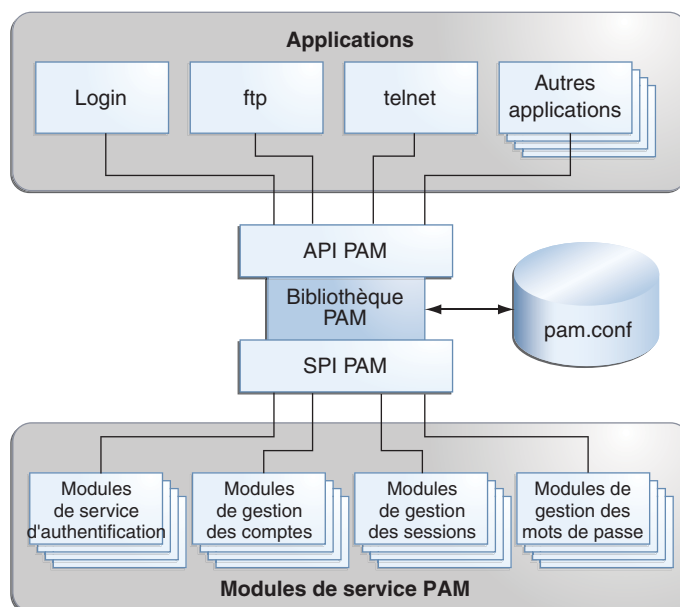
La structure PAM s'organise autour de quatre composants :

- Consommateurs PAM
- Bibliothèque PAM
- Fichier de configuration [pam.conf\(4\)](#)
- Modules de service PAM, également appelés fournisseurs

La structure permet d'uniformiser les activités liées à l'authentification. Cette approche permet aux développeurs d'applications d'utiliser les services PAM sans connaissance préalable de la sémantique de la stratégie. Les algorithmes sont fournis de manière centralisée. Ils peuvent être modifiés indépendamment de chaque application. Grâce à PAM, les administrateurs peuvent adapter le processus d'authentification aux besoins d'un système particulier sans avoir à modifier aucune application. Les ajustements sont effectués par le biais du fichier de configuration PAM `pam.conf`.

La figure ci-dessous illustre l'architecture PAM. Les applications communiquent avec la bibliothèque PAM par l'intermédiaire de l'API (Application Programming Interface, interface de programmation d'application) PAM. Les modules PAM communiquent avec la bibliothèque PAM par l'intermédiaire de la SPI (Service Provider Interface, interface de fournisseur de services) PAM. Ainsi, la bibliothèque PAM permet aux applications et modules de communiquer entre eux.

FIGURE 15-1 Architecture PAM



## Modifications apportées à la structure des modules PAM pour cette version

La structure PAM pour la version Oracle Solaris 11 Express inclut un nouveau module `pam_allow`. Le module peut être utilisé pour accorder l'accès à tous les utilisateurs, sans imposer de sécurité. Le module doit être utilisé avec précaution. Pour plus d'informations, reportez-vous à la page de manuel [pam\\_allow\(5\)](#).

## PAM (tâches)

Cette section examine certaines tâches qui peuvent être nécessaires pour que la structure PAM utilise une stratégie de sécurité spécifique. Sachez que certains problèmes de sécurité sont associés au fichier de configuration PAM. Pour plus d'informations sur les problèmes de sécurité, reportez-vous à la section [“Planification de la mise en oeuvre PAM”](#) à la page 300.

## PAM (liste des tâches)

| Tâche                                           | Description                                                                                                                                                                                                       | Voir                                                                                                             |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Planification de l'installation PAM             | Avant de procéder à la configuration du logiciel, vous devez examiner les problèmes qu'elle risque de poser et prendre les décisions qui s'imposent.                                                              | <a href="#">“Planification de la mise en oeuvre PAM” à la page 300</a>                                           |
| Ajout de nouveaux modules PAM                   | Parfois, des modules spécifiques au site doivent être écrits et installés en fonction d'exigences qui ne relèvent pas du logiciel générique. Cette procédure explique comment installer ces nouveaux modules PAM. | <a href="#">“Procédure d'ajout d'un module PAM” à la page 301</a>                                                |
| Blocage de l'accès via <code>~/ .rhosts</code>  | Renforcez la sécurité en interdisant l'accès via <code>~/ .rhosts</code> .                                                                                                                                        | <a href="#">“Procédure d'interdiction de l'accès rhost à partir de systèmes distants avec PAM” à la page 302</a> |
| Initialisation de la journalisation des erreurs | Démarrez la journalisation des messages d'erreur PAM via <code>syslog</code> .                                                                                                                                    | <a href="#">“Procédure de journalisation de rapports d'erreur PAM” à la page 302</a>                             |

## Planification de la mise en oeuvre PAM

Tel qu'il est livré, le fichier de configuration `pam.conf` met en oeuvre la stratégie de sécurité standard. Cette stratégie doit fonctionner dans de nombreuses situations. Si vous avez besoin d'appliquer une stratégie de sécurité différente, prenez en compte les points suivants :

- Identifiez vos besoins, en particulier les modules de service PAM que vous devez sélectionner.
- Identifiez les services qui nécessitent une configuration spéciale. Utilisez `other`, si nécessaire.
- Décidez de l'ordre d'exécution des modules.
- Sélectionnez l'indicateur de contrôle pour chaque module. Pour plus d'informations sur tous les indicateurs de contrôle, reportez-vous à la section [“Fonctionnement de la superposition PAM” à la page 303](#).
- Choisissez les options nécessaires pour chaque module. La page de manuel pour chaque module doit répertorier toutes les options spéciales.

Voici quelques suggestions à prendre en compte avant de modifier le fichier de configuration PAM :

- Utilisez les entrées `other` pour chaque type de module afin de ne pas devoir inclure chaque application dans le fichier `/etc/pam.conf`.
- Veillez à prendre en compte les implications en matière de sécurité des indicateurs de contrôle `bind`, `sufficient` et `optional`.

- Prenez connaissance des pages de manuel associées aux modules. Elles peuvent vous aider à mieux comprendre le fonctionnement de chaque module, la disponibilité des options et les interactions entre modules empilés.



**Attention** – Si le fichier de configuration PAM est mal configuré ou corrompu, aucun utilisateur n'est en mesure de se connecter. Etant donné que la commande `su login` n'utilise pas PAM, le mot de passe root est alors nécessaire pour initialiser la machine en mode monutilisateur et résoudre le problème.

Une fois le fichier `/etc/pam.conf` modifié, révisiez-le autant que possible tant que votre accès au système vous permet de résoudre les problèmes. Testez toutes les commandes sur lesquelles vos modifications ont peut-être eu une incidence. Si vous ajoutez par exemple un module au service `telnet`, vous devez utiliser la commande `telnet` et vérifier que le service se comporte comme attendu, suite à vos modifications.

## ▼ Procédure d'ajout d'un module PAM

Cette procédure indique comment ajouter un nouveau module PAM. Vous pouvez créer des modules pour prendre en charge des applications tierces ou des stratégies de sécurité spécifiques à votre site.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

### 2 Déterminez les indicateurs de contrôle et les autres options à utiliser.

Pour plus d'informations sur les indicateurs de contrôle, reportez-vous à la section [“Fonctionnement de la superposition PAM”](#) à la page 303.

### 3 Assurez-vous que la propriété et les autorisations sont définies de telle sorte que le fichier de module appartienne à root et les droits soient 555.

### 4 Modifiez le fichier de configuration PAM, `/etc/pam.conf`, et ajoutez ce module aux services appropriés.

### 5 Vérifiez que le module a été ajouté correctement.

Vous devez réaliser le test *avant* la réinitialisation du système au cas où le fichier de configuration serait mal configuré. Connectez-vous à l'aide d'un service direct, tel que `ssh`, et exécutez la commande `su` avant de réinitialiser le système. Le service peut être un démon généré dynamiquement une seule fois lors de l'initialisation du système. Vous devez ensuite réinitialiser le système avant de vérifier l'ajout du module.

## ▼ Procédure d'interdiction de l'accès rhost à partir de systèmes distants avec PAM

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

### 2 Supprimez toutes les lignes comportant `rhosts_auth.so.1` dans le fichier de configuration PAM.

Cette étape permet d'éviter la lecture des fichiers `~/ .rhosts` au cours d'une session `rlogin`. Par conséquent, elle permet d'empêcher l'accès non authentifié au système local à partir de systèmes distants. Tous les accès `rlogin` requièrent un mot de passe, indépendamment de la présence ou du contenu des fichiers `~/ .rhosts` ou `/etc/hosts.equiv`.

### 3 Désactivez le service `rsh`.

Pour empêcher d'autres accès non authentifiés aux fichiers `~/ .rhosts`, n'oubliez pas de désactiver le service `rsh`.

```
# svcadm disable network/shell
```

## ▼ Procédure de journalisation de rapports d'erreur PAM

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

### 2 Configurez le fichier `/etc/syslog.conf` en fonction du niveau de journalisation dont vous avez besoin.

Pour plus d'informations sur les niveaux de journalisation, reportez-vous à [`syslog.conf\(4\)`](#).

### 3 Actualisez les informations de configuration pour le démon `syslog`.

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

## Configuration PAM (référence)

Le fichier de configuration PAM, [`pam.conf\(4\)`](#), permet de configurer les modules du service PAM pour les services de système `login`, `rlogin`, `su` et `cron`. Il incombe à l'administrateur système de gérer ce fichier. Un ordre d'entrée incorrect dans le fichier `pam.conf` peut entraîner des effets secondaires imprévus. Par exemple, un fichier `pam.conf` mal configuré peut

verrouiller les utilisateurs, de manière que le mode monutilisateur s'impose pour effectuer des réparations. La section [“Fonctionnement de la superposition PAM” à la page 303](#) décrit comment définir l'ordre.

## Syntaxe du fichier de configuration PAM

Le format des entrées du fichier de configuration est le suivant :

*service-name module-type control-flag module-path module-options*

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>service-name</i>   | Nom du service, par exemple, ftp, login ou passwd. Une application peut utiliser différents noms pour les services offerts par l'application. Par exemple, le démon shell sécurisé Oracle Solaris utilise les noms de services suivants : sshd - none, sshd - password, sshd - kbdint, sshd - pubkey et sshd - hostbased. Le nom de service <i>other</i> est un nom prédéfini, utilisé comme nom de service générique. Si aucun nom de service spécifique n'est trouvé dans le fichier de configuration, la configuration pour <i>other</i> est utilisée. |
| <i>module-type</i>    | Type du service, c'est-à-dire auth, account, session ou password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <i>control-flag</i>   | Rôle du module dans la détermination de la valeur intégrée de réussite ou d'échec pour le service. Les indicateurs de contrôle valides sont binding, include, optional, required, requisite et sufficient. Pour plus d'informations sur l'utilisation de ces indicateurs, reportez-vous à la section <a href="#">“Fonctionnement de la superposition PAM” à la page 303</a> .                                                                                                                                                                             |
| <i>module-path</i>    | Chemin d'accès à l'objet de bibliothèque qui met en oeuvre le service. S'il n'est pas absolu, on suppose qu'il est relatif à /usr/lib/security/\$ISA/. Utilisez la macro dépendante de l'architecture \$ISA pour que libpam recherche l'architecture spécifique de l'application dans le répertoire.                                                                                                                                                                                                                                                      |
| <i>module-options</i> | Options transmises aux modules de service. Une page de manuel du module décrit les options acceptées par ce module. nowarn et debug sont deux options de module typiques.                                                                                                                                                                                                                                                                                                                                                                                 |

## Fonctionnement de la superposition PAM

Lorsqu'une application appelle les fonctions suivantes, libpam lit le fichier de configuration /etc/pam.conf pour identifier les modules qui participent à l'opération pour ce service :

- [pam\\_authenticate\(3PAM\)](#)
- [pam\\_acct\\_mgmt\(3PAM\)](#)
- [pam\\_setcred\(3PAM\)](#)
- [pam\\_open\\_session\(3PAM\)](#)

- `pam_close_session(3PAM)`
- `pam_chauthtok(3PAM)`

Si `/etc/pam.conf` ne contient qu'un seul module pour une opération pour ce service (authentification ou gestion de compte, par exemple), le résultat de ce module détermine celui de l'opération. Par exemple, l'opération d'authentification par défaut pour l'application `passwd` contient un module, `pam_passwd_auth.so.1` :

```
passwd auth required pam_passwd_auth.so.1
```

D'autre part, si plusieurs modules sont définis pour l'opération du service, on parle de modules *empilés* et d'une *pile PAM* pour ce service. Par exemple, prenons le cas où `pam.conf` contient les entrées suivantes :

```
login auth requisite pam_authtok_get.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
```

Ces entrées représentent un exemple de pile `auth` pour le service `login`. Pour déterminer le résultat de cette pile, les codes de résultat de chaque module requièrent un *processus d'intégration*. Dans le processus d'intégration, les modules sont exécutés dans l'ordre indiqué par `/etc/pam.conf`. Chaque code de réussite ou d'échec est intégré dans le résultat global en fonction de l'indicateur de contrôle du module. L'indicateur de contrôle peut entraîner la fin anticipée de la pile. Par exemple, un module `requisite` peut échouer, ou un module `sufficient` ou `binding` peut réussir. Une fois la pile traitée, tous les résultats sont regroupés en un résultat global unique, qui est transmis à l'application.

L'indicateur de contrôle précise le rôle joué par le module PAM pour déterminer l'accès au service. Les indicateurs de contrôle ont les effets suivants :

- **Binding** : lorsque les exigences d'un module `binding` (obligatoire) sont satisfaites, la réussite est immédiatement renvoyée à l'application si aucun module `required` précédent n'a échoué. Si ces conditions sont vérifiées, aucun autre module n'est exécuté. En cas d'échec, un échec `required` est enregistré et le traitement des modules se poursuit.
- **Include** : ajoute des lignes d'un autre fichier de configuration PAM à utiliser à ce stade de la pile PAM. Cet indicateur ne contrôle pas les comportements de réussite ni d'échec. Lorsqu'un nouveau fichier est lu, la pile `include` (inclure) PAM est incrémentée. Au terme de la vérification de la pile dans le nouveau fichier, la valeur de la pile `include` est décrémentée. Une fois la fin du fichier atteinte et la valeur de la pile `include` PAM définie sur 0, le traitement de la pile prend fin. La valeur maximale pour la pile `include` PAM est 32.
- **Optional** : il n'est pas nécessaire que les exigences d'un module `optional` (facultatif) soient satisfaites pour que le service puisse être utilisé. En cas d'échec, un échec `optional` est enregistré.



- **Required** : les exigences d'un module required (requis) doivent être satisfaites pour que le service puisse être utilisé. Un échec entraîne le renvoi d'une erreur après l'exécution des modules restants pour ce service. La réussite finale du service n'est renvoyée que si aucun module binding ou required n'a signalé d'échec.
- **Requisite** : les exigences d'un module requisite (indispensable) doivent être satisfaites pour que le service puisse être utilisé. Un échec entraîne le renvoi immédiat d'une erreur et l'arrêt de l'exécution des modules. Tous les modules requisite pour un service doivent renvoyer un résultat positif pour que la fonction puisse renvoyer une réussite à l'application.
- **Sufficient** : si aucun échec required précédent ne s'est produit, la réussite dans un module sufficient (suffisant) renvoie immédiatement un résultat positif à l'application et aucun autre module n'est exécuté. En cas d'échec, un échec optional est enregistré.

Les deux diagrammes suivants indiquent comment l'accès est déterminé lors du processus d'intégration. Le premier diagramme indique comment la réussite ou l'échec sont enregistrés pour chaque type d'indicateur de contrôle. Le second diagramme indique comment la valeur intégrée est déterminée.

FIGURE 15-2 Superposition PAM : effet des indicateurs de contrôle

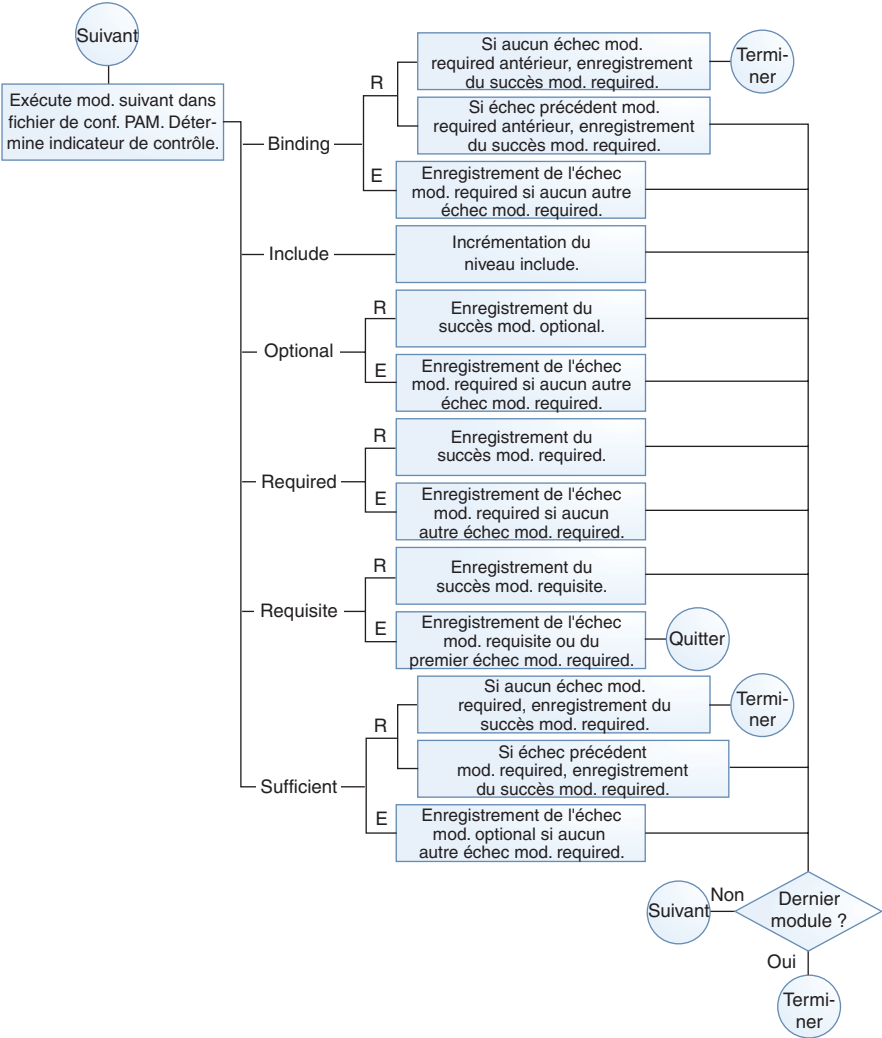
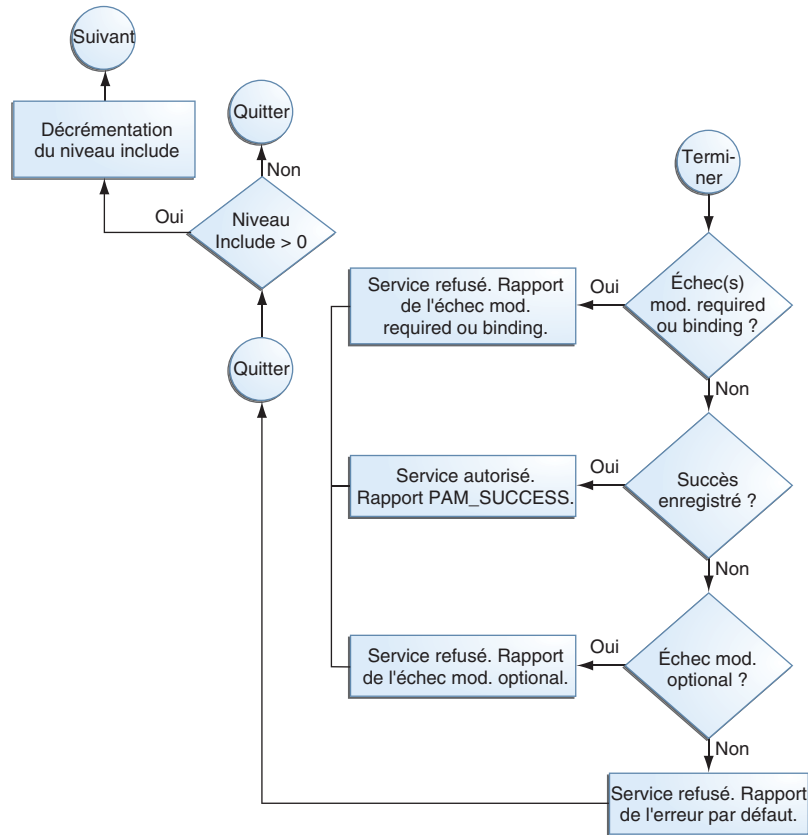


FIGURE 15-3 Superposition PAM : détermination de la valeur intégrée



## Exemple de superposition PAM

Examinez l'exemple suivant d'un service `rlogin` qui demande une authentification.

**EXEMPLE 15-1** Contenu partiel d'un fichier de configuration PAM standard

Le fichier `pam.conf` dans cet exemple comporte les éléments suivants pour les services `rlogin` :

```

# Authentication management
...
# rlogin service
rlogin auth sufficient      pam_rhosts_auth.so.1
rlogin auth requisite       pam_authok_get.so.1
rlogin auth required        pam_dhkeys.so.1
rlogin auth required        pam_unix_auth.so.1
...

```

**EXEMPLE 15-1** Contenu partiel d'un fichier de configuration PAM standard (Suite)

Lorsque le service `rlogin` demande une authentification, `libpam` exécute d'abord le module `pam_rhosts_auth(5)`. L'indicateur de contrôle est défini sur `sufficient` pour le module `pam_rhosts_auth`. Si le module `pam_rhosts_auth` est en mesure d'authentifier l'utilisateur, le traitement s'arrête et la réussite est renvoyée à l'application.

Si le module `pam_rhosts_auth` n'est pas en mesure d'authentifier l'utilisateur, le module PAM suivant, `pam_authtok_get(5)` est exécuté. L'indicateur de contrôle de ce module est défini sur `required`. Si `pam_authtok_get` échoue, le processus d'authentification se termine et l'échec est renvoyé à `rlogin`.

Si `pam_authtok_get` réussit, les deux modules suivants, `pam_dhkeys(5)` et `pam_unix_auth(5)`, sont exécutés. Les indicateurs de contrôle associés des deux modules sont définis sur `required` de sorte que le processus se poursuit même si un échec individuel est renvoyé. Une fois `pam_unix_auth` exécuté, il ne reste plus de modules pour l'authentification `rlogin`. A ce stade, si `pam_dhkeys` ou `pam_unix_auth` a renvoyé un échec, l'accès via `rlogin` est refusé à l'utilisateur.

## Utilisation de SASL

---

Ce chapitre contient des informations sur SASL (Simple Authentication and Security Layer, couche d'authentification et de sécurité simple).

- “SASL (présentation)” à la page 309
- “SASL (référence)” à la page 310

### SASL (présentation)

La couche SASL (Simple Authentication and Security Layer) est une structure fournissant des services d'authentification et de sécurité facultatifs aux protocoles réseau. Une application appelle la bibliothèque SASL, `/usr/lib/libsasl.so`, qui fournit une couche de collage entre l'application et les divers mécanismes SASL. Les mécanismes sont utilisés dans le processus d'authentification et lors de la fourniture de services de sécurité facultatifs. La version de SASL est dérivée de la couche Cyrus SASL avec quelques changements.

SASL fournit les services suivants :

- Chargement de plug-ins
- Détermination des options de sécurité nécessaires dans l'application afin de faciliter le choix d'un mécanisme de sécurité
- Liste des plug-ins disponibles pour l'application
- Choix du meilleur mécanisme dans une liste des mécanismes disponibles pour une tentative d'authentification particulière
- Routage des données d'authentification entre l'application et le mécanisme sélectionné
- Renvoi des informations sur la négociation SASL à l'application

## SASL (référence)

La section suivante fournit des informations sur l'implémentation de SASL.

### Plug-ins SASL

Les plug-ins SASL assurent la prise en charge des mécanismes de sécurité, la normalisation utilisateur et la récupération des propriétés auxiliaires. Par défaut, les plug-ins 32 bits chargés de manière dynamique sont installés dans `/usr/lib/sasl` et les plug-ins 64 bits sont installés dans `/usr/lib/sasl/ $ISA`. Les plug-ins de mécanismes de sécurité suivants sont fournis :

|                             |                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>crammd5.so.1</code>   | CRAM-MD5, qui prend en charge l'authentification uniquement, et non l'autorisation.                                                                                                                          |
| <code>digestmd5.so.1</code> | DIGEST-MD5, qui prend en charge l'authentification, l'intégrité et la confidentialité, ainsi que l'autorisation.                                                                                             |
| <code>gssapi.so.1</code>    | GSSAPI, qui prend en charge l'authentification, l'intégrité et la confidentialité, ainsi que l'autorisation. Le mécanisme de sécurité GSSAPI requiert une infrastructure Kerberos en état de fonctionnement. |
| <code>plain.so.1</code>     | PLAIN, qui prend en charge l'authentification et l'autorisation.                                                                                                                                             |

En outre, les plug-ins de mécanismes de sécurité EXTERNES et les plug-ins de normalisation utilisateur INTERNE sont créés dans `libsasl.so.1`. Le mécanisme EXTERNE prend en charge l'authentification et l'autorisation. Le mécanisme prend en charge l'intégrité et la confidentialité si la source de sécurité externe les fournit. Le plug-in INTERNE ajoute le nom de domaine si nécessaire pour le nom d'utilisateur.

Actuellement, la version d'Oracle Solaris ne fournit aucun plug-in `auxprop`. Pour que les plug-ins de mécanismes CRAM-MD5 et DIGEST-MD5 soient entièrement opérationnels côté serveur, l'utilisateur doit fournir un plug-in `auxprop` pour récupérer des mots de passe en clair. Le plug-in PLAIN (en clair) requiert une prise en charge supplémentaire pour vérifier le mot de passe. La prise en charge de la vérification du mot de passe peut se faire à travers l'un des éléments suivants : un rappel à l'application de serveur, un plug-in `auxprop`, `saslauthd` ou `pwcheck`. Les démons `saslauthd` et `pwcheck` ne sont pas fournis dans les versions Oracle Solaris. Pour une meilleure interopérabilité, limitez les applications de serveur aux mécanismes qui sont entièrement opérationnel en utilisant l'option `SASL mech_list`.

### Variable d'environnement SASL

Par défaut, le nom d'authentification client est défini sur `getenv("LOGNAME")`. Cette variable peut être réinitialisée par le client ou par le plug-in.

## Options SASL

Le comportement de `libsasl` et les plug-ins peuvent être modifiés côté serveur à l'aide d'options pouvant être définies dans le fichier `/etc/sasl/app.conf`. La variable `app` est le nom défini côté serveur pour l'application. La documentation du serveur `app` doit indiquer le nom de l'application.

Les options suivantes sont prises en charge :

|                                |                                                                                                                                                                                                                                                                                        |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>auto_transition</code>   | Effectue la transition automatique de l'utilisateur vers d'autres mécanismes lorsque celui-ci réalise une authentification en texte simple réussie.                                                                                                                                    |
| <code>auxprop_login</code>     | Dresse la liste des noms de plug-ins de propriétés auxiliaires à utiliser.                                                                                                                                                                                                             |
| <code>canon_user_plugin</code> | Sélectionne le plug-in <code>canon_user</code> à utiliser.                                                                                                                                                                                                                             |
| <code>mech_list</code>         | Dresse la liste des mécanismes autorisés à être utilisés par l'application de serveur.                                                                                                                                                                                                 |
| <code>pwcheck_method</code>    | Dresse la liste des mécanismes utilisés pour vérifier les mots de passe. Actuellement, <code>auxprop</code> est la seule valeur autorisée.                                                                                                                                             |
| <code>reauth_timeout</code>    | Définit la durée, en minutes, pendant laquelle les informations d'authentification sont mises en mémoire cache pour une réauthentification rapide. Cette option est utilisée par le plug-in DIGEST-MD5. La définition de cette option sur la valeur 0 désactive la réauthentification. |

Les options suivantes ne sont pas prises en charge :

|                             |                                                                                                                                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>plugin_list</code>    | Dresse la liste des mécanismes disponibles. Non utilisé, car l'option modifie le comportement de chargement dynamique des plug-ins.                                                                                                                                                |
| <code>saslauthd_path</code> | Définit l'emplacement de la porte <code>saslauthd</code> , qui est utilisée pour la communication avec le démon <code>saslauthd</code> . Le démon <code>saslauthd</code> n'est pas inclus dans la version Oracle Solaris. Par conséquent, cette option n'est pas incluse non plus. |
| <code>keytab</code>         | Définit l'emplacement du fichier <code>keytab</code> utilisé par le plug-in GSSAPI. Utilisez à la place la variable d'environnement <code>KRB5_KTNAME</code> pour définir l'emplacement <code>keytab</code> par défaut.                                                            |

Les options suivantes ne figurent pas dans Cyrus SASL. Cependant, elles ont été ajoutées dans la version Oracle Solaris :

|                         |                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>use_authid</code> | Permet d'obtenir les informations d'identification du client plutôt que d'utiliser les informations d'identification par défaut lors de la création du contexte de sécurité client GSS. Par défaut, l'identité Kerberos du client est utilisée. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

`log_level` Définit le niveau souhaité de journalisation d'un serveur.



## Utilisation de Secure Shell (tâches)

---

La fonction Secure Shell d'Oracle Solaris fournit un accès sécurisé à un hôte distant sur un réseau non sécurisé. Le shell fournit des commandes pour une connexion à distance et le transfert de fichier distant. Vous trouverez ci-après une liste des sujets abordés dans ce chapitre.

- “Secure Shell (présentation)” à la page 313
- “Secure Shell et le projet OpenSSH” à la page 316
- “Secure Shell et prise en charge FIPS-140” à la page 317
- “Secure Shell (liste des tâches)” à la page 317

Pour obtenir des informations de référence, reportez-vous au [Chapitre 18, “Secure Shell \(référence\)”](#).

### Secure Shell (présentation)

Avec Secure Shell, l'authentification s'effectue via l'utilisation de mots de passe et/ou de clés publiques. Tout le trafic réseau est chiffré. Par conséquent, Secure Shell empêche tout intrus potentiel de lire une communication interceptée. Secure Shell empêche également un adversaire de mystifier le système.

Secure Shell peut également être utilisé comme un [VPN](#) à la demande. Un VPN peut transmettre le trafic système X Window ou connecter des numéros de port individuels compris entre les machines locales et distantes via un lien réseau crypté.

Avec Secure Shell, vous pouvez effectuer les actions suivantes :

- Se connecter de manière sécurisée à un autre hôte sur un réseau non sécurisé.
- Copier des fichiers en toute sécurité entre les deux hôtes.
- Exécuter des commandes en toute sécurité sur l'hôte distant.

Côté serveur, Secure Shell prend en charge deux versions du protocole SSH, la version 1 (v1) et la version 2. La version 2 (v2) est plus sécurisée. La version 1 de Secure Shell est fournie

uniquement pour aider les utilisateurs qui migrent vers la version v2. Pour plus d'informations sur la version 1, reportez-vous à la section [System Administration Guide: Security Services](#).

## Authentification Secure Shell

Secure Shell fournit des méthodes de clé publique et mot de passe pour l'authentification de la connexion à l'hôte distant. L'authentification avec clé publique est un mécanisme d'authentification plus fiable que l'authentification par mot de passe, car la clé privée ne se déplace pas sur le réseau.

Les méthodes d'authentification sont tentées dans l'ordre suivant. Lorsque la configuration ne satisfait pas à une méthode d'authentification, la méthode suivante est tentée.

- **GSS-API** : utilise les informations d'authentification des mécanismes GSS-API tels que `mech_krb5` (Kerberos V) et `mech_dh` (AUTH\_DH) pour authentifier les clients et serveurs. Pour plus d'informations sur GSS-API, reportez-vous à la section “[Introduction to GSS-API](#)” du manuel *Developer's Guide to Oracle Solaris 11 Security*.
- **Authentification basée sur l'hôte** : utilise les clés d'hôte et les fichiers rhosts. Utilise les clés d'hôte privées/publiques RSA et DSA du client pour authentifier ce dernier. Utilise les fichiers rhosts pour autoriser les clients à des utilisateurs.
- **Authentification avec clé publique** : authentifie les utilisateurs avec leurs clés publiques et privées RSA et DSA.
- **Authentification du mot de passe** : utilise PAM pour authentifier les utilisateurs. La méthode d'authentification du clavier dans v2 permet l'invitation arbitraire par PAM. Pour plus d'informations, reportez-vous à la section SECURITY de la page de manuel [sshd\(1M\)](#).

Le tableau suivant répertorie les conditions requises pour l'authentification d'un utilisateur essayant de se connecter à un hôte distant. L'utilisateur est sur l'hôte local, le client. L'hôte distant, le serveur, exécute le démon `sshd`. Le tableau présente les méthodes d'authentification Secure Shell, les versions de protocole compatibles et les exigences de l'hôte.

TABLEAU 17-1 Méthodes d'authentification pour Secure Shell

| Méthode d'authentification | Exigences de l'hôte local (client)                                   | Exigences de l'hôte distant (serveur)                                                                                                                                                                                         |
|----------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GSS-API                    | Informations d'identification de l'initiateur pour le mécanisme GSS. | Informations d'identification de l'accepteur pour le mécanisme GSS. Pour plus d'informations, reportez-vous à la section “ <a href="#">Acquisition d'informations d'identification GSS dans Secure Shell</a> ” à la page 334. |

TABLEAU 17-1 Méthodes d'authentification pour Secure Shell (Suite)

| Méthode d'authentification                            | Exigences de l'hôte local (client)                                                                                                                                            | Exigences de l'hôte distant (serveur)                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basée sur l'hôte                                      | Compte utilisateur<br>Clé privée de l'hôte local dans<br>/etc/ssh/ssh_host_rsa_key ou<br>/etc/ssh/ssh_host_dsa_key<br>HostbasedAuthentication yes dans<br>/etc/ssh/ssh_config | Compte utilisateur<br>Clé privée de l'hôte local dans<br>/etc/ssh/known_hosts ou ~/.ssh/known_hosts<br>HostbasedAuthentication yes dans<br>/etc/ssh/sshd_config<br>IgnoreRhosts no dans /etc/ssh/sshd_config<br>Entrée d'hôte local dans /etc/ssh/shosts.equiv,<br>/etc/hosts.equiv, ~/.rhosts ou ~/.shosts |
| Clé publique RSA ou DSA                               | Compte utilisateur<br>Clé privée dans ~/.ssh/id_rsa ou ~/.ssh/id_dsa<br>Clé publique d'utilisateur dans ~/.ssh/id_rsa.pub<br>ou ~/.ssh/id_dsa.pub                             | Compte utilisateur<br>Clé publique d'utilisateur en<br>~/.ssh/authorized_keys                                                                                                                                                                                                                               |
| Basée sur mot de passe                                | Compte utilisateur                                                                                                                                                            | Compte utilisateur<br>Prend en charge PAM.                                                                                                                                                                                                                                                                  |
| .rhosts avec RSA (v1)<br>sur le serveur<br>uniquement | Compte utilisateur<br>Clé publique de l'hôte local dans<br>/etc/ssh/ssh_host_rsa1_key                                                                                         | Compte utilisateur<br>Clé publique de l'hôte local dans<br>/etc/ssh/ssh_known_hosts ou<br>~/.ssh/known_hosts<br>IgnoreRhosts no dans /etc/ssh/sshd_config<br>Entrée d'hôte local dans /etc/ssh/shosts.equiv,<br>/etc/hosts.equiv, ~/.shosts ou ~/.rhosts                                                    |

## Secure Shell dans l'entreprise

Pour obtenir des informations complètes sur la fonction Secure Shell sur un système Oracle Solaris, reportez-vous à l'ouvrage *Secure Shell in the Enterprise*, de Jason Reid, ISBN 0-13-142900-0, Juin 2003. Ce manuel fait partie de la série Sun BluePrints publiée par Sun Microsystems Press.

## Secure Shell et le projet OpenSSH

La fonction Secure Shell est un fork du projet [OpenSSH \(http://www.openssh.com\)](http://www.openssh.com). Les correctifs de sécurité pour la correction des vulnérabilités découvertes dans les versions ultérieures d'OpenSSH sont intégrés à Secure Shell, tout comme des corrections de bogues et des fonctions. Le développement interne se poursuit sur le fork Secure Shell.

Les fonctionnalités suivantes sont mises en oeuvre pour le protocole v2 dans cette version de Secure Shell :

- **Mot-clé ForceCommand** : force l'exécution de la commande spécifiée indépendamment de ce que l'utilisateur tape sur la ligne de commande. Ce mot-clé est très utile à l'intérieur d'un bloc Match. Cette option de configuration `sshd_config` est semblable à l'option `command="..."` dans `$HOME/.ssh/authorized_keys`.
- **AES-128**, protection par phrase de passe : dans cette version, les clés privées qui sont générées par la commande `ssh-keygen` sont protégées avec l'algorithme AES-128. Cet algorithme protège les clés qui viennent d'être générées et les clés rechiffrées, comme par exemple lorsqu'une phrase de passe est modifiée.
- **Option -u de la commande sftp-server** : permet à aux utilisateurs de définir explicitement un umask sur des fichiers et des répertoires. Cette option remplace la valeur umask par défaut de l'utilisateur. Pour voir un exemple, reportez-vous à la description de Subsystem à la page de manuel [sshd\\_config\(4\)](#).
- **Mots-clés supplémentaires pour les blocs Match** : `AuthorizedKeysFile`, `ForceCommand`, et `HostbasedUsesNameFromPacketOnly` sont pris en charge à l'intérieur des blocs Match. Par défaut, la valeur de `AuthorizedKeysFile` est `$HOME/.ssh/authorized_keys` et celle de `HostbasedUsesNameFromPacketOnly` est `no`. Pour utiliser les blocs Match, reportez-vous à la section "[Procédure de création d'exceptions d'utilisateur et d'hôte SSH aux valeurs par défaut du système](#)" à la page 321.

En plus des corrections de bogues dans le projet, les ingénieurs d'Oracle Solaris ont également intégré les fonctionnalités Oracle Solaris suivantes dans le fork de Secure Shell :

- **PAM** : Secure Shell utilise PAM. L'option de configuration `UsePAM` OpenSSH n'est pas prise en charge.
- **Séparation des privilèges** : Secure Shell n'utilise pas le code de séparation des privilèges du projet OpenSSH. Secure Shell sépare le traitement de l'audit, de la conservation des enregistrements et de la re-saisie du traitement des protocoles de session.

Le code de séparation des privilèges Secure Shell est toujours actif et ne peut pas être désactivé. L'option OpenSSH `UsePrivilegeSeparation` n'est pas prise en charge.

- **Environnement linguistique** : Secure Shell prend entièrement en charge les langues négociées dans RFC 4253, *Secure Shell Transfer Protocol*. Une fois que l'utilisateur se connecte, le shell de connexion de l'utilisateur peut remplacer les paramètres régionaux négociés avec Secure Shell.

- **Audit** : Secure Shell est totalement intégré au service d'audit Solaris. Pour plus d'informations sur le service d'audit, reportez-vous à la [Partie VII](#).
- **Prise en charge GSS-API** : GSS-API peut être utilisé pour l'authentification des utilisateurs *et* pour l'échange de clé initiale. La fonction GSS-API est définie dans RFC4462, *Generic Security Service Application Program Interface*.
- **Commandes proxy** : Secure Shell fournit les commandes de proxy pour les protocoles SOCKS5 et HTTP. Pour consulter un exemple, reportez-vous à la section “[Procédure de configuration de connexions par défaut à des hôtes en dehors du pare-feu](#)” à la page 330.

Dans les versions Oracle Solaris, &SSH resynchronise l'indicateur de compatibilité `SSH_OLD_FORWARD_ADDR` à partir du projet OpenSSH. A partir de mars 2011, la version Secure Shell est 1.5.

## Secure Shell et prise en charge FIPS-140

Lorsque vous utilisez une carte Sun Crypto Accelerator 6000 pour les opérations Secure Shell, Secure Shell s'exécute avec la prise en charge FIPS-140 au niveau 3. Le matériel de niveau 3 est certifié pour résister au sabotage physique, utiliser l'authentification basée sur l'identité et isoler les interfaces qui gèrent les paramètres de sécurité critique à partir des autres interfaces du matériel.

## Secure Shell (liste des tâches)

La liste des tâches suivante fournit des liens vers les tâches de configuration Secure Shell et d'utilisation de la fonction Secure Shell dans Oracle Solaris.

| Tâche                         | Description                                                                                       | Voir                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Configuration de Secure Shell | Guide les administrateurs tout au long de la configuration de Secure Shell pour les utilisateurs. | <a href="#">“Configuration de Secure Shell (liste des tâches)”</a> à la page 318 |
| Utilisation de Secure Shell   | Aide les utilisateurs à utiliser Secure Shell.                                                    | <a href="#">“Utilisation de Secure Shell (liste des tâches)”</a> à la page 322   |

# Configuration de Secure Shell (tâches)

Par défaut, l'authentification basée sur l'hôte et l'utilisation des deux protocoles ne sont pas activées dans Secure Shell. La modification de ces valeurs par défaut nécessite une intervention de l'administrateur. L'administrateur doit également intervenir pour que le transfert de port de fonctionne.

## Configuration de Secure Shell (liste des tâches)

La liste des tâches suivante présente les procédures de configuration de Secure Shell.

| Tâche                                                           | Description                                                                                                                                       | Voir                                                                                                                             |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Configuration de l'authentification basée sur l'hôte.           | Configure l'authentification basée sur l'hôte sur le serveur et sur le client.                                                                    | <a href="#">“Procédure de configuration de l'authentification basée sur l'hôte pour Secure Shell” à la page 318</a>              |
| Configuration du transfert de port.                             | Permet aux utilisateurs d'utiliser le transfert de port.                                                                                          | <a href="#">“Procédure de configuration du transfert de port dans Secure Shell” à la page 321</a>                                |
| Configure des exceptions aux valeurs par défaut du système SSH. | Pour les utilisateurs, les hôtes, les groupes et les adresses, spécifie les paramètres SSH qui sont différents des valeurs par défaut du système. | <a href="#">“Procédure de création d'exceptions d'utilisateur et d'hôte SSH aux valeurs par défaut du système” à la page 321</a> |

### ▼ Procédure de configuration de l'authentification basée sur l'hôte pour Secure Shell

La procédure suivante définit un système de clé publique où la clé publique du client est utilisée pour l'authentification sur le serveur. L'utilisateur doit également créer une paire de clés publiques ou privées.

Dans cette procédure, les termes *client* et *hôte local* désignent la machine sur laquelle un utilisateur saisit la commande ssh. Les termes *serveur* et *hôte distant* désignent la machine que le client tente d'atteindre.

**Avant de commencer**

Vous devez être dans le rôle root.

**1 Sur le client, activez l'authentification basée sur l'hôte.**

Dans le fichier de configuration du client, `/etc/ssh/ssh_config`, tapez l'entrée suivante :

`HostbasedAuthentication yes`

Pour connaître la syntaxe du fichier de configuration, reportez-vous à la page de manuel

[ssh\\_config\(4\)](#)

**2 Sur le serveur, activez l'authentification basée sur l'hôte.**

Dans le fichier de configuration du serveur, `/etc/ssh/sshd_config`, saisissez la même entrée :  
`HostbasedAuthentication yes`

Pour connaître la syntaxe du fichier de configuration, reportez-vous à la page de manuel [sshd\\_config\(4\)](#)

**3 Sur le serveur, vous devez configurer un fichier qui permet au client d'être reconnu en tant qu'hôte de confiance.**

Pour plus d'informations, reportez-vous à la section FILES de la page de manuel [sshd\(1M\)](#).

- **Ajoutez le client sous la forme d'une entrée pour le fichier `/etc/ssh/shosts.equiv` du serveur.**

*client-host*

- **Ou bien, vous pouvez demander aux utilisateurs d'ajouter une entrée pour le client dans leur fichier `~/.shosts` sur le serveur.**

*client-host*

**4 Sur le serveur, vérifiez que le démon `sshd` peut accéder à la liste des hôtes de confiance.**

Définissez `IgnoreRhosts` sur `no` dans le fichier `/etc/ssh/sshd_config`.

```
## sshd_config
IgnoreRhosts no
```

**5 Assurez-vous que les utilisateurs de Secure Shell sur votre site possèdent des comptes sur les deux hôtes.****6 Procédez de l'une des manières suivantes pour placer la clé publique du client sur le serveur.**

- **Modifiez le fichier `sshd_config` sur le serveur, puis demandez à vos utilisateurs d'ajouter les clés d'hôte publiques du client à leur fichier `~/.ssh/known_hosts`.**

```
## sshd_config
IgnoreUserKnownHosts no
```

Pour des instructions d'utilisation, reportez-vous à la section “[Procédure de génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell](#)” à la page 323.

- **Copiez la clé publique du client sur le serveur.**

Les clés d'hôte sont stockées dans le répertoire `/etc/ssh`. Ces clés sont généralement générées par le démon `sshd` à la première initialisation.

**a. Ajoutez la clé au fichier `/etc/ssh/ssh_known_hosts` sur le serveur.**

Sur le client, saisissez la commande sur une seule ligne, sans barre oblique inverse.

```
# cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> /etc/ssh/ssh_known_hosts && echo "Host key copied"'
```

**b. Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.**

Lorsque le fichier est copié, le message "Host key copied" (Clé d'hôte copiée) s'affiche.

Chaque ligne du fichier `/etc/ssh/ssh_known_hosts` se compose de champs séparés par des espaces :

*hostnames algorithm-name publickey comment*

**c. Modifiez le fichier `/etc/ssh/ssh_known_hosts` et ajoutez *RemoteHost* comme premier champ de l'entrée copiée.**

```
## /etc/ssh/ssh_known_hosts File
RemoteHost <copied entry>
```

**Exemple 17-1 Configuration de l'authentification basée sur l'hôte**

Dans l'exemple ci-dessous, chaque hôte est configuré en tant que serveur et en tant que client. Un utilisateur de l'un ou l'autre hôte peut lancer une connexion `ssh` à l'autre hôte. La configuration suivante convertit chaque hôte en serveur et client :

- Sur chaque hôte, les fichiers de configuration Secure Shell contiennent les entrées suivantes :

```
## /etc/ssh/ssh_config
HostBasedAuthentication yes
#
## /etc/ssh/sshd_config
HostBasedAuthentication yes
IgnoreRhosts no
```

- Sur chaque hôte, le fichier `shosts.equiv` contient une entrée pour l'autre hôte :

```
## /etc/ssh/shosts.equiv on machine2
machine1

## /etc/ssh/shosts.equiv on machine1
machine2
```

- La clé publique pour chaque hôte est dans le fichier `/etc/ssh/ssh_known_hosts` sur l'autre hôte :

```
## /etc/ssh/ssh_known_hosts on machine2
... machine1

## /etc/ssh/ssh_known_hosts on machine1
... machine2
```

- Les utilisateurs ont un compte sur les deux hôtes :

```
## /etc/passwd on machine1
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh

## /etc/passwd on machine2
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh
```



## ▼ Procédure de configuration du transfert de port dans Secure Shell

Le transfert de port permet à un port local d'être transmis à un hôte distant. En réalité, un socket est alloué pour écouter le port côté local. De la même façon, un port peut être spécifié côté distant.

---

**Remarque** – Le transfert de port Secure Shell doit utiliser des connexions TCP. Secure Shell ne prend pas en charge les connexions UDP pour le transfert de port.

---

### Avant de commencer

Vous devez être dans le rôle root.

#### 1 Configurez une définition Secure Shell sur le serveur distant pour autoriser le transfert de port.

Définissez la valeur de `AllowTcpForwarding` sur `yes` dans le fichier `/etc/ssh/sshd_config`.

```
# Port forwarding
AllowTcpForwarding yes
```

#### 2 Redémarrez le service Secure Shell.

```
remoteHost# svcadm restart network/ssh:default
```

Pour plus d'informations sur la gestion des services persistants, reportez-vous au [Chapitre 6, "Gestion des services \(présentation\)"](#) du manuel *Administration d'Oracle Solaris : Tâches courantes* et à la page de manuel [svcadm\(1M\)](#).

#### 3 Vérifiez que le transfert de port peut être utilisé.

```
remoteHost# /usr/bin/pgrep -lf sshd
1296 ssh -L 2001:remoteHost:23 remoteHost
```

## ▼ Procédure de création d'exceptions d'utilisateur et d'hôte SSH aux valeurs par défaut du système

Cette procédure permet d'ajouter un bloc `Match` conditionnel après la section globale du fichier `/etc/ssh/sshd_config`. Les paires de valeurs de mot clé qui suivent le bloc `Match` spécifient des exceptions pour l'utilisateur, le groupe, l'hôte ou l'adresse spécifié comme la correspondance.

### Avant de commencer

Vous devez être dans le rôle root.

#### 1 Modifiez le fichier `sshd_config`.

#### 2 Configurez un utilisateur, un groupe, un hôte ou une adresse pour qu'ils utilisent d'autres paramètres de mot-clé SSH que les paramètres par défaut.

Placez les blocs `Match` après les paramètres globaux.

**Remarque** – La section globale du fichier peut ou ne peut pas afficher la liste des paramètres par défaut. Pour les valeurs par défaut, reportez-vous à la page de manuel [sshd\\_config\(4\)](#).

Vous avez peut-être les utilisateurs qui ne devraient pas être autorisés à utiliser le transfert TCP. Dans l'exemple ci-dessous, tout utilisateur dans le groupe public et tout nom d'utilisateur commençant par test ne peut pas utiliser le transfert TCP :

```
## sshd_config file
## Global settings

# Example (reflects default settings):
#
# Host *
#   ForwardAgent no
#   ForwardX11 no
#   PubkeyAuthentication yes
#   PasswordAuthentication yes
#   FallBackToRsh no
#   UseRsh no
#   BatchMode no
#   CheckHostIP yes
#   StrictHostKeyChecking ask
#   EscapeChar ~
Match Group public
  AllowTcpForwarding no
Match User test*
  AllowTcpForwarding no
```

Pour connaître la syntaxe du bloc Match, reportez-vous à la page de manuel [sshd\\_config\(4\)](#).

# Utilisation de Secure Shell (tâches)

Secure Shell fournit un accès sécurisé entre un shell local et un shell distant. Pour plus d'informations, reportez-vous aux pages de manuel [ssh\\_config\(4\)](#) et [ssh\(1\)](#).

## Utilisation de Secure Shell (liste des tâches)

La liste des tâches suivante présente les procédures d'utilisation de Secure Shell.

| Tâche                                        | Description                                                                                          | Voir                                                                                                          |
|----------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Création d'une paire de clés publique/privée | Permet l'accès à Secure Shell pour des sites qui nécessitent une authentification avec clé publique. | "Procédure de génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell" à la page 323 |

| Tâche                                                                                                     | Description                                                                                                                                                 | Voir                                                                                                  |
|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Modification de votre phrase de passe                                                                     | Change la phrase qui authentifie votre clé privée.                                                                                                          | “Procédure de modification de la phrase de passe pour une clé privée Secure Shell” à la page 325      |
| Connexion par le biais de Secure Shell                                                                    | Permet la communication chiffrée Secure Shell lors d'une connexion à distance. Le processus est similaire à l'utilisation de la commande <code>rsh</code> . | “Procédure de connexion à un hôte distant avec Secure Shell” à la page 325                            |
| Connexion à Secure Shell sans mot de passe                                                                | Permet la connexion par le biais d'un agent qui fournit votre mot de passe à Secure Shell.                                                                  | “Procédure de réduction des invites de mot de passe dans Secure Shell” à la page 327                  |
| Utilisation du transfert de port dans Secure Shell                                                        | Spécifie un port local ou un port distant à utiliser pour les connexions Secure Shell via TCP.                                                              | “Procédure d'utilisation du transfert de port dans Secure Shell” à la page 328                        |
| Copie de fichiers avec Secure Shell                                                                       | Copie les fichiers d'un hôte à l'autre en toute sécurité.                                                                                                   | “Procédure de copie de fichiers avec Secure Shell” à la page 329                                      |
| Connexion sécurisée à partir d'un hôte à l'intérieur d'un pare-feu sur un hôte à l'extérieur du pare-feu. | Utilise les commandes Secure Shell compatibles avec le protocole HTTP ou SOCKS5 pour connecter les hôtes séparés par un pare-feu.                           | “Procédure de configuration de connexions par défaut à des hôtes en dehors du pare-feu” à la page 330 |

## ▼ Procédure de génération d'une paire de clés publiques ou privées à utiliser avec Secure Shell

Les utilisateurs doivent générer une paire de clés publiques ou privées lorsque leur site met en oeuvre l'authentification basée sur l'hôte ou l'authentification avec clé publique de l'utilisateur. Pour plus d'options, reportez-vous à la page de manuel [ssh-keygen\(1\)](#).

### Avant de commencer

Vérifiez auprès de votre administrateur système si l'authentification basée sur l'hôte est configurée.

#### 1 Démarrez le programme de génération de clés.

```
myLocalHost% ssh-keygen -t rsa
Generating public/private rsa key pair.
...
```

Où `-t` est le type d'algorithme, `rsa`, `dsa`, ou `rsa1`.

#### 2 Spécifiez le chemin vers le fichier qui contiendra la clé.

Par défaut, le nom de fichier `id_rsa`, qui représente une clé RSA v2, s'affiche entre parenthèses. Vous pouvez sélectionner ce fichier en appuyant sur la touche Retour. Ou bien, vous pouvez taper un autre nom de fichier.

Enter file in which to save the key (/home/jdoe/.ssh/id\_rsa): *<Press Return>*

Le nom de fichier de la clé publique est créé automatiquement par l'ajout de la chaîne `.pub` au nom du fichier de clés privées.

### 3 Entrez une phrase de passe pour utiliser votre clé.

Cette phrase de passe est utilisée pour chiffrer votre clé privée. Une entrée nulle est *fortement déconseillée*. Notez que la phrase de passe ne s'affiche pas lorsque vous la saisissez.

Enter passphrase (empty for no passphrase): *<Type passphrase>*

### 4 Entrez de nouveau la phrase de passe pour la confirmer.

Enter same passphrase again: *<Type passphrase>*

Your identification has been saved in `/home/jdoe/.ssh/id_rsa`.

Your public key has been saved in `/home/jdoe/.ssh/id_rsa.pub`.

The key fingerprint is:

`0e:fb:3d:57:71:73:bf:58:b8:eb:f3:a3:aa:df:e0:d1 jdoe@myLocalHost`

### 5 Vérifiez les résultats.

Vérifiez que le chemin d'accès au fichier de la clé est correct.

```
% ls ~/.ssh
id_rsa
id_rsa.pub
```

A ce stade, vous avez créé une paire de clés publiques ou privées.

### 6 Choisissez l'option appropriée :

- Si votre administrateur a configuré l'authentification basée sur l'hôte, vous pouvez être amené à copier la clé publique de l'hôte local sur l'hôte distant.

Vous pouvez maintenant vous connecter à l'hôte distant. Pour plus de détails, reportez-vous à la section [“Procédure de connexion à un hôte distant avec Secure Shell”](#) à la page 325.

#### a. Saisissez la commande sur une seule ligne, sans barre oblique inverse.

```
% cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> ~/.ssh/known_hosts && echo "Host key copied"'
```

#### b. Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.

```
Enter password: <Type password>
Host key copied
%
```

- Si votre site utilise l'authentification de l'utilisateur avec les clés publiques, remplissez votre fichier `authorized_keys` sur l'hôte distant.

- a. Copiez votre clé publique sur l'hôte distant.

Saisissez la commande sur une seule ligne, sans barre oblique inverse.

```
myLocalHost% cat $HOME/.ssh/id_rsa.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

- b. Lorsque vous y êtes invité, indiquez votre mot de passe de connexion.

Lorsque le fichier est copié, le message "Key copied" (Clé copiée) s'affiche.

```
Enter password:      Type login password
Key copied
myLocalHost%
```

## 7 (Facultatif) Réduisez le nombre d'invites de phrases de passe.

Pour connaître la procédure, reportez-vous à la section “[Procédure de réduction des invites de mot de passe dans Secure Shell](#)” à la page 327. Pour plus d'informations, reportez-vous aux pages de manuel [ssh-agent\(1\)](#) et [ssh-add\(1\)](#).

## ▼ Procédure de modification de la phrase de passe pour une clé privée Secure Shell

La procédure suivante ne change pas la clé privée. La procédure modifie le mécanisme d'authentification pour la clé privée, la phrase de passe. Pour plus d'informations, reportez-vous à la page de manuel [ssh-keygen\(1\)](#).

- Modification de votre phrase de passe

Tapez la commande `ssh-keygen` avec l'option `-p`, et répondez aux invites.

```
myLocalHost% ssh-keygen -p
Enter file which contains the private key (/home/jdoe/.ssh/id_rsa):    <Press Return>
Enter passphrase (empty for no passphrase):    <Type passphrase>
Enter same passphrase again:    <Type passphrase>
```

Où `-p` demande la modification de la phrase de passe d'un fichier de clés privées.

## ▼ Procédure de connexion à un hôte distant avec Secure Shell

### 1 Démarrez une session Secure Shell.

Tapez la commande `ssh` et spécifiez le nom de l'hôte distant et votre identifiant de connexion.

```
myLocalHost% ssh myRemoteHost -l username
```

Une invite met en doute l'authenticité de l'hôte distant :

```
The authenticity of host 'myRemoteHost' can't be established.
RSA key fingerprint in md5 is: 04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26
Are you sure you want to continue connecting(yes/no)?
```

Cette invite est normale pour les connexions initiales sur des hôtes distants.

## 2 A l'invite, vérifiez l'authenticité de la clé de l'hôte distant.

- Si vous ne pouvez pas confirmer l'authenticité de l'hôte distant, saisissez **no** et contactez votre administrateur système.

```
Are you sure you want to continue connecting(yes/no)? no
```

L'administrateur est responsable de la mise à jour du fichier `/etc/ssh/ssh_known_hosts` global. Un fichier `ssh_known_hosts` mis à jour empêche l'affichage de cette invite.

- Si vous confirmez l'authenticité de l'hôte distant, répondez à l'invite et passez à l'étape suivante.

```
Are you sure you want to continue connecting(yes/no)? yes
```

## 3 Authentifiez-vous sur Secure Shell.

### a. Lorsque vous y êtes invité, saisissez votre phrase de passe.

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa': <Type passphrase>
```

### b. Lorsque vous y êtes invité, saisissez votre mot de passe de compte.

```
jdoe@myRemoteHost's password: <Type password>
Last login: Wed Sep  7 09:07:49 2011 from myLocalHost
Oracle Corporation      SunOS 5.11      September 2011
myRemoteHost%
```

## 4 Effectuez des transactions sur l'hôte distant.

Les commandes que vous envoyez sont chiffrées. Les réponses que vous recevez sont chiffrées.

## 5 Arrêtez la connexion Secure Shell.

Lorsque vous avez terminé, saisissez **exit** ou utilisez votre méthode habituelle pour quitter votre shell.

```
myRemoteHost% exit
myRemoteHost% logout
Connection to myRemoteHost closed
myLocalHost%
```

## ▼ Procédure de réduction des invites de mot de passe dans Secure Shell

Si vous ne voulez pas saisir votre phrase de passe et votre mot de passe pour utiliser Secure Shell, vous pouvez utiliser le démon de l'agent. Démarrez ce démon au début de la session. Ensuite, stockez vos clés privées avec le démon de l'agent à l'aide de la commande `ssh-add`. Si vous avez des comptes différents sur différents hôtes, ajoutez les clés dont vous avez besoin pour la session.

Vous pouvez démarrer le démon de l'agent manuellement lorsque vous en avez besoin, comme décrit dans la procédure suivante.

### 1 Démarrez le démon de l'agent.

```
myLocalHost% eval 'ssh-agent'
Agent pid 9892
```

### 2 Vérifiez que le démon de l'agent a été démarré.

```
myLocalHost% pgrep ssh-agent
9892
```

### 3 Ajoutez votre clé privée au démon de l'agent.

Saisissez la commande `ssh-add`.

```
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa: <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost%
```

### 4 Démarrez une session Secure Shell.

```
myLocalHost% ssh myRemoteHost -l jdoe
```

Vous n'êtes pas invité à saisir une phrase de passe.

## Exemple 17-2 Utilisation des options `ssh-add`

Dans cet exemple, `jdoe` ajoute deux clés pour le démon de l'agent. L'option `-l` sert à répertorier toutes les clés stockées dans le démon. A la fin de la session, l'option `-D` sert à supprimer toutes les clés du démon de l'agent.

```
myLocalHost% ssh-agent
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa: <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost% ssh-add /home/jdoe/.ssh/id_dsa
Enter passphrase for /home/jdoe/.ssh/id_dsa: <Type passphrase>
Identity added:
/home/jdoe/.ssh/id_dsa(/home/jdoe/.ssh/id_dsa)
```

```
myLocalHost% ssh-add -l
md5 1024 0e:fb:3d:53:71:77:bf:57:b8:eb:f7:a7:aa:df:e0:d1
/home/jdoe/.ssh/id_rsa(RSA)
md5 1024 c1:d3:21:5e:40:60:c5:73:d8:87:09:3a:fa:5f:32:53
/home/jdoe/.ssh/id_dsa(DSA)
```

*User conducts Oracle Solaris Secure Shell transactions*

```
myLocalHost% ssh-add -D
Identity removed:
/home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa.pub)
/home/jdoe/.ssh/id_dsa(DSA)
```

## ▼ Procédure d'utilisation du transfert de port dans Secure Shell

Vous pouvez spécifier qu'un port local est transmis à un hôte distant. En réalité, un socket est alloué pour écouter le port côté local. La connexion sur l'hôte distant à partir de ce port est effectuée par le biais d'un canal sécurisé. Par exemple, vous pouvez spécifier un port 143 afin de recevoir votre courrier à distance avec IMAP4. De la même façon, un port peut être spécifié côté distant.

### Avant de commencer

Pour utiliser le transfert de port, l'administrateur doit avoir activé le transfert de port sur le serveur Secure Shell distant. Pour plus de détails, reportez-vous à la section [“Procédure de configuration du transfert de port dans Secure Shell”](#) à la page 321.

### ● Pour utiliser le transfert de port sécurisé, choisissez l'une des options suivantes :

- **Pour définir un port local pour recevoir une communication sécurisée à partir d'un port distant, spécifiez les deux ports.**

Spécifiez le port local à l'écoute de la communication à distance. De même, indiquez l'hôte distant et le port distant qui transfèrent la communication.

```
myLocalHost% ssh -L localPort:remoteHost:remotePort
```

- **Pour définir un port distant de manière à ce qu'il reçoive une connexion sécurisée d'un port local, spécifiez les deux ports.**

Spécifiez le port distant à l'écoute de la communication à distance. De même, indiquez l'hôte local et le port local qui transfèrent la communication.

```
myLocalHost% ssh -R remotePort:localhost:localPort
```



**Exemple 17–3** Utilisation du transfert de port local pour recevoir du courrier

L'exemple suivant illustre l'utilisation du transfert du port local pour recevoir du courrier en toute sécurité à partir d'un serveur distant.

```
myLocalHost% ssh -L 9143:myRemoteHost:143 myRemoteHost
```

Cette commande transmet les connexions à partir du port 9143 sur myLocalHost au port 143. Port 143 est le port du serveur IMAP v2 sur myRemoteHost. Lorsque l'utilisateur lance une application de messagerie, celui-ci doit spécifier le numéro de port local pour le serveur IMAP, comme dans localhost:9143.

Il ne faut pas confondre localhost avec myLocalHost. myLocalHost est un nom d'hôte hypothétique. localhost est un mot-clé qui identifie votre système local.

**Exemple 17–4** Utilisation du transfert de port distant pour communiquer à l'extérieur d'un pare-feu

Cet exemple montre comment l'utilisateur, dans un environnement d'entreprise, peut transférer vers un hôte à l'intérieur d'un pare-feu d'entreprise des connexions d'un hôte sur un réseau externe.

```
myLocalHost% ssh -R 9022:myLocalHost:22 myOutsideHost
```

Cette commande transmet les connexions à partir du port 9022 sur myOutsideHost au port 22, le serveur sshd, sur l'hôte local.

```
myOutsideHost% ssh -p 9022 localhost
myLocalHost%
```

## ▼ Procédure de copie de fichiers avec Secure Shell

La procédure suivante décrit la façon dont la commande scp copie les fichiers chiffrés entre les hôtes. Vous pouvez copier les fichiers chiffrés entre un hôte local et un hôte distant, ou entre deux hôtes distants. La commande scp invite à s'authentifier. Pour plus d'informations, reportez-vous à la page de manuel [scp\(1\)](#).

Vous pouvez également utiliser le programme de transfert de fichiers sécurisé sftp. Pour plus d'informations, reportez-vous à la page de manuel [sftp\(1\)](#). Pour un exemple, reportez-vous à l'[Exemple 17–5](#).

---

**Remarque** – Le service d'audit permet d'auditer les transactions sftp via la classe d'audit ft. Pour scp, le service d'audit peut auditer l'accès et la sortie pour la session ssh.

---

**1 Démarrez le programme de copie sécurisée.**

Spécifiez le fichier source, le nom d'utilisateur au niveau de la destination distante et le répertoire de destination.

```
myLocalHost% scp myfile.1 jdoe@myRemoteHost:~
```

**2 Indiquez votre phrase de passe lorsque vous y êtes invité.**

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':    <Type passphrase>
myfile.1      25% |*****|      640 KB  0:20 ETA
myfile.1
```

Une fois que vous avez saisi la phrase de passe, un indicateur de progression s'affiche. Reportez-vous à la seconde ligne de la sortie ci-dessus. L'indicateur de progression affiche les données suivantes :

- Le nom de fichier
- Le pourcentage du fichier qui a été transféré
- Une série d'astérisques qui indiquent le pourcentage du fichier qui a été transmis
- La quantité de données transférées
- L'heure d'arrivée prévue de la totalité du fichier (c'est-à-dire, le temps restant)

**Exemple 17-5 Spécification d'un port à l'aide de la commande sftp**

Dans cet exemple, l'utilisateur souhaite que la commande `sftp` utilise un port spécifique. L'utilisateur utilise l'option `-o` pour spécifier le port.

```
% sftp -o port=2222 guest@RemoteFileServer
```

## ▼ Procédure de configuration de connexions par défaut à des hôtes en dehors du pare-feu

Vous pouvez utiliser Secure Shell pour établir une connexion entre un hôte à l'intérieur d'un pare-feu et un hôte à l'extérieur du pare-feu. Cette tâche s'effectue en spécifiant une commande proxy pour `ssh` dans un fichier de configuration ou sous forme d'option dans la ligne de commande. Pour l'option de ligne de commande, reportez-vous à l'[Exemple 17-6](#).

En général, vous pouvez personnaliser vos interactions `ssh` par le biais d'un fichier de configuration.

- Vous pouvez personnaliser votre propre fichier personnel dans `~/.ssh/config`.
- Ou bien, vous pouvez utiliser les paramètres dans le fichier de configuration administrative, `/etc/ssh/ssh_config`.

Les fichiers peuvent être personnalisés avec deux types de commandes proxy. Une commande proxy sert aux connexions HTTP. L'autre commande proxy sert aux connexions SOCKS5. Pour plus d'informations, reportez-vous à la page de manuel [ssh\\_config\(4\)](#).

## 1 Spécifiez les commandes proxy et les hôtes dans un fichier de configuration.

Utilisez la syntaxe suivante pour ajouter autant de lignes qu'il est nécessaire :

```
[Host outside-host]  
ProxyCommand proxy-command [-h proxy-server] \  
[-p proxy-port] outside-host %h outside-port %p
```

*Host outside-host*

Limite la spécification de la commande proxy aux instances lorsqu'un nom d'hôte distant est spécifié dans la ligne de commande. Si vous utilisez un caractère générique pour *outside-host*, vous appliquez la spécification de la commande proxy à un ensemble d'hôtes.

*proxy-command*

Spécifie la commande proxy.

La commande peut avoir l'une des formes suivantes :

- `/usr/lib/ssh/ssh-http-proxy-connect` pour les connexions HTTP
- `/usr/lib/ssh/ssh-socks5-proxy-connect` pour les connexions SOCKS5

*-h proxy-server* et *-p proxy-port*

Ces options spécifient respectivement un serveur proxy et un port proxy. Si des proxys sont présents, ils remplacent toutes les variables d'environnement qui spécifient les serveurs et ports proxy, tel que HTTPPROXY, HTTPPROXYPORT, SOCKS5\_PORT, SOCKS5\_SERVER et http\_proxy. La variable http\_proxy spécifie une adresse URL. Si ces options ne sont pas utilisées, les variables d'environnement doivent être définies. Pour plus d'informations, reportez-vous aux pages de manuel [ssh-socks5-proxy-connect\(1\)](#) et [ssh-http-proxy-connect\(1\)](#).

*outside-host*

Désigne un hôte spécifique pour la connexion. Utilisez l'argument de substitution %h pour spécifier l'hôte sur la ligne de commande.

*outside-port*

Désigne un port spécifique pour la connexion. Utilisez l'argument de substitution %p pour spécifier le port sur la ligne de commande. En spécifiant %h et %p sans utiliser l'option *Host outside-host*, la commande proxy est appliquée à l'argument de l'hôte chaque fois que la commande ssh est appelée.

## 2 Exécutez Secure Shell en indiquant l'hôte externe.

Par exemple, tapez la commande suivante :

```
myLocalHost% ssh myOutsideHost
```

Cette commande recherche une spécification de commande proxy pour `myOutsideHost` dans votre fichier de configuration. Si la spécification est introuvable, la commande recherche dans le fichier de configuration du système, `/etc/ssh/ssh_config`. La commande proxy remplace la commande `ssh`.

### Exemple 17–6 Connexion à des hôtes en dehors du pare-feu à partir de la ligne de commande

La section “[Procédure de configuration de connexions par défaut à des hôtes en dehors du pare-feu](#)” à la page 330 décrit la procédure de spécification d'une commande proxy dans un fichier de configuration. Dans cet exemple, une commande proxy est spécifiée sur la ligne de commande `ssh`.

```
% ssh -o'Proxycommand=/usr/lib/ssh/ssh-http-proxy-connect \  
-h myProxyServer -p 8080 myOutsideHost 22' myOutsideHost
```

L'option `-o` de la commande `ssh` fournit une méthode de ligne de commande pour spécifier une commande proxy. Cet exemple de commande effectue les opérations suivantes :

- La commande proxy HTTP remplace `ssh`
- Le port 8080 est utilisé et `myProxyServer` défini en tant que serveur proxy
- La connexion a lieu sur le port 22 de `myOutsideHost`

## Secure Shell (référence)

---

Ce chapitre décrit les options de configuration de la fonction Secure Shell d'Oracle Solaris. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre.

- “Session Secure Shell standard” à la page 333
- “Configuration des clients et des serveurs dans Secure Shell” à la page 336
- “Mots-clés dans Secure Shell” à la page 336
- “Mise à jour des hôtes connus dans Secure Shell” à la page 342
- “Fichier Secure Shell” à la page 342
- “Commandes Secure Shell” à la page 344

Pour plus d'informations sur les procédures de configuration de Secure Shell, reportez-vous au Chapitre 17, “Utilisation de Secure Shell (tâches)”.

### Session Secure Shell standard

Le démon Secure Shell (`sshd`) est démarré normalement au moment de l'initialisation lorsque les services réseau sont démarrés. Le démon détecte les connexions des clients. Une session Secure Shell commence lorsque l'utilisateur exécute une commande `ssh`, `scp` ou `sftp`. Un nouveau démon `sshd` est cloné pour chaque connexion entrante. Le démon cloné gère l'échange de clés, le chiffrement, l'authentification, l'exécution des commandes et l'échange de données avec le client. Ces caractéristiques de session sont déterminées par les fichiers de configuration côté client et côté serveur. Les arguments de la ligne de commande peuvent remplacer les paramètres des fichiers de configuration.

Le client doit s'authentifier auprès du serveur et vice-versa. Après la réussite de l'authentification, l'utilisateur peut exécuter des commandes à distance et copier des données entre les hôtes.

## Caractéristiques des sessions dans Secure Shell

Le comportement côté serveur du démon `sshd` est contrôlé par les paramètres de mot-clé dans le fichier `/etc/ssh/sshd_config`. Par exemple, le fichier `sshd_config` détermine les types d'authentification qui sont autorisés pour l'accès au serveur. Le comportement côté serveur peut également être contrôlé par les options de la ligne de commande lorsque le démon `sshd` est démarré.

Le comportement côté client est contrôlé par les mots-clés Secure Shell dans l'ordre de priorité suivant :

- Options de ligne de commande
- Fichier de configuration de l'utilisateur, `~/.ssh/config`
- Fichier de configuration à l'échelle du système, `/etc/ssh/ssh_config`

Par exemple, un utilisateur peut remplacer un paramètre `Ciphers` de configuration à l'échelle du système qui préfère `aes128-cen` en spécifiant `-c aes256-cen,aes128-cen,arcfour` sur la ligne de commande. Le premier chiffre, `aes256-cen`, est désormais préféré.

## Authentification et échange de clés dans Secure Shell

Le protocole Secure Shell prend en charge l'authentification utilisateur/hôte et l'authentification hôte serveur. Les clés cryptographiques sont échangées pour la protection des sessions Secure Shell. Secure Shell fournit plusieurs méthodes pour l'authentification et l'échange de clés. Certaines de ces méthodes sont facultatives. Les mécanismes d'authentification client sont répertoriés dans le [Tableau 17-1](#). Les serveurs sont authentifiés à l'aide de clés publiques d'hôte connu.

Pour l'authentification, Secure Shell prend en charge l'authentification de l'utilisateur et l'authentification interactive générique, qui implique généralement des mots de passe. Secure Shell prend également en charge l'authentification avec des clés publiques utilisateur et des clés publiques d'hôte de confiance. Il peut s'agir de clés RSA ou [DSA](#). Les échanges de clés de session sont des échanges de clés éphémères Diffie-Hellman qui sont signées à l'étape d'authentification du serveur. En outre, Secure Shell peut utiliser des informations d'identification GSS pour l'authentification.

## Acquisition d'informations d'identification GSS dans Secure Shell

Pour utiliser GSS-API pour l'authentification dans Secure Shell, le serveur doit disposer des informations d'identification de l'accepteur GSS-API et le client doit disposer des informations d'identification de l'initiateur GSS-API. La prise en charge est disponible pour `mech_dh` et pour `mech_krb5`.

Pour `mech_dh`, le serveur dispose des informations d'identification de l'accepteur GSS-API si `root` a exécuté la commande `keylogin`.

Pour `mech_krb5`, le serveur dispose des informations d'identification de GSS-API lorsque l'hôte principal qui correspond au serveur possède une valeur correcte dans `/etc/krb5/krb5.keytab`.

Le client dispose des informations d'identification de l'initiateur pour `mech_dh` si l'une des actions ci-après a été effectuée :

- La commande `keylogin` a été exécutée.
- Le module `pam_dhkeys` est utilisé dans le fichier `pam.conf`.

Le client dispose des informations d'identification de l'initiateur pour `mech_krb5` si l'une des actions ci-après a été effectuée :

- La commande `kinit` a été exécutée.
- Le module `pam_krb5` est utilisé dans le fichier `pam.conf`.

Pour l'utilisation de `mech_dh` dans le RPC sécurisé, reportez-vous au [Chapitre 14](#), “Authentification des services réseau (tâches)”. Pour l'utilisation de `mech_krb5`, reportez-vous au [Chapitre 19](#), “Introduction au service Kerberos”. Pour plus d'informations sur les mécanismes, reportez-vous aux pages de manuel [mech\(4\)](#) et [mech\\_spnego\(5\)](#).

## Exécution des commandes et transmission de données dans Secure Shell

Une fois l'authentification terminée, l'utilisateur peut utiliser Secure Shell, généralement en demandant un shell ou en exécutant une commande. Par l'intermédiaire des options de commande `ssh`, l'utilisateur peut effectuer des demandes. Les demandes peuvent inclure l'allocation d'un pseudo-tty, la transmission des connexions X11 ou TCP/IP, ou l'activation d'un programme d'authentification `ssh-agent` via une connexion sécurisée.

Les composants de base d'une session utilisateur sont les suivants :

1. L'utilisateur demande un shell ou l'exécution d'une commande, ce qui lance le mode de session.  
Dans ce mode, les données sont envoyées ou reçues par le biais du terminal sur le côté client. Sur le côté serveur, les données sont envoyées par l'intermédiaire du shell ou d'une commande.
2. Lorsque la transmission des données est terminée, le programme utilisateur s'arrête.
3. L'ensemble de la transmission X11 et de la transmission TCP/IP est arrêté, sauf pour les connexions qui existent déjà. Les connexions X11 et TCP/IP existantes restent ouvertes.
4. Le serveur envoie un message d'état de sortie au client. Lorsque toutes les connexions sont fermées, telles que les ports transmis qui étaient restés ouverts, le client ferme la connexion au serveur. Ensuite, le client se ferme.

# Configuration des clients et des serveurs dans Secure Shell

Les caractéristiques d'une session Secure Shell sont contrôlées par les fichiers de configuration. Les fichiers de configuration peuvent être remplacés dans une certaine mesure par des options de la ligne de commande.

## Configuration des clients dans Secure Shell

Dans la plupart des cas, les caractéristiques côté client d'une session Secure Shell sont régies par le fichier de configuration à l'échelle du système, `/etc/ssh/ssh_config`. Les paramètres dans le fichier `ssh_config` peuvent être remplacés par le fichier de configuration de l'utilisateur, `~/.ssh/config`. En outre, l'utilisateur peut remplacer les deux fichiers de configuration sur la ligne de commande.

Les paramètres du fichier `/etc/ssh/sshd_config` du serveur déterminent quelles demandes client sont autorisées par le serveur. Pour obtenir la liste des paramètres de configuration de serveur, reportez-vous à la section “[Mots-clés dans Secure Shell](#)” à la page 336. Pour plus d'informations, reportez-vous à la page de manuel `sshd_config(4)`.

Les mots-clés du fichier de configuration du client sont répertoriés dans la section “[Mots-clés dans Secure Shell](#)” à la page 336. Si le mot-clé a une valeur par défaut, la valeur est donnée. Ces mots-clés sont décrits en détails dans les pages de manuel `ssh(1)`, `scp(1)`, `sftp(1)` et `ssh_config(4)`. Pour obtenir la liste des mots-clés dans l'ordre alphabétique et leurs substituts de ligne de commande équivalents, reportez-vous au [Tableau 18–8](#).

## Configuration du serveur dans Secure Shell

Les caractéristiques côté serveur d'une session Secure Shell sont régies par le fichier `/etc/ssh/sshd_config`. Les mots-clés dans le fichier de configuration du serveur sont répertoriés dans “[Mots-clés dans Secure Shell](#)” à la page 336. Si le mot-clé a une valeur par défaut, la valeur est donnée. Pour une description complète des mots-clés, reportez-vous à la page de manuel `sshd_config(4)`.

## Mots-clés dans Secure Shell

Les tableaux ci-dessous répertorient les mots-clés et leurs valeurs par défaut, le cas échéant. Les mots-clés sont dans l'ordre alphabétique. Les mots-clés qui s'appliquent au client sont dans le fichier `ssh_config`. Les mots-clés qui s'appliquent au serveur sont dans le fichier `sshd_config`. Certains mots-clés sont définis dans les deux fichiers. Les mots-clés pour un serveur Secure Shell exécutant le protocole v1 sont marqués.



TABLEAU 18-1 Mots-clés des fichiers de configuration Secure Shell (A à Escape)

| Mot-clé             | Valeur par défaut                                       | Emplacement |
|---------------------|---------------------------------------------------------|-------------|
| AllowGroups         | Pas de valeur par défaut.                               | Serveur     |
| AllowTcpForwarding  | yes                                                     | Serveur     |
| AllowUsers          | Pas de valeur par défaut.                               | Serveur     |
| AuthorizedKeysFile  | ~/.ssh/authorized_keys                                  | Serveur     |
| Banner              | /etc/issue                                              | Serveur     |
| Batchmode           | no                                                      | Client      |
| BindAddress         | Pas de valeur par défaut.                               | Client      |
| CheckHostIP         | yes                                                     | Client      |
| ChrootDirectory     | no                                                      | Serveur     |
| Cipher              | blowfish, 3des                                          | Client      |
| Ciphers             | aes128-ctr, aes128-cbc, 3des-cbc, blowfish-cbc, arcfour | Les deux    |
| ClearAllForwardings | no                                                      | Client      |
| ClientAliveCountMax | 3                                                       | Serveur     |
| ClientAliveInterval | 0                                                       | Serveur     |
| Compression         | no                                                      | Les deux    |
| CompressionLevel    | Pas de valeur par défaut.                               | Client      |
| ConnectionAttempts  | 1                                                       | Client      |
| ConnectTimeout      | Délai d'attente TCP système                             | Client      |
| DenyGroups          | Pas de valeur par défaut                                | Serveur     |
| DenyUsers           | Pas de valeur par défaut                                | Serveur     |
| DisableBanner       | no                                                      | Client      |
| DynamicForward      | Pas de valeur par défaut.                               | Client      |
| EscapeChar          | ~                                                       | Client      |

TABLEAU 18-2 Mots-clés dans les fichiers de configuration Secure Shell (Fall à Local)

| Mot-clé       | Valeur par défaut | Emplacement |
|---------------|-------------------|-------------|
| FallBackToRsh | no                | Client      |

TABLEAU 18-2 Mots-clés dans les fichiers de configuration Secure Shell (Fall à Local) (Suite)

| Mot-clé                         | Valeur par défaut                                                                                                                         | Emplacement |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| ForwardAgent                    | no                                                                                                                                        | Client      |
| ForwardX11                      | no                                                                                                                                        | Client      |
| ForwardX11Trusted               | yes                                                                                                                                       | Client      |
| GatewayPorts                    | no                                                                                                                                        | Les deux    |
| GlobalKnownHostsFile            | /etc/ssh/ssh_known_hosts                                                                                                                  | Client      |
| GSSAPIAuthentication            | yes                                                                                                                                       | Les deux    |
| GSSAPIDelegateCredentials       | no                                                                                                                                        | Client      |
| GSSAPIKeyExchange               | yes                                                                                                                                       | Les deux    |
| GSSAPIStoreDelegateCredentials  | yes                                                                                                                                       | Serveur     |
| HashKnownHosts                  | no                                                                                                                                        | Client      |
| Host                            | * Pour plus d'informations, reportez-vous à la section <a href="#">“Paramètres spécifiques à l'hôte dans Secure Shell”</a> à la page 341. | Client      |
| HostbasedAuthentication         | no                                                                                                                                        | Les deux    |
| HostbasedUsesNameFromPacketOnly | no                                                                                                                                        | Serveur     |
| HostKey                         | /etc/ssh/ssh_host_key                                                                                                                     | Serveur, v1 |
| HostKey                         | /etc/ssh/host_rsa_key,<br>/etc/ssh/host_dsa_key                                                                                           | Serveur     |
| HostKeyAlgorithms               | ssh-rsa, ssh-dss                                                                                                                          | Client      |
| HostKeyAlias                    | Pas de valeur par défaut.                                                                                                                 | Client      |
| HostName                        | Pas de valeur par défaut.                                                                                                                 | Client      |
| IdentityFile                    | ~/.ssh/id_dsa, ~/.ssh/id_rsa                                                                                                              | Client      |
| IgnoreIfUnknown                 | Pas de valeur par défaut                                                                                                                  | Client      |
| IgnoreRhosts                    | yes                                                                                                                                       | Serveur     |
| IgnoreUserKnownHosts            | yes                                                                                                                                       | Serveur     |
| KbdInteractiveAuthentication    | yes                                                                                                                                       | Les deux    |
| KeepAlive                       | yes                                                                                                                                       | Les deux    |
| KeyRegenerationInterval         | 3600 (secondes)                                                                                                                           | Serveur     |

**TABLEAU 18-2** Mots-clés dans les fichiers de configuration Secure Shell (Fall à Local) *(Suite)*

| Mot-clé       | Valeur par défaut         | Emplacement |
|---------------|---------------------------|-------------|
| ListenAddress | Pas de valeur par défaut. | Serveur     |
| LocalForward  | Pas de valeur par défaut. | Client      |

**TABLEAU 18-3** Mots-clés dans les fichiers de configuration Secure Shell (Login à R)

| Mot-clé                          | Valeur par défaut                                 | Emplacement |
|----------------------------------|---------------------------------------------------|-------------|
| LoginGraceTime                   | 120 (secondes)                                    | Serveur     |
| LogLevel                         | info                                              | Les deux    |
| LookupClientHostnames            | yes                                               | Serveur     |
| MACs                             | hmac-sha1,hmac-md5                                | Les deux    |
| Match                            | Pas de valeur par défaut                          | Serveur     |
| MaxStartups                      | 10:30:60                                          | Serveur     |
| NoHostAuthenticationForLocalHost | no                                                | Client      |
| NumberOfPasswordPrompts          | 3                                                 | Client      |
| PAMServiceName                   | Pas de valeur par défaut                          | Serveur     |
| PAMServicePrefix                 | Pas de valeur par défaut                          | Serveur     |
| PasswordAuthentication           | yes                                               | Les deux    |
| PermitEmptyPasswords             | no                                                | Serveur     |
| PermitRootLogin                  | no                                                | Serveur     |
| PermitUserEnvironment            | no                                                | Serveur     |
| PidFile                          | /system/volatile/sshd.pid                         | Serveur     |
| Port                             | 22                                                | Les deux    |
| PreferredAuthentications         | hostbased,publickey,keyboard-interactive,password | Client      |
| PreUserauthHook                  | Pas de valeur par défaut                          | Serveur     |
| PrintLastLog                     | yes                                               | Serveur     |
| PrintMotd                        | no                                                | Serveur     |
| Protocol                         | 2,1                                               | Les deux    |
| ProxyCommand                     | Pas de valeur par défaut.                         | Client      |

**TABEAU 18-3** Mots-clés dans les fichiers de configuration Secure Shell (Login à R) *(Suite)*

| Mot-clé                 | Valeur par défaut         | Emplacement |
|-------------------------|---------------------------|-------------|
| PubkeyAuthentication    | yes                       | Les deux    |
| RekeyLimit              | 1G à 4G                   | Client      |
| RemoteForward           | Pas de valeur par défaut. | Client      |
| RhostsAuthentication    | no                        | Serveur, v1 |
| RhostsRSAAuthentication | no                        | Serveur, v1 |
| RSAAuthentication       | no                        | Serveur, v1 |

**TABEAU 18-4** Mots-clés dans les fichiers de configuration Secure Shell (S à X)

| Mot-clé               | Valeur par défaut            | Emplacement |
|-----------------------|------------------------------|-------------|
| ServerAliveCountMax   | 3                            | Client      |
| ServerAliveInterval   | 0                            | Client      |
| ServerKeyBits         | 512 à 768                    | Serveur, v1 |
| StrictHostKeyChecking | ask                          | Client      |
| StrictModes           | yes                          | Serveur     |
| Subsystem             | sftp/usr/lib/ssh/sftp-server | Serveur     |
| SyslogFacility        | auth                         | Serveur     |
| UseOpenSSLEngine      | yes                          | Les deux    |
| UsePrivilegedPort     | no                           | Les deux    |
| User                  | Pas de valeur par défaut     | Client      |
| UserKnownHostsFile    | ~/.ssh/known_hosts           | Client      |
| UseRsh                | no                           | Client      |
| VerifyReverseMapping  | no                           | Serveur     |
| X11DisplayOffset      | 10                           | Serveur     |
| X11Forwarding         | yes                          | Serveur     |
| X11UseLocalHost       | yes                          | Serveur     |
| XAuthLocation         | /usr/openwin/bin/xauth       | Les deux    |

## Paramètres spécifiques à l'hôte dans Secure Shell

S'il est utile de disposer de différentes caractéristiques Secure Shell pour différents hôtes locaux, l'administrateur peut définir différents ensembles de paramètres dans le fichier `/etc/ssh/ssh_config` à appliquer en fonction de l'hôte ou d'une expression régulière. Cette tâche s'effectue en regroupant les entrées dans le fichier par le mot-clé `Host`. Si le mot-clé `Host` n'est pas utilisé, les entrées dans le fichier de configuration du client s'appliquent à n'importe lequel des hôtes locaux sur lesquels un utilisateur travaille.

## Secure Shell et les variables d'environnement de connexion

Si les mots-clés Secure Shell suivants ne sont pas définis dans le fichier `sshd_config`, ils obtiennent leur valeur des entrées équivalentes à partir du fichier `/etc/default/login`.

| Entrée dans <code>/etc/default/login</code>               | Mot-clé et valeur dans <code>sshd_config</code>                                                                      |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>CONSOLE=*</code>                                    | <code>PermitRootLogin=without-password</code>                                                                        |
| <code>#CONSOLE=*</code>                                   | <code>PermitRootLogin=yes</code>                                                                                     |
| <code>PASSREQ=YES</code>                                  | <code>PermitEmptyPasswords=no</code>                                                                                 |
| <code>PASSREQ=NO</code>                                   | <code>PermitEmptyPasswords=yes</code>                                                                                |
| <code>#PASSREQ</code>                                     | <code>PermitEmptyPasswords=no</code>                                                                                 |
| <code>TIMEOUT=secs</code>                                 | <code>LoginGraceTime=secs</code>                                                                                     |
| <code>#TIMEOUT</code>                                     | <code>LoginGraceTime=120</code>                                                                                      |
| <code>RETRIES</code> et <code>SYSLOG_FAILED_LOGINS</code> | S'appliquent uniquement aux méthodes d'authentification <code>password</code> et <code>keyboard-interactive</code> . |

Lorsque les variables suivantes sont définies par les scripts d'initialisation du shell de connexion de l'utilisateur, le démon `sshd` utilise ces valeurs. Lorsque les variables ne sont pas définies, le démon utilise la valeur par défaut.

|          |                                                                                                                                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TIMEZONE | Contrôle la définition de la variable d'environnement TZ. Lorsque cette variable n'est pas définie, le démon <code>sshd</code> utilise la valeur de TZ telle qu'elle était au moment de son démarrage.                                                              |
| ALTSHELL | Contrôle la définition de la variable d'environnement SHELL. La valeur par défaut est <code>ALTSHELL=YES</code> , où le démon <code>sshd</code> utilise la valeur de shell de l'utilisateur. Quand <code>ALTSHELL=NO</code> , la valeur de SHELL n'est pas définie. |

|        |                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PATH   | Contrôle la définition de la variable d'environnement PATH. Lorsque la valeur n'est pas définie, le chemin d'accès par défaut est /usr/bin.                     |
| SUPATH | Contrôle la définition de la variable d'environnement PATH pour root. Lorsque la valeur n'est pas définie, le chemin d'accès par défaut est /usr/sbin:/usr/bin. |

Pour plus d'informations, reportez-vous aux pages de manuel [login\(1\)](#) et [sshd\(1M\)](#).

## Mise à jour des hôtes connus dans Secure Shell

Chaque hôte qui doit communiquer de manière sécurisée avec un autre hôte doit avoir la clé publique du serveur stockée dans le fichier /etc/ssh/les de l'hôte local. Bien qu'un script puisse être utilisé pour mettre à jour les fichiers /etc/ssh/ssh\_known\_hosts, une telle pratique est fortement déconseillée parce qu'un script crée une grande vulnérabilité de la sécurité.

Le fichier /etc/ssh/ssh\_known\_hosts doit uniquement être distribué par un mécanisme sécurisé comme suit :

- Via une connexion sécurisée, comme par exemple Secure Shell, IPsec, ou ftp utilisant Kerberos à partir d'une machine connue et de confiance
- Au moment de l'installation

Pour éviter toute possibilité qu'un intrus obtienne l'accès en insérant de fausses clés publiques dans un fichier known\_hosts, vous devez utiliser une source connue et de confiance du fichier ssh\_known\_hosts. Le fichier ssh\_known\_hosts peut être distribué au cours de l'installation. Plus tard, les scripts utilisant la commande scp peuvent être utilisés pour récupérer la version la plus récente.

## Fichier Secure Shell

Le tableau suivant montre les fichiers Secure Shell importants et les autorisations de fichier suggérées.

TABLEAU 18-5 Fichier Secure Shell

| Nom du fichier                                               | Description                                                             | Autorisations suggérées et propriétaire |
|--------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------|
| /etc/ssh/sshd_config                                         | Contient des données de configuration pour sshd, le démon Secure Shell. | -rw-r--r-- root                         |
| /etc/ssh/ssh_host_dsa_key<br>ou<br>/etc/ssh/ssh_host_rsa_key | Contient la clé privée de l'hôte.                                       | -rw----- root                           |

TABLEAU 18-5 Fichier Secure Shell (Suite)

| Nom du fichier                         | Description                                                                                                                                                                                                                                                                                                   | Autorisations suggérées et propriétaire |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| <i>host-private-key .pub</i>           | Contient la clé publique de l'hôte, par exemple, <code>/etc/ssh/ssh_host_rsa_key.pub</code> . Est utilisé pour copier la clé d'hôte dans le fichier <code>known_hosts</code> local.                                                                                                                           | <code>-rw-r--r-- root</code>            |
| <code>/system/volatile/sshd.pid</code> | Contient l'ID de processus du démon Secure Shell, <code>sshd</code> . Si plusieurs démons sont en cours d'exécution, le fichier contient la dernier démon qui a été démarré.                                                                                                                                  | <code>-rw-r--r-- root</code>            |
| <code>~/.ssh/authorized_keys</code>    | Contient les clés publiques de l'utilisateur qui est autorisé à se connecter au compte utilisateur.                                                                                                                                                                                                           | <code>-rw-r--r-- username</code>        |
| <code>/etc/ssh/ssh_known_hosts</code>  | Contient les clés publiques pour tous les hôtes avec lesquels le client peut communiquer de manière sécurisée. Le fichier est renseigné par l'administrateur.                                                                                                                                                 | <code>-rw-r--r-- root</code>            |
| <code>~/.ssh/known_hosts</code>        | Contient les clés publiques pour tous les hôtes avec lesquels le client peut communiquer de manière sécurisée. Le fichier est mis à jour automatiquement. Chaque fois que l'utilisateur se connecte à l'aide d'un hôte inconnu, la clé de l'hôte distant est ajoutée au fichier.                              | <code>-rw-r--r-- username</code>        |
| <code>/etc/default/login</code>        | Fournit les valeurs par défaut pour le démon <code>sshd</code> lorsque les paramètres <code>sshd_config</code> correspondants ne sont pas définis.                                                                                                                                                            | <code>-r--r--r-- root</code>            |
| <code>/etc/nologin</code>              | Si ce fichier existe, le démon <code>sshd</code> n'autorise que <code>root</code> à se connecter. Le contenu de ce fichier est affiché pour les utilisateurs qui tentent de se connecter.                                                                                                                     | <code>-rw-r--r-- root</code>            |
| <code>~/.rhosts</code>                 | Contient les paires de noms hôte-utilisateur qui permettent d'indiquer les hôtes auxquels l'utilisateur peut se connecter sans mot de passe. Ce fichier est également utilisé par les démons <code>rlogind</code> et <code>rshd</code> .                                                                      | <code>-rw-r--r-- username</code>        |
| <code>~/.shosts</code>                 | Contient les paires de noms hôte-utilisateur qui permettent d'indiquer les hôtes auxquels l'utilisateur peut se connecter sans mot de passe. Ce fichier n'est utilisé par aucun autre utilitaire. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">sshd(1M)</a> dans la section FILES. | <code>-rw-r--r-- username</code>        |
| <code>/etc/hosts.equiv</code>          | Contient les hôtes qui sont utilisés dans l'authentification <code>.rhosts</code> . Ce fichier est également utilisé par les démons <code>rlogind</code> et <code>rshd</code> .                                                                                                                               | <code>-rw-r--r-- root</code>            |
| <code>/etc/ssh/shosts.equiv</code>     | Contient les hôtes qui sont utilisés dans l'authentification basée sur les hôtes. Ce fichier n'est utilisé par aucun autre utilitaire.                                                                                                                                                                        | <code>-rw-r--r-- root</code>            |
| <code>~/.ssh/environment</code>        | Contient les affectations initiales au moment de la connexion. Par défaut, ce fichier n'est pas lu. Le mot-clé <code>PermitUserEnvironment</code> du fichier <code>sshd_config</code> doit être défini sur <code>yes</code> pour que ce fichier soit lu.                                                      | <code>-rw-r--r-- username</code>        |

TABLEAU 18-5 Fichier Secure Shell (Suite)

| Nom du fichier      | Description                                                                                                                                                                                                        | Autorisations suggérées et propriétaire |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| ~/.ssh/rc           | Contient les routines d'initialisation qui sont exécutées avant que le shell utilisateur ne démarre. Pour un échantillon de routine d'initialisation, reportez-vous à la page de manuel <a href="#">sshd(1M)</a> . | -rw-r--r-- username                     |
| /etc/ssh/crsh       | Contient les routines d'initialisation spécifiques à un hôte qui sont spécifiées par un administrateur.                                                                                                            | -rw-r--r-- root                         |
| /etc/ssh/ssh_config | Configure les paramètres système sur le système client.                                                                                                                                                            | -rw-r--r-- root                         |
| ~/.ssh/config       | Permet de configurer les paramètres utilisateur qui remplacent les paramètres système.                                                                                                                             | -rw-r--r-- username                     |

Le tableau ci-dessous répertorie les fichiers Secure Shell qui peuvent être remplacés par des mots-clés ou des options de commande.

TABLEAU 18-6 Remplacement pour l'emplacement des fichiers Secure Shell

| Nom du fichier              | Remplacement par mot-clé | Remplacement via la ligne de commande    |
|-----------------------------|--------------------------|------------------------------------------|
| /etc/ssh/ssh_config         |                          | ssh -F config-file<br>scp -F config-file |
| ~/.ssh/config               |                          | ssh -F config-file                       |
| /etc/ssh/host_rsa_key       | HostKey                  |                                          |
| /etc/ssh/host_dsa_key       |                          |                                          |
| ~/.ssh/identity             | IdentityFile             | ssh -i id-file                           |
| ~/.ssh/id_dsa,~/.ssh/id_rsa |                          | scp -i id-file                           |
| ~/.ssh/authorized_keys      | AuthorizedKeysFile       |                                          |
| /etc/ssh/ssh_known_hosts    | GlobalKnownHostsFile     |                                          |
| ~/.ssh/known_hosts          | UserKnownHostsFile       |                                          |
|                             | IgnoreUserKnownHosts     |                                          |

# Commandes Secure Shell

Le tableau suivant récapitule les principales commandes Secure Shell.



TABLEAU 18-7 Commandes Secure Shell

| Page de manuel pour les commandes | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ssh(1)</code>               | Connecte un utilisateur à une machine distante et exécute de manière sécurisée les commandes sur une machine distante. Cette commande est le remplacement Secure Shell des commandes <code>rlogin</code> et <code>rsh</code> . La commande <code>ssh</code> permet de protéger les communications chiffrées entre deux hôtes non autorisés sur un réseau non sécurisé. Les connexions X11 et les ports TCP/IP arbitraires peuvent également être transmis via le canal sécurisé.                                                                         |
| <code>sshd(1M)</code>             | Est le démon pour Secure Shell. Le démon détecte les connexions des clients et sécurise les communications chiffrées entre deux hôtes non autorisés sur un réseau non sécurisé.                                                                                                                                                                                                                                                                                                                                                                          |
| <code>ssh-add(1)</code>           | Ajoute des identités RSA ou DSA à l'agent d'authentification, <code>ssh-agent</code> . Les identités sont également appelées <i>clés</i> .                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>ssh-agent(1)</code>         | Contient les clés privées qui sont utilisées pour l'authentification avec clé publique. Le programme <code>ssh-agent</code> est lancé au début d'une session X ou d'une session de connexion. Toutes les autres fenêtres et les autres programmes sont lancés en tant que clients du programme <code>ssh-agent</code> . Par le biais de l'utilisation de variables d'environnement, l'agent peut être localisé et utilisé pour l'authentification lorsque les utilisateurs utilisent la commande <code>ssh</code> pour se connecter à d'autres systèmes. |
| <code>ssh-keygen(1)</code>        | Génère et gère des clés d'authentification pour Secure Shell.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>ssh-keyscan(1)</code>       | Regroupe les clés publiques d'un certain nombre d'hôtes Secure Shell. Facilite la création et la vérification des fichiers <code>ssh_known_hosts</code> .                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>ssh-keysign(1M)</code>      | Est utilisé par les commandes <code>ssh</code> pour accéder aux clés d'hôte sur l'hôte local. Génère la signature numérique requise pendant l'authentification basée sur l'hôte avec Secure Shell v2. La commande est appelée par la commande <code>ssh</code> , et non par l'utilisateur.                                                                                                                                                                                                                                                               |
| <code>scp(1)</code>               | Copie les fichiers de manière sécurisée entre les hôtes d'un réseau via un transport <code>ssh</code> chiffré. Contrairement à la commande <code>rcp</code> , la commande <code>scp</code> demande à saisir les mots de passe ou les phrases de passe, si des informations de mot de passe sont nécessaires pour l'authentification.                                                                                                                                                                                                                     |
| <code>sftp(1)</code>              | Est un programme de transmission de fichier interactif similaire à la commande <code>ftp</code> . Contrairement à la commande <code>ftp</code> , la commande <code>sftp</code> effectue toutes les opérations sur un transport <code>ssh</code> chiffré. La commande établit la connexion, se connecte au nom d'hôte spécifié, puis entre en mode de commande interactif.                                                                                                                                                                                |

Le tableau suivant répertorie les options de commande qui se substituent aux mots-clés Secure Shell. Les mots-clés sont spécifiés dans les fichiers `ssh_config` et `sshd_config`.

TABLEAU 18-8 Options de ligne de commande équivalentes aux mots-clés Secure Shell

| Mot-clé     | Option de ligne de commande de substitution ssh | Option de ligne de commande de substitution scp |
|-------------|-------------------------------------------------|-------------------------------------------------|
| BatchMode   |                                                 | <code>scp -B</code>                             |
| BindAddress | <code>ssh -b bind-addr</code>                   | <code>scp -a bind-addr</code>                   |

TABLEAU 18-8 Options de ligne de commande équivalentes aux mots-clés Secure Shell (Suite)

| Mot-clé        | Option de ligne de commande de substitution ssh | Option de ligne de commande de substitution scp |
|----------------|-------------------------------------------------|-------------------------------------------------|
| Cipher         | ssh -c <i>cipher</i>                            | scp -c <i>cipher</i>                            |
| Ciphers        | ssh -c <i>cipher-spec</i>                       | scp -c <i>cipher-spec</i>                       |
| Compression    | ssh -C                                          | scp -C                                          |
| DynamicForward | ssh -D <i>SOCKS4-port</i>                       |                                                 |
| EscapeChar     | ssh -e <i>escape-char</i>                       |                                                 |
| ForwardAgent   | ssh -A pour activer<br>ssh -a pour désactiver   |                                                 |
| ForwardX11     | ssh -X pour activer<br>ssh -x pour désactiver   |                                                 |
| GatewayPorts   | ssh -g                                          |                                                 |
| IPv4           | ssh -4                                          | scp -4                                          |
| IPv6           | ssh -6                                          | scp -6                                          |
| LocalForward   | ssh -L <i>localport:remotehost:remoteport</i>   |                                                 |
| MACS           | ssh -m <i>mac-spec</i>                          |                                                 |
| Port           | ssh -p <i>port</i>                              | scp -P <i>port</i>                              |
| Protocol       | ssh -2 pour v2 uniquement                       |                                                 |
| RemoteForward  | ssh -R <i>remoteport:localhost:localport</i>    |                                                 |

## PARTIE VI

# Service Kerberos

Cette section fournit des informations sur la configuration, la gestion et l'utilisation du service Kerberos dans les chapitres suivants :

- Chapitre 19, "Introduction au service Kerberos"
- Chapitre 20, "Planification du service Kerberos"
- Chapitre 21, "Configuration du service Kerberos (tâches)"
- Chapitre 22, "Messages d'erreur et dépannage de Kerberos"
- Chapitre 23, "Administration des principaux et des stratégies Kerberos (tâches)"
- Chapitre 24, "Utilisation des applications Kerberos (tâches)"
- Chapitre 25, "Service Kerberos (référence)"



## Introduction au service Kerberos

---

Ce chapitre présente le service Kerberos. Vous trouverez ci-dessous une liste des informations générales contenues dans ce chapitre.

- “Description du service Kerberos” à la page 349
- “Fonctionnement du service Kerberos” à la page 350
- “Services de sécurité Kerberos” à la page 357
- “Composants des différentes versions Kerberos” à la page 358

### Description du service Kerberos

Le *service Kerberos* est une architecture client-serveur qui garantit la sécurité des transactions sur les réseaux. Le service assure l'authentification fiable des utilisateurs, ainsi que l'intégrité et la confidentialité. L'*authentification* garantit que l'identité de l'expéditeur et du destinataire d'une transaction réseau sont toutes deux réelles. Le service peut également vérifier la validité des données transmises (*intégrité*) et le chiffrement des données lors de la transmission (*confidentialité*). A l'aide du service Kerberos, vous pouvez vous connecter à d'autres machines, exécuter des commandes, échanger des données et transférer des fichiers en toute sécurité. En outre, ce service offre des services d'*autorisation*, ce qui permet aux administrateurs de limiter l'accès aux services et aux machines. Par ailleurs, en tant qu'utilisateur Kerberos, vous pouvez réguler l'accès d'autres personnes à votre compte.

Le service Kerberos est un système à *connexion unique*, ce qui signifie que vous ne devez vous authentifier auprès du service qu'une fois par session et toutes les transactions ultérieures au cours de la session sont automatiquement protégées. Une fois authentifié par le service, vous n'avez plus besoin de vous authentifier à chaque utilisation d'une commande basée sur Kerberos, comme `ftp` ou `rsh`, ou pour accéder à des données sur un système de fichiers NFS. Par conséquent, vous n'avez pas à envoyer votre mot de passe sur le réseau, où il peut être intercepté à chaque fois que vous utilisez ces services.

Le service Kerberos dans la version Oracle Solaris est basé sur le protocole d'authentification réseau Kerberos V5 développé au Massachusetts Institute of Technology (MIT). Les utilisateurs

du produit Kerberos V5 trouveront donc la version Oracle Solaris très familière. Le protocole Kerberos V5 étant une norme *de facto* de l'industrie en matière de réseau, la version d'Oracle Solaris favorise l'interopérabilité avec d'autres systèmes. En d'autres termes, puisque le service Kerberos dans la version Oracle Solaris fonctionne avec les systèmes utilisant le protocole Kerberos V5, ce service permet de sécuriser les transactions même sur des réseaux hétérogènes. En outre, le service assure l'authentification et la sécurité entre les domaines et au sein d'un domaine unique.

Le service Kerberos offre une plus grande flexibilité dans l'exécution des applications Oracle Solaris. Vous pouvez configurer ce service pour autoriser les demandes de services réseau Kerberos et non Kerberos, notamment les services NFS, telnet et ftp. Par conséquent, les applications actuelles fonctionnent toujours, même si elles sont en cours d'exécution sur des systèmes sur lesquels le service Kerberos n'est pas activé. Bien entendu, vous pouvez également configurer le service Kerberos pour n'autoriser que les requêtes de réseau Kerberos.

Le service Kerberos fournit un mécanisme de sécurité permettant d'utiliser Kerberos pour l'authentification, l'intégrité et la confidentialité lors de l'utilisation d'applications ayant recours à GSS-API (API générique de services de sécurité). Toutefois, il n'est pas nécessaire que les applications restent dédiées au service Kerberos si d'autres mécanismes de sécurité sont développés. Etant donné que le service est conçu pour s'intégrer de façon modulaire à GSS-API, les applications qui l'utilisent peuvent utiliser le mécanisme de sécurité le plus adapté à leurs besoins.

## Fonctionnement du service Kerberos

Vous trouverez ci-dessous une présentation de l'authentification Kerberos. Pour une description plus détaillée, reportez-vous à la section [“Fonctionnement du système d'authentification Kerberos”](#) à la page 540.

Du point de vue de l'utilisateur, le service Kerberos est pratiquement invisible une fois la session Kerberos démarrée. Les commandes telles que rsh ou ftp fonctionnent de la même manière. L'initialisation d'une session Kerberos n'implique souvent rien de plus que la connexion et l'indication du mot de passe Kerberos.

Le système Kerberos est basé sur le concept de *ticket*. Un ticket est un ensemble d'informations électroniques qui identifient un utilisateur ou un service tel que le service NFS. Tout comme votre permis de conduire vous identifie et indique les privilèges de conduite dont vous disposez, un ticket vous identifie ainsi que vos privilèges d'accès au réseau. Lorsque vous effectuez une transaction basée sur Kerberos (par exemple, si vous vous connectez à distance à une autre machine), vous envoyez de façon transparente une demande de ticket à un KDC (Key Distribution Center, centre de distribution des clés). Le KDC accède à une base de données pour authentifier votre identité et renvoie un ticket qui vous autorise à accéder à l'autre machine. "De façon transparente" signifie que vous n'avez pas à demander explicitement un

ticket. La demande s'effectue dans le cadre de la commande `rlogin`. Puisque seul un client authentifié peut obtenir un ticket d'un service particulier, un autre client ne peut pas utiliser `rlogin` sous une fausse identité.

Certains attributs sont associés aux tickets. Par exemple, un ticket peut être *transmissible*, ce qui signifie qu'il peut être utilisé sur un autre ordinateur sans nouveau processus d'authentification. Un ticket peut également être *postdaté*, ce qui signifie qu'il n'est pas valide avant une heure spécifiée. Les utilisations des tickets, par exemple, pour spécifier quels utilisateurs sont autorisés à obtenir quels types de ticket, sont définies par des *stratégies*. Les stratégies sont déterminées lors de l'installation ou de l'administration de Kerberos.

---

**Remarque** – Vous rencontrerez fréquemment les termes *informations d'identification* et *ticket*. Dans l'univers Kerberos, ils sont souvent utilisés de façon interchangeable. D'un point de vue technique, cependant, les informations d'identification correspondent à un ticket et à la *clé de session* pour cette session. Cette différence est expliquée plus en détail à la section “[Obtention de l'accès à un service à l'aide de Kerberos](#)” à la page 541.

---

Les sections suivantes expliquent davantage les processus d'authentification Kerberos.

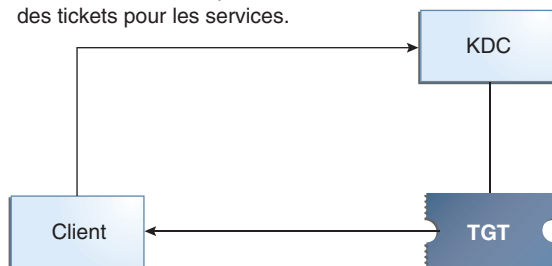
## Authentification initiale : le TGT

L'authentification Kerberos comprend deux phases : une authentification initiale qui autorise toutes les authentifications, puis les authentifications suivantes.

La figure ci-dessous illustre la manière dont l'authentification initiale a lieu.

FIGURE 19-1 Authentification Kerberos initiale pour une session

1. A la connexion (ou avec `kinit`), le client demande un TGT lui permettant d'obtenir des tickets pour les services.



2. KDC vérifie la base de données et envoie le TGT
3. Le client utilise un mot de passe pour déchiffrer le TGT, fournissant ainsi une identité ; il peut désormais utiliser le TGT pour obtenir d'autres tickets.

TGT = Ticket d'octroi de tickets  
KDC = Centre de distribution de clés

1. Un client (un utilisateur, ou un service comme NFS) commence une session Kerberos en demandant un *TGT* (ticket d'octroi de tickets) dans le KDC (centre de distribution de clés). Cette demande est souvent effectuée automatiquement à la connexion.

Un TGT est nécessaire pour obtenir d'autres tickets pour des services spécifiques. Considérez le TGT comme étant semblable à un passeport. Comme un passeport, le TGT vous identifie et vous permet d'obtenir de nombreux "visas", où les "visas" (tickets) ne sont pas des pays étrangers mais des machines distantes ou des services réseau. Comme les passeports et les visas, le TGT et les autres différents tickets ont une durée de vie limitée. La seule différence réside dans le fait que les commandes Kerberos voient que vous avez un passeport et qu'elles obtiennent les visas pour vous. Vous n'avez pas à effectuer les transactions vous-même.

Une autre analogie pour le TGT est celle du passe de ski de trois jours valable dans quatre différentes stations. Vous pouvez montrer le passe dans la station de votre choix et vous recevez un ticket pour les pistes correspondantes, tant que le passe n'a pas expiré. Une fois que vous avez accès aux pistes, vous pouvez skier autant que vous le voulez dans cette station. Si vous passez à une autre station le jour suivant, vous devez montrer votre passe à nouveau, et vous obtenez l'accès aux pistes de la nouvelle station. La différence réside dans le fait que les commandes Kerberos voient que vous avez un passe de ski de trois jours, et qu'elles obtiennent l'accès aux pistes pour vous. Ainsi, vous n'avez pas à effectuer les opérations vous-même.

2. Le KDC crée un TGT qu'il renvoie, sous forme chiffrée, au client. Le client déchiffre le TGT en utilisant le mot de passe du client.



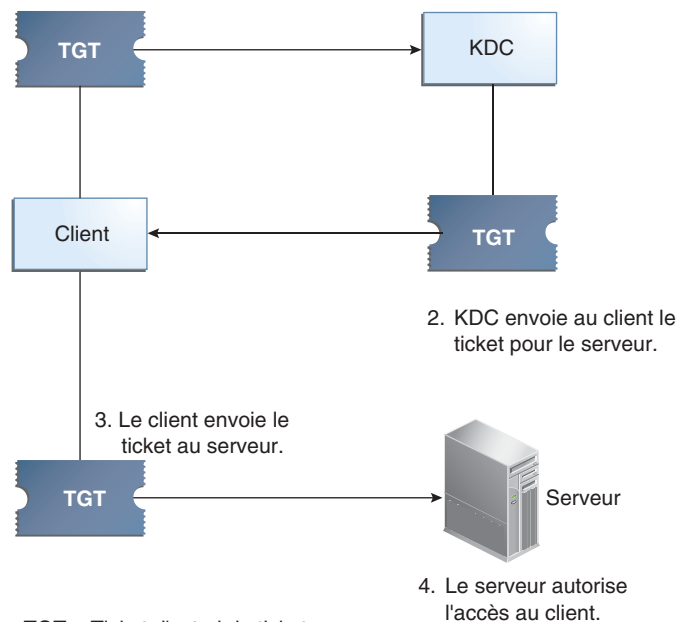
- Maintenant en possession d'un TGT en cours de validité, le client peut demander des tickets pour toutes sortes d'opérations réseau, telles que `rlogin` ou `telnet`, aussi longtemps que le TGT est valide. Ce ticket dure généralement quelques heures. A chaque fois que le client effectue une opération réseau unique, il demande un ticket pour cette opération au KDC.

## Authentifications Kerberos suivantes

Une fois que le client a reçu l'authentification initiale, chaque nouvelle authentification suit le modèle indiqué dans la figure ci-dessous.

FIGURE 19-2 Obtention de l'accès à un service à l'aide de l'authentification Kerberos

- Le client demande un ticket pour le serveur, envoie le TGT au KDC comme preuve d'identité.



- Le client demande un ticket au KDC pour un service particulier, par exemple, pour se connecter à distance à une autre machine, en envoyant au KDC son TGT comme preuve d'identité.
- Le KDC envoie le ticket pour le service spécifique au client.

Par exemple, si l'utilisateur joe demande l'accès à un système de fichiers NFS qui a été partagé avec krb5, l'authentification est nécessaire. Puisqu'il est déjà authentifié (c'est-à-dire, qu'il possède déjà un TGT), lorsqu'il tente d'accéder aux fichiers, le système client NFS obtient automatiquement et de façon transparente un ticket du KDC pour le service NFS.

Par exemple, supposons que l'utilisateur joe utilise `rlogin` sur le serveur `boston`. Comme il est déjà authentifié, c'est-à-dire qu'il a déjà un TGT, il obtient automatiquement et de façon transparente un ticket en tant que partie de la commande `rlogin`. Ce ticket lui permet de se connecter à distance à `boston` aussi souvent qu'il le souhaite jusqu'à expiration du ticket. Si joe veut se connecter à distance à la machine `denver`, il obtient un autre ticket, comme à l'étape 1.

3. Le client envoie le ticket au serveur.

Lors de l'utilisation du service NFS, le client NFS envoie le ticket automatiquement et de manière transparente au service NFS pour le serveur NFS.

4. Le serveur autorise l'accès au client.

Ces étapes montrent que le serveur ne communique pas toujours avec le KDC. Cependant, le serveur s'enregistre auprès du KDC, tout comme le premier client. A des fins de simplification, cette partie a été omise.

## Applications distantes Kerberos

Les commandes basées sur Kerberos disponibles pour un utilisateur comme joe sont les suivantes :

- `ftp`
- `rcp`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Ces applications sont les mêmes que les applications Solaris du même nom. Cependant, elles ont été étendues pour utiliser les principaux Kerberos pour authentifier les transactions, afin que vous disposiez d'une sécurité Kerberos. Pour plus d'informations sur les principaux, reportez-vous à la section [“Principaux Kerberos” à la page 355](#)

Ces commandes sont traitées plus en détail à la section [“Commandes utilisateur Kerberos” à la page 524](#).

## Principaux Kerberos

Un client dans le service Kerberos est identifié par son *principal*. Un principal est une identité unique à laquelle le KDC peut affecter les tickets. Un principal peut être un utilisateur, tel que joe, ou un service, tel que nfs ou telnet.

Par convention, un nom de principal est divisé en trois composants : le *primaire*, l'*instance* et le *domaine*. Un principal Kerberos type peut être, par exemple, joe/admin@ENG.EXAMPLE.COM.

Dans cet exemple :

- joe est le primaire. Le primaire peut être un nom d'utilisateur, comme ici, ou un service, comme nfs. Le primaire peut également être le mot host, ce qui signifie que ce principal est un principal de service qui est configuré pour fournir divers services réseau, ftp, rcp, rlogin etc.
- admin est l'instance. Une instance est facultative dans le cas de principaux d'utilisateur, mais elle est nécessaire pour les principaux de service. Par exemple, si l'utilisateur joe agit parfois en tant qu'administrateur système, il peut utiliser joe/admin pour se distinguer dans son identité d'utilisateur habituelle. De même, si joe a des comptes sur deux hôtes différents, il peut utiliser deux noms de principal avec différentes instances, par exemple, joe/denver.example.com et joe/boston.example.com. Notez que le service Kerberos traite joe et joe/admin comme deux principaux totalement différents.

Dans le cas d'un principal de service, l'instance est le nom d'hôte complet.

bigmachine.eng.example.com est un exemple d'une telle instance. Le principal ou l'instance pour cet exemple pourrait être ftp/bigmachine.eng.example.com ou host/bigmachine.eng.example.com.

- ENG.EXAMPLE.COM est le domaine Kerberos. Les domaines sont abordés dans [“Domaines Kerberos” à la page 355](#).

Les éléments suivants sont tous les noms de principaux valides :

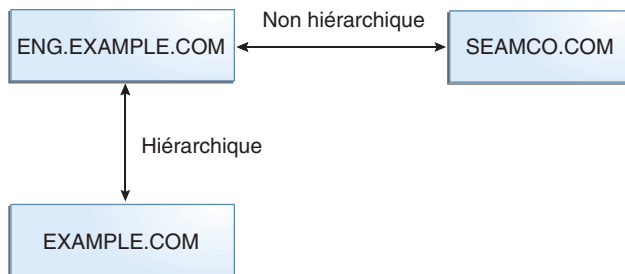
- joe
- joe/admin
- joe/admin@ENG.EXAMPLE.COM
- nfs/host.eng.example.com@ENG.EXAMPLE.COM
- host/eng.example.com@ENG.EXAMPLE.COM

## Domaines Kerberos

Un *domaine* est un réseau logique qui définit un groupe de systèmes sous le même *KDC maître*. La [Figure 19–3](#) montre comment les domaines peuvent se rapporter les uns aux autres. Certains domaines sont hiérarchiques, où un domaine est un surensemble de l'autre domaine. Dans le cas contraire, les domaines sont non hiérarchiques (ou "directs") et le mappage entre les deux domaines doit être défini. Une fonction du service Kerberos est d'autoriser l'authentification au

sein des domaines. Chaque domaine a seulement besoin de disposer d'une entrée de principal pour l'autre domaine dans son KDC. Cette fonction Kerberos est appelée *authentification inter-domaine*.

FIGURE 19-3 Domaines Kerberos



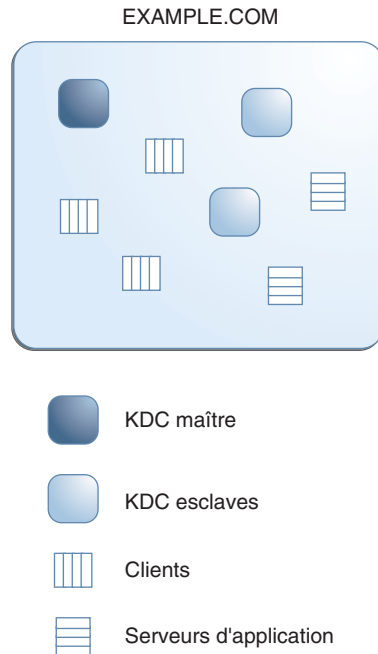
## Serveurs Kerberos

Chaque domaine doit inclure un serveur qui gère la copie principale de la base de données du principal. Ce serveur est appelé le *serveur KDC maître*. En outre, chaque domaine doit contenir au moins un *serveur KDC esclave*, qui contient des copies de la base de données du principal. Le serveur KDC maître et le serveur KDC esclave créent tous deux des tickets utilisés pour établir l'authentification.

Le domaine peut également inclure un *serveur d'application* Kerberos. Ce serveur permet d'accéder aux services utilisant Kerberos (tels que ftp, telnet, rsh et NFS). Si vous avez installé SEAM 1.0 ou 1.0.1, le domaine peut inclure un serveur d'application de réseau Kerberos, mais ce logiciel n'a pas été inclus avec ces versions.

La figure suivante illustre le contenu possible d'un domaine.

FIGURE 19-4 Domaine Kerberos typique



## Services de sécurité Kerberos

En plus d'assurer l'authentification sécurisée des utilisateurs, le service Kerberos fournit deux services de sécurité :

- **Intégrité** : tout comme l'authentification permet de s'assurer que les clients sur un réseau sont bien ceux qu'ils prétendent être, l'intégrité des données permet de s'assurer que les données qu'ils envoient sont valides et qu'elles n'ont pas été falsifiées pendant le transport. L'intégrité est assurée par l'intermédiaire de la somme de contrôle des données. L'intégrité inclut également l'authentification de l'utilisateur.
- **Confidentialité** : la confidentialité renforce la sécurité. La confidentialité n'inclut pas seulement la vérification de l'intégrité des données transmises, mais elle chiffre en outre les données avant leur transmission, afin de les protéger contre les écoutes électroniques. La confidentialité permet également d'authentifier les utilisateurs.

Les développeurs peuvent concevoir des applications basées sur RPC pour choisir un service de sécurité en utilisant l'interface de programmation RPCSEC\_GSS.

# Composants des différentes versions Kerberos

Les composants du service Kerberos ont été inclus dans de nombreuses versions. A l'origine, le service Kerberos et les modifications apportées au système d'exploitation de base pour la prise en charge du service Kerberos ont été distribués sous le nom du produit SEAM (Sun Enterprise Authentication Mechanism). A mesure que d'autres composants du produit SEAM ont été inclus dans le logiciel Oracle Solaris, le contenu de la version Oracle Solaris a diminué. A partir de la version Oracle Solaris 10, tous les composants du produit SEAM sont inclus, de sorte que le produit SEAM n'est pas nécessaire. Le nom de produit SEAM figure dans la documentation pour des raisons historiques.

Le tableau suivant décrit les composants inclus dans chaque version. Les versions de produit sont répertoriées dans l'ordre chronologique. Tous les composants sont décrits dans les sections suivantes.

**TABEAU 19-1** Contenu des versions Kerberos

| Nom de version                                               | Sommaire                                                                |
|--------------------------------------------------------------|-------------------------------------------------------------------------|
| SEAM 1.0 dans Solaris Easy Access Server 3.0                 | Version complète du service Kerberos pour les versions Solaris 2.6 et 7 |
| Service Kerberos dans la version Solaris 8                   | Logiciel client Kerberos uniquement                                     |
| SEAM 1.0.1 dans Solaris 8 Admin Pack                         | KDC Kerberos et applications distantes pour la version Solaris 8        |
| Service Kerberos dans la version Solaris 9                   | Fonctionnalité KDC et logiciel client uniquement                        |
| SEAM 1.0.2                                                   | Applications distantes Kerberos pour la version Solaris 9               |
| Service Kerberos démarrant dans la version Oracle Solaris 10 | Version complète du service Kerberos avec améliorations                 |

Pour plus d'informations les améliorations incluses dans la version Oracle Solaris 10, reportez-vous à la section [Composants Kerberos](#).

## Composants Kerberos

Similaire à la distribution par MIT du produit Kerberos V5, le service Kerberos dans la version Oracle Solaris comprend les éléments suivants :

- KDC (Key Distribution Center, centre de distribution de clés) :
  - Démon d'administration de base de données Kerberos : kadmind.
  - Démon de traitement des tickets Kerberos : krb5kdc.

- Programmes d'administration de base de données : `kadmin` (maître uniquement), `kadmin.local` et `kdb5_util`.
- Logiciel de propagation de base de données : `kprop` (esclave uniquement) et `kpropd`.
- Programmes utilisateur de gestion des informations d'identification : `kinit`, `klist` et `kdestroy`.
- Programme utilisateur de modification du mot de passe Kerberos : `kpasswd`.
- Applications distantes : `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` et `telnet`.
- Démons d'application distante : `ftpd`, `rlogind`, `rshd`, `sshd` et `telnetd`.
- Utilitaire d'administration de `keytab` : `ktutil`.
- GSS-API (API de service de sécurité générique) : permet aux applications d'utiliser plusieurs mécanismes de sécurité sans avoir à recompiler l'application à chaque fois qu'un nouveau mécanisme est ajouté. GSS-API utilise les interfaces standard permettant aux applications d'être portables pour de nombreux systèmes d'exploitation. GSS-API permet aux applications d'inclure les services de sécurité d'intégrité et de confidentialité, ainsi que l'authentification. Les commandes `ftp` et `ssh` utilisent GSS-API.
- RPCSEC\_GSS API : permet d'activer les services NFS afin d'utiliser l'authentification Kerberos. RPCSEC\_GSS est une variante de sécurité fournissant des services de sécurité indépendants des mécanismes utilisés. RPCSEC\_GSS est installé sur la couche GSS-API. N'importe quel mécanisme de sécurité enfichable basé sur GSS\_API peut être utilisé par des applications utilisant RPCSEC\_GSS.

En outre, le service Kerberos dans la version Oracle Solaris inclut les éléments suivants :

- Outil d'administration graphique Kerberos (`gkadmin`) : permet d'administrer les principaux et les stratégies des principaux. Cette interface graphique basée sur Java est une alternative à la commande `kadmin`.
- Module de service Kerberos V5 pour PAM : assure l'authentification, la gestion de compte, la gestion de session et la gestion des mots de passe pour le service Kerberos. Le module peut être utilisé pour que l'authentification Kerberos soit transparente pour l'utilisateur.
- Modules de noyau : fournissent des implémentations basées sur le noyau du service Kerberos pour une utilisation par le service NFS, ce qui améliore considérablement les performances.

## A propos de Kerberos dans la version Oracle Solaris 11

Cette section répertorie les modifications qui sont disponibles dans la version Oracle Solaris 11.

- Le logiciel Kerberos a été synchronisé avec la version MIT 1.8. Les fonctions suivantes ont été incluses :
  - Les types de chiffrement faible `arcfour-hmac-md5-exp`, `des-cbc-md5` et `des-cbc-crc` sont interdits par défaut. La déclaration `allow_weak_crypto = true` dans le fichier `/etc/krb5/krb5.conf` peut être ajoutée pour permettre l'utilisation d'algorithmes de chiffrement plus faible.
  - Dans le fichier `/etc/krb5/krb5.conf`, la relation `permitted_enctypes` peut prendre un mot-clé `DEFAULT` facultatif avec `+` ou `-` `enctyp_family` pour ajouter ou supprimer un type de chiffrement de l'ensemble par défaut.
  - Dans la plupart des cas, vous pouvez éliminer le besoin de la table de mappage `domain_realm` côté client en mettant en oeuvre une prise en charge de référence minimale dans le KDC et en fournissant les informations de mappage aux clients par l'intermédiaire de ce protocole. Les clients peuvent fonctionner sans table de mappage `domain_realm` en envoyant des demandes pour le principal de service `name/service/canonical-fqdn@LOCAL.REALM` au KDC local et en demandant des références. Cette fonctionnalité peut être limitée aux noms de principaux de service avec des types de nom spécifiques ou des formes précises. Le KDC ne peut utiliser que sa table de mappage `domain_realm`. Aucune requête bloquante à DNS ne peut être introduite.
  - Vous pouvez créer des alias pour des entrées de principal si vous utilisez un backend LDAP pour la base de données Kerberos. La prise en charge des alias de principal est utile si un service est accessible par différents noms d'hôte ou si le DNS n'est pas disponible pour normaliser le nom de l'hôte, ce qui signifie que la forme abrégée est utilisée. Vous pouvez utiliser un alias pour les différents noms de principaux qualifiant un service et le système n'a besoin que d'un ensemble de clés pour le service principal réel dans son fichier `keytab`.
  - Vous pouvez utiliser l'utilitaire `kvno` pour diagnostiquer les problèmes avec les clés du service principal qui sont stockées dans `/etc/krb5/krb5.keytab`.
  - La commande `kadmin ktadd` prend en charge l'option `-norandkey` qui empêche la commande `kadmin` de créer une nouvelle clé aléatoire. L'option `-norandkey` peut être utile lorsque vous souhaitez créer un `keytab` pour un principal dont la clé est dérivée d'un mot de passe. Vous pouvez créer un `keytab` servant à exécuter la commande `kinit` sans devoir spécifier un mot de passe.
  - Les principaux peuvent être bloqués après un certain nombre d'échecs de pré-authentification dans un délai imparti. Pour plus d'informations, reportez-vous à la section [“Procédure de configuration du verrouillage de compte”](#) à la page 426.



- L'indicateur OK\_AS\_DELEGATE permet au KDC de communiquer la stratégie du domaine local à un client indiquant si un serveur intermédiaire est autorisé à accepter des références déléguées. Pour plus d'informations, reportez-vous à la section [“Approbation de services pour la délégation” à la page 371](#).
- Un ensemble de points de suivi défini statiquement au niveau de l'utilisateur pour Kerberos a été ajouté. Ces sondes fournissent une vue logique des messages du protocole Kerberos. Reportez-vous à la section [“Utilisation de DTrace avec le service Kerberos” à la page 473](#) pour un exemple.
- Le script `kclient` a été amélioré. Ce script comprend la possibilité de joindre des serveurs Microsoft Active Directory. Pour plus d'informations, reportez-vous aux sections [“Procédure de configuration interactive d'un client Kerberos” à la page 413](#) et [“Procédure de configuration d'un client Kerberos pour un serveur Active Directory” à la page 416](#). En outre, le script contient une option `-T` qui peut être utilisé pour identifier le type de serveur KDC pour le client. Toutes les options de ce script sont abordées dans la page de manuel `kclient(1M)`.
- Le fichier `/etc/krb5/kadm5.keytab` n'est plus nécessaire. Les clés qui étaient stockées dans ce fichier sont désormais lues directement dans la base de données Kerberos.
- La prise en charge de l'accès aux enregistrements de principaux et de stratégie Kerberos à l'aide de LDAP à partir d'un serveur d'annuaire a été ajoutée. Cette modification simplifie l'administration et peut fournir une plus grande disponibilité, selon le déploiement des KDC et des serveurs d'annuaire. Reportez-vous à la section [“Gestion d'un KDC sur un serveur d'annuaire LDAP” à la page 450](#) pour obtenir une liste des procédures relatives à LDAP.
- La nouvelle commande `kdcmgr` peut être utilisée pour configurer automatiquement ou de façon interactive un KDC. Cette commande crée à la fois le serveur KDC maître et esclave. En outre, lorsqu'elle est utilisée avec l'option `status`, la commande `kdcmgr` affiche des informations sur un KDC qui est installé sur l'hôte local. Recherchez les pointeurs vers les procédures automatiques et interactives dans le [Tableau 21-1](#).
- La prise en charge des clients Oracle Solaris sans configuration supplémentaire a été ajoutée à cette version. Des modifications ont été apportées au service Kerberos et à certaines valeurs par défaut. Les clients Kerberos fonctionnent sans configuration côté client dans des environnements correctement configurés. Pour plus d'informations, reportez-vous à la section [“Options de configuration du client” à la page 369](#).



## Planification du service Kerberos

---

Ce chapitre doit être étudié par les administrateurs qui sont impliqués dans l'installation et la maintenance du service Kerberos. Le chapitre traite de plusieurs options d'installation et de configuration que les administrateurs doivent résoudre avant d'installer ou de configurer le service.

La liste suivante répertorie les sujets qu'un administrateur système ou d'autres membres du personnel technique compétent doivent étudier :

- “Intérêt de la planification des déploiements de Kerberos” à la page 363
- “Planification de domaines Kerberos” à la page 364
- “Mappage de noms d'hôtes sur des domaines” à la page 365
- “Noms des clients et des principaux de service” à la page 366
- “Ports pour les services d'administration et le KDC” à la page 367
- “Nombre de KDC esclaves” à la page 367
- “Choix du système de propagation de base de données” à la page 369
- “Synchronisation de l'horloge dans un domaine” à la page 369
- “Options de configuration du client” à la page 369
- “Amélioration de la sécurité de connexion des clients” à la page 370
- “Options de configuration de KDC” à la page 371
- “Approbation de services pour la délégation” à la page 371
- “Types de chiffrement Kerberos” à la page 372
- “URL d'aide en ligne dans l'outil d'administration graphique de Kerberos” à la page 373

### Intérêt de la planification des déploiements de Kerberos

Avant d'installer le service Kerberos, vous devez résoudre plusieurs problèmes de configuration. Bien que la modification de la configuration après l'installation initiale ne soit pas impossible, certaines modifications peuvent être difficiles à implémenter. En outre, certaines modifications impliquent que le KDC soit reconstruit, de sorte qu'il est préférable d'examiner les objectifs à long terme lorsque vous planifiez votre configuration de Kerberos.

Le déploiement d'une infrastructure Kerberos implique d'effectuer des tâches telles que l'installation de KDC, de créer des clés pour les hôtes et de faire migrer des utilisateurs. La reconfiguration d'un déploiement Kerberos peut être aussi difficile que l'exécution d'un déploiement initial, donc planifiez un déploiement avec soin pour éviter d'avoir à reconfigurer.

## Planification de domaines Kerberos

Un *domaine* est réseau logique qui définit un groupe de systèmes qui sont sous le même KDC maître. Comme pour l'établissement d'un nom de domaine DNS, les problèmes tels que le nom de domaine, le nombre et la taille de chaque domaine, ainsi que la relation d'un domaine à d'autres domaines pour l'authentification inter-domaine, doivent être résolus avant de configurer le service Kerberos.

### Noms de domaine

Les noms de domaine peuvent être constitués de n'importe quelle chaîne de caractères ASCII. En général, le nom de domaine est le même que celui de votre nom de domaine DNS, sauf que le nom de domaine est en majuscules. Cette convention permet de différencier les problèmes avec le service Kerberos des problèmes avec l'espace de noms DNS, tout en utilisant un nom familier. Si vous ne souhaitez pas utiliser DNS ou que vous choisissez d'utiliser une autre chaîne, vous pouvez utiliser n'importe quelle chaîne. Toutefois, le processus de configuration nécessite plus de travail. L'utilisation de noms de domaine qui suivent les conventions de désignation d'Internet est judicieuse.

### Nombre de domaines

Le nombre de domaines requis par votre installation dépend de plusieurs facteurs :

- Le nombre de clients à prendre en charge. Trop de clients dans un domaine rend l'administration plus difficile et finit par vous forcer à diviser le domaine. Les principaux facteurs qui déterminent le nombre de clients pouvant être pris en charge sont les suivants :
  - Quantité de trafic générée par chaque client Kerberos
  - Bande passante du réseau physique
  - Vitesse de l'hôte

Etant donné que chaque installation aura différentes limitations, aucune règle n'existe pour déterminer le nombre maximum de clients.

- La distance qui les sépare des clients. Configurer plusieurs petits domaines peut avoir un sens si les clients sont dans différentes régions.
- Le nombre d'hôtes disponibles pour être installés en tant que KDC. Chaque domaine doit disposer d'au moins deux serveurs KDC, un serveur maître et un serveur esclave.

L'alignement des domaines Kerberos avec les domaines d'administration est recommandé. Il convient de noter qu'un domaine Kerberos V peut s'étendre sur plusieurs sous-domaines du domaine DNS auquel le domaine correspond.

## Hiérarchie des domaines

Lorsque vous configurez plusieurs domaines pour l'authentification inter-domaine, vous devez décider comment lier les domaines entre eux. Vous pouvez établir une relation hiérarchique entre les domaines, ce qui fournit automatiquement les chemins d'accès aux domaines associés. Bien entendu, tous les domaines dans la chaîne hiérarchique doivent être configurés correctement. Les chemins d'accès automatiques peuvent alléger la charge administrative. Cependant, s'il existe de nombreux niveaux de domaines, il se peut que vous ne souhaitiez pas utiliser le chemin par défaut car cela nécessite trop de transactions.

Vous pouvez également choisir d'établir la relation de confiance de manière directe. Une relation de confiance directe est plus utile lorsqu'un trop grand nombre de niveaux hiérarchiques existent entre deux domaines ou lorsqu'il n'existe aucune relation hiérarchique. La connexion doit être définie dans le fichier `/etc/krb5/krb5.conf` sur tous les hôtes qui utilisent la connexion. Par conséquent, certains travaux supplémentaires sont nécessaires. La relation de confiance directe est également appelée relation transitive. Pour une introduction, reportez-vous à [“Domaines Kerberos” à la page 355](#). Pour les procédures de configuration de plusieurs domaines, reportez-vous à la section [“Configuration de l'authentification inter-domaine” à la page 397](#).

## Mappage de noms d'hôtes sur des domaines

Le mappage de noms d'hôtes sur des noms de domaines est défini dans la section `domain_realm` du fichier `krb5.conf`. Ces mappages peuvent être définis pour un domaine ou pour des hôtes spécifiques, selon les besoins.

Le DNS peut également être utilisé pour chercher des informations sur le KDC. L'utilisation du DNS facilite la modification des informations car vous n'avez pas besoin de modifier le fichier `krb5.conf` sur tous les clients chaque fois que vous apportez une modification. Pour plus d'informations, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

Les clients Solaris Kerberos peuvent mieux interopérer avec les serveurs Active Directory. Les serveurs Active Directory peuvent être configurés de façon à fournir le domaine au mappage d'hôte.

## Noms des clients et des principaux de service

Lorsque vous utilisez le service Kerberos, le DNS doit être activé sur tous les hôtes. Avec le DNS, le principal doit contenir le nom de domaine complet (FQDN, fully qualified domain name) de chaque hôte. Par exemple, si le nom d'hôte est `boston`, le nom de domaine DNS `example.com` et le nom de domaine `EXAMPLE.COM`, alors le nom de principal de l'hôte doit être `host/boston.example.com@EXAMPLE.COM`. Les exemples de ce manuel nécessitent que le DNS soit configuré et utilisent le nom de domaine complet pour chaque hôte.

Le service Kerberos normalise les noms d'alias d'hôtes par l'intermédiaire du DNS, et utilise le formulaire normalisé (cname) lors de la construction du principal de service pour le service associé. C'est pourquoi, lors de la création d'un principal de service, le composant nom d'hôte des noms des principaux de service doit être la forme normalisée du nom d'hôte du système qui héberge le service.

Ce qui suit est un exemple de la façon dont le service Kerberos normalise les noms d'hôte. Si un utilisateur utilise la commande `"ssh alpha.example.com"`, où `alpha.example.com` est un alias de nom d'hôte DNS pour le cname `beta.example.com`. Lorsque SSH appelle Kerberos et demande un ticket de service hôte pour `alpha.example.com`, le service Kerberos normalise `d'alpha.example.com` à `beta.example.com` et demande un ticket pour le principal de service `"host/beta.example.com"` au KDC.

Pour les noms de principal qui comprennent le nom de domaine complet (FQDN) de l'hôte, il est important de faire correspondre la chaîne qui décrit le nom de domaine DNS dans le fichier `/etc/resolv.conf`. Le service Kerberos requiert que le nom de domaine DNS soit en minuscules lorsque vous spécifiez le nom de domaine complet (FQDN) pour un principal. Le nom de domaine DNS peuvent inclure des majuscules et des minuscules, mais n'utilisez des lettres minuscules que lorsque vous créez un principal d'hôte. Par exemple, le nom de domaine DNS peut être `example.com`, `Example.COM` ou n'importe quelle autre variante. Le nom du principal d'hôte sera toujours `host/boston.example.com@EXAMPLE.COM`.

En outre, l'utilitaire de gestion des services a été configuré de manière à ce qu'un grand nombre de ces démons ou commandes ne démarre pas si le service de client DNS n'est pas en cours d'exécution. Les démons `kdb5_util`, `kadmind` et `kproxd`, ainsi que la commande `kprop`, sont configurés pour dépendre du service DNS. Pour exploiter au mieux les fonctionnalités disponibles à l'aide du service Kerberos et SMF, vous devez activer le service de client DNS sur tous les hôtes.

## Ports pour les services d'administration et le KDC

Par défaut, les ports 88 et 750 sont utilisés pour le KDC, et le port 749 est utilisé pour le démon d'administration du KDC. Des numéros de port différents peuvent être utilisés. Toutefois, si vous modifiez les numéros de port, alors les fichiers `/etc/services` et `/etc/krb5/krb5.conf` doivent être modifiés sur chaque client. En plus de ces fichiers, le fichier `/etc/krb5/kdc.conf` doit être mis à jour sur chaque KDC.

## Nombre de KDC esclaves

Les KDC esclaves génèrent des informations d'identification tout comme le KDC maître. Les KDC esclaves fournissent une sauvegarde si le maître n'est plus disponible. Chaque domaine doit avoir au moins un KDC esclave. Des KDC esclaves supplémentaires peuvent être nécessaires, selon les facteurs suivants :

- Nombre de segments physiques dans le domaine. Normalement, le réseau doit être défini de manière à ce que chaque segment puisse fonctionner, au moins de manière minimale, sans le reste du domaine. Pour ce faire, un KDC doit être accessible à partir de chaque segment. Le KDC dans cette instance pourrait être un maître ou un esclave.
- Nombre de clients dans le domaine. En ajoutant plusieurs serveurs KDC esclaves, vous pouvez réduire la charge des serveurs actuels.

Il est possible d'ajouter un trop grand nombre de KDC esclaves. N'oubliez pas que la base de données KDC doit être diffusée vers chaque serveur. Par conséquent, plus le nombre de serveurs KDC installés est grand, plus la mise à jour des données dans l'ensemble du domaine peut être longue. En outre, puisque chaque esclave conserve une copie de la base de données KDC, le risque de violation de sécurité augmente avec le nombre d'esclaves.

Par ailleurs, un ou plusieurs KDC esclaves peuvent facilement être configurés de façon à être échangés avec le KDC maître. L'avantage de configurer au moins un KDC esclave de cette manière est de pouvoir disposer d'un système préconfiguré facile à échanger avec le KDC maître en cas de panne de celui-ci. Pour obtenir des instructions sur la manière de configurer un KDC esclave échangeable, reportez-vous à la section [“Echange d'un KDC maître et d'un KDC esclave” à la page 428](#).

# Mappage d'informations d'identification GSS sur des informations d'identification UNIX

Le service Kerberos fournit un mappage par défaut des noms d'informations d'identification GSS sur les noms d'utilisateurs UNIX (UID) pour les applications GSS nécessitant ce mappage, comme NFS. Les noms d'informations d'identification GSS sont équivalents aux noms de principaux Kerberos lors de l'utilisation du service Kerberos. L'algorithme de mappage par défaut consiste à prendre un composant du nom de principal Kerberos et d'utiliser ce composant, qui est le nom primaire du principal, pour rechercher l'UID. La recherche est effectuée dans le domaine par défaut ou tout domaine autorisé à l'aide du paramètre `auth_to_local_realm` dans `/etc/krb5/krb5.conf`. Par exemple, le nom de principal d'utilisateur `bob@EXAMPLE.COM` est mappé sur l'UID de l'utilisateur UNIX nommé `bob` à l'aide de la table de mots de passe. Le nom de principal d'utilisateur `bob/admin@EXAMPLE.COM` n'est pas mappé, car le nom de principal comprend un composant d'instance d'`admin`. Si les mappages par défaut pour les informations d'identification de l'utilisateur sont suffisants, la table des informations d'identification GSS n'a pas besoin d'être renseignée. Dans les versions précédentes, le remplissage de la table des informations d'identification GSS était nécessaire pour faire fonctionner le service NFS. Si le mappage par défaut n'est pas suffisant, par exemple si vous souhaitez mapper un nom de principal contenant un composant d'instance, d'autres méthodes doivent être utilisées. Pour plus d'informations, consultez les références suivantes :

- [“Procédure de création d'une table d'informations d'identification” à la page 405](#)
- [“Procédure d'ajout d'une entrée unique à la table d'informations d'identification” à la page 406](#)
- [“Procédure de mappage d'informations d'identification entre domaines” à la page 407](#)
- [“Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 473](#)

## Migration automatique d'utilisateur vers un domaine Kerberos

Les utilisateurs UNIX ne disposant pas de comptes utilisateur valables dans le domaine Kerberos par défaut peuvent être automatiquement migrés à l'aide de la structure PAM. Plus précisément, le module `pam_krb5_migrate` est utilisé dans la pile d'authentification du service PAM. Les services sont configurés de sorte que, chaque fois qu'un utilisateur ne disposant pas d'un principal Kerberos parvient à se connecter à un système à l'aide de son mot de passe, un principal Kerberos est automatiquement créé pour celui-ci. Le mot de passe du nouveau principal est le même que le mot de passe UNIX. Reportez-vous à la section [“Procédure de configuration de la migration automatique des utilisateurs dans un domaine Kerberos” à la page 424](#) pour obtenir des instructions sur la façon d'utiliser le module `pam_krb5_migrate`.



## Choix du système de propagation de base de données

La base de données stockée sur le KDC maître doit être régulièrement propagée aux KDC esclaves. Vous pouvez configurer la propagation de la base de données pour qu'elle soit incrémentielle. Le processus incrémentiel propage uniquement les informations mises à jour aux KDC esclaves, plutôt que l'intégralité de la base de données. Pour plus d'informations sur la propagation de base de données, reportez-vous à la section [“Administration de la base de données Kerberos” à la page 433](#).

Si vous n'utilisez pas la propagation incrémentielle, l'une des premières questions à résoudre est la fréquence de mise à jour des KDC esclaves. Le besoin d'avoir des informations à jour disponibles pour tous les clients doit être comparé à la durée nécessaire pour effectuer la mise à jour.

Dans les installations de grande taille avec de nombreux KDC dans un domaine, un ou plusieurs esclaves peuvent propager les données de manière à ce que le processus s'effectue en parallèle. Cette stratégie permet de réduire le temps de la mise à jour, mais il augmente également le niveau de complexité dans l'administration du domaine. Pour obtenir une description complète de cette stratégie, reportez-vous à la section [“Configuration d'une propagation parallèle” à la page 446](#).

## Synchronisation de l'horloge dans un domaine

Tous les hôtes qui participent au système d'authentification Kerberos doivent avoir leurs horloges internes synchronisées dans une durée maximale spécifiée. Appelée *écart d'horloge*, cette fonction fournit un autre contrôle de sécurité Kerberos. Si l'écart d'horloge est dépassé entre des hôtes participants, les demandes sont rejetées.

Une façon de synchroniser toutes les horloges est d'utiliser le logiciel NTP (Network Time Protocol). Pour plus d'informations, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos” à la page 427](#). D'autres façons de synchroniser les horloges sont disponibles, de sorte que l'utilisation du protocole NTP n'est pas nécessaire. Cependant, une forme ou une autre de synchronisation doit être utilisée pour empêcher les défaillances d'accès dues à un écart d'horloge.

## Options de configuration du client

Une nouvelle fonctionnalité de la version Solaris 10 est l'utilitaire de configuration `kclient`. L'utilitaire peut être exécuté en mode interactif ou non interactif. En mode interactif, l'utilisateur est invité à entrer des valeurs de paramètre spécifiques à Kerberos, ce qui permet à l'utilisateur d'effectuer des modifications sur une installation existante lors de la configuration du client. En mode non interactif, un fichier avec des valeurs de paramètre prédéfinies est

utilisé. Les options de ligne de commande peuvent également être utilisées en mode non interactif. Les modes interactif et non interactif nécessitent moins d'étapes que le processus manuel, ce qui devrait rendre le processus plus rapide et moins sujet aux erreurs.

Dans la version Solaris Express Developer Edition 1/08 des modifications ont été apportées pour autoriser un client Kerberos sans configuration. Si ces règles sont respectées dans votre environnement, aucune procédure de configuration explicite n'est nécessaire pour un client Solaris Kerberos :

- Le service DNS est configuré de façon à renvoyer des enregistrements SRV aux KDC.
- Le nom de domaine correspond au nom de domaine DNS ou le KDC prend en charge les références.
- Le client Kerberos ne requiert pas de fichier keytab.

Dans certains cas, il peut être préférable de configurer explicitement le client Kerberos :

- Si les références ne sont pas utilisées, la logique d'absence de configuration se base sur le nom de domaine DNS de l'hôte pour déterminer le domaine. Cela introduit un petit risque pour la sécurité, mais celui-ci est beaucoup plus faible que l'activation de `dns_lookup_realm`.
- Le module `pam_krb5` s'appuie sur une entrée de clé d'hôte dans le keytab. Cette condition peut être désactivée dans le fichier `krb5.conf`, cependant ce n'est pas recommandé pour des raisons de sécurité. Reportez-vous à la page de manuel [krb5.conf\(4\)](#).
- Le processus sans configuration est moins efficace que la configuration directe et se repose plus sur le DNS. Le processus effectue plus de recherches DNS que les clients configurés directement.

Pour une description de tous les processus de configuration des clients, reportez-vous à la section "[Configuration des clients Kerberos](#)" à la page 410

## Amélioration de la sécurité de connexion des clients

A l'ouverture de la session d'un client, le module `pam_krb5` vérifie que le KDC ayant émis le dernier TGT est le même KDC ayant émis le principal d'hôte du client stocké dans `/etc/krb5/krb5.keytab`. Le module `pam_krb5` vérifie le KDC lorsque le module est configuré dans la pile d'authentification. Pour certaines configurations, telles que des clients DHCP ne stockant pas de principal d'hôte de client, cette vérification doit être désactivée. Pour désactiver cette vérification, vous devez définir l'option `verify_ap_req_no_fail` dans le fichier `krb5.conf` sur `false`. Pour plus d'informations, reportez-vous à la section "[Procédure de désactivation de la vérification du ticket d'octroi de tickets](#)" à la page 422

## Options de configuration de KDC

Il existe plusieurs façons de configurer un KDC. Les façons les plus simples utilisent l'utilitaire `kdcmgr` pour configurer le KDC automatiquement ou de façon interactive. La version automatique nécessite que vous utilisiez les options de ligne de commande afin de définir les paramètres de configuration. Cette méthode est particulièrement utile pour les scripts. La version interactive vous invite à fournir toutes les informations nécessaires. Reportez-vous au [Tableau 21-1](#) pour accéder à des pointeurs vers les instructions d'utilisation de cette commande.

La prise en charge de l'utilisation de LDAP pour gérer les fichiers de base de données de Kerberos est également disponible. Reportez-vous à [“Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP” à la page 384](#) pour obtenir des instructions. L'utilisation de LDAP simplifie l'administration des sites qui nécessitent une meilleure coordination entre les bases de données Kerberos et la configuration existante de leur serveur d'annuaire.

## Approbation de services pour la délégation

Pour certaines applications, un client peut avoir besoin de déléguer l'autorité à un serveur pour qu'il agisse en son nom lorsqu'il contacte d'autres services. Le client doit transférer des informations d'identification à un serveur intermédiaire. La capacité du client à obtenir un ticket de service à un serveur ne communique aucune information au client permettant de savoir si le serveur doit être autorisé à accepter des références déléguées. L'option `ok_to_auth_as_delegate` de la commande `kadmin` permet à un KDC de communiquer la stratégie du domaine local à un client indiquant si un serveur intermédiaire est autorisé à accepter de telles informations d'identification.

La copie d'indicateurs de ticket d'information d'identification dans la partie chiffrée de la réponse KDC peut comporter l'option `ok_to_auth_as_delegate` afin d'indiquer au client que le serveur spécifié dans le ticket a été déterminé par la stratégie du domaine comme étant un destinataire approprié de la délégation. Un client peut utiliser la présence de cette information pour déterminer s'il faut attribuer ou non des informations d'identification (en octroyant un proxy ou un TGT transmis) à ce serveur. Lors de la définition cette option, un administrateur doit tenir compte de la sécurité et de la position du serveur sur lequel le service s'exécute, et si le service requiert l'utilisation d'informations d'identification déléguées.

## Types de chiffrement Kerberos

Un *type de chiffrement* est un identificateur qui spécifie l'algorithme de chiffrement, le mode de chiffrement et les algorithmes de hachage utilisés dans le service Kerberos. Les clés dans le service Kerberos sont associées à un type de chiffrement pour identifier l'algorithme et le mode cryptographiques à utiliser lorsque le service effectue des opérations cryptographiques à l'aide de la clé. Types de chiffrement pris en charge :

- `des-cbc-md5`
- `des-cbc-crc`
- `des3-cbc-sha1-kd`
- `arcfour-hmac-md5`
- `arcfour-hmac-md5-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

---

**Remarque** – Dans les versions antérieures à Solaris 10 8/07, le type de chiffrement `aes256-cts-hmac-sha1-96` peut être utilisé avec le service Kerberos si les packages Strong Cryptographic non fournis en standard sont installés.

---

Si vous souhaitez modifier le type de chiffrement, vous devez le faire lors de la création d'une nouvelle base de données de principal. En raison de l'interaction entre le KDC, le serveur et le client, il est difficile de modifier le type de chiffrement sur une base de données existante. Laissez ces paramètres non définis, sauf si vous recréez la base de données. Pour plus d'informations, reportez-vous à la section [“Utilisation des types de chiffrement Kerberos”](#) à la page 544.

---

**Remarque** – Si vous avez un KDC maître installé n'exécutant pas la version Solaris 10, les KDC esclaves doivent être mis à niveau vers la version Solaris 10 avant de mettre à niveau le KDC maître. Un KDC maître Solaris 10 utilise les nouveaux types de chiffrement, ce qu'un esclave plus ancien n'est pas en mesure de faire.

---

Les types de chiffrement faible `arcfour-hmac-md5-exp`, `des-cbc-md5` et `des-cbc-crc` sont interdits par défaut dans la version 11 d'Oracle Solaris. Si vous souhaitez continuer à utiliser ces types de chiffrement, définissez `allow_weak_crypto = true` dans la section `libdefaults` du fichier `/etc/krb5/krb5.conf`.

## URL d'aide en ligne dans l'outil d'administration graphique de Kerberos

L'URL d'aide en ligne est utilisée par l'outil d'administration graphique de Kerberos, `gkadmin`, donc l'URL doit être correctement définie pour activer le menu Help Contents (Sommaire de l'aide). La version HTML de ce manuel peut être installée sur n'importe quel serveur approprié. Vous pouvez également décider d'utiliser les collections à l'adresse suivante :

<http://www.oracle.com/technetwork/indexes/documentation/index.html>.

L'URL est spécifiée dans le fichier `krb5.conf` lors de la configuration d'un hôte afin d'utiliser le service Kerberos. L'URL doit pointer vers la section “[outil SEAM](#)” à la page 476 in the *Administering Kerberos Principals and Policies (Tasks)* de ce manuel. Vous pouvez choisir une autre page HTML, si un autre emplacement est plus approprié.



## Configuration du service Kerberos (tâches)

---

Ce chapitre fournit les procédures de configuration pour les serveurs KDC, les serveurs d'application réseau, les serveurs NFS et les clients Kerberos. L'accès superutilisateur est requis pour un grand nombre de ces procédures ; elles doivent donc être utilisées par les administrateurs système ou les utilisateurs avancés. Les procédures de configuration inter-domaines et d'autres sujets liés aux serveurs KDC sont également abordés.

Liste des sujets abordés dans ce chapitre :

- “Configuration du service Kerberos (liste des tâches)” à la page 375
- “Configuration des serveurs KDC” à la page 377
- “Configuration des clients Kerberos” à la page 410
- “Configuration de l'authentification inter-domaine” à la page 397
- “Configuration des serveurs d'application réseau Kerberos” à la page 400
- “Configuration de serveurs NFS Kerberos” à la page 403
- “Synchronisation des horloges entre les KDC et les clients Kerberos” à la page 427
- “Echange d'un KDC maître et d'un KDC esclave” à la page 428
- “Administration de la base de données Kerberos” à la page 433
- “Renforcement de la sécurité des serveurs Kerberos” à la page 452

### Configuration du service Kerberos (liste des tâches)

Certaines parties de la procédure de configuration dépendent d'autres parties et doivent être effectuées selon un ordre spécifique. Ces procédures établissent souvent les services requis pour utiliser le service Kerberos. D'autres procédures ne sont pas dépendantes de l'ordre et peuvent être effectuées si nécessaire. La liste des tâches ci-dessous présente un ordre suggéré en vue d'une installation Kerberos.

| Tâche                                                            | Description                                                                                                                                                                                                                          | Voir                                                                               |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 1. Planification de votre installation Kerberos                  | Permet de résoudre les problèmes de configuration avant de démarrer le processus de configuration du logiciel. La planification permet d'économiser du temps et d'autres ressources sur le long terme.                               | Chapitre 20, "Planification du service Kerberos"                                   |
| 2. (Facultatif) Installation du NTP                              | Configure le logiciel NTP (Network Time Protocol) ou un autre protocole de synchronisation d'horloge. Pour que le service Kerberos fonctionne correctement, les horloges de tous les systèmes du domaine doivent être synchronisées. | "Synchronisation des horloges entre les KDC et les clients Kerberos" à la page 427 |
| 3. Configuration des serveurs KDC                                | Configure et construit des serveurs KDC maître et KDC esclave et la base de données KDC pour un domaine.                                                                                                                             | "Configuration des serveurs KDC" à la page 377                                     |
| 4. (Facultatif) Augmentation de la sécurité sur les serveurs KDC | Permet d'éviter les violations de sécurité sur le serveur KDC.                                                                                                                                                                       | "Procédure de restriction de l'accès aux serveurs KDC" à la page 453               |
| 5. (Facultatif) Configuration des serveurs KDC échangeables      | Facilite la tâche d'échange du serveur KDC maître et esclave.                                                                                                                                                                        | "Procédure de configuration d'un KDC échangeable" à la page 429                    |

## Configuration de services Kerberos supplémentaires (liste des tâches)

Une fois les étapes requises effectuées, les procédures suivantes peuvent être utilisées, le cas échéant.

| Tâche                                                           | Description                                                                                                              | Voir                                                                                  |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Configuration de l'authentification inter-domaine               | Active les communications entre deux domaines.                                                                           | "Configuration de l'authentification inter-domaine" à la page 397                     |
| Configuration de serveurs d'application Kerberos                | Permet à un serveur de prendre en charge des services tels que ftp, telnet et rsh utilisant l'authentification Kerberos. | "Configuration des serveurs d'application réseau Kerberos" à la page 400              |
| Configuration des clients Kerberos                              | Permet à un client d'utiliser des services Kerberos.                                                                     | "Configuration des clients Kerberos" à la page 410                                    |
| Configuration du serveur NFS Kerberos                           | Permet à un serveur de partager un système de fichiers requérant l'authentification Kerberos.                            | "Configuration de serveurs NFS Kerberos" à la page 403                                |
| Augmentation du niveau de sécurité sur un serveur d'application | Augmente la sécurité sur un serveur d'application en restreignant l'accès aux transactions authentifiées uniquement.     | "Procédure d'activation des applications utilisant Kerberos uniquement" à la page 452 |



# Configuration des serveurs KDC

Une fois que vous avez installé le logiciel Kerberos, vous devez configurer les serveurs KDC. La configuration d'un KDC maître et d'au moins un KDC esclave fournit le service émetteur des informations d'identification. Ces informations d'identification étant la base du service Kerberos, les KDC doivent être installés avant de tenter d'effectuer d'autres tâches.

La différence principale entre un KDC maître et un KDC esclave est que seul le KDC maître peut traiter les demandes d'administration de base de données. Par exemple, la modification d'un mot de passe ou l'ajout d'un nouveau principal doivent s'effectuer sur le KDC maître. Ces modifications peuvent alors être propagées aux KDC esclaves. Les KDC esclaves et maître génèrent tous deux des informations d'identification. Cette fonction fournit une redondance au cas où le KDC maître ne répond pas.

TABLEAU 21-1 Configuration de serveurs KDC (liste des tâches)

| Tâche                                   | Description                                                                                                                                                                      | Voir                                                                                                                |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Configuration d'un KDC maître.          | Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus automatique, opération appropriée pour les scripts.                  | <a href="#">“Procédure de configuration automatique d'un KDC maître” à la page 378</a>                              |
|                                         | Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus automatique, opération suffisante pour la plupart des installations. | <a href="#">“Procédure de configuration interactive d'un KDC maître” à la page 379</a>                              |
|                                         | Configure et construit le serveur KDC maître et une base de données d'un domaine à l'aide d'un processus manuel, opération requise pour les installations plus complexes.        | <a href="#">“Procédure de configuration manuelle d'un KDC maître” à la page 380</a>                                 |
|                                         | Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus manuel et à l'aide de LDAP pour le KDC.                              | <a href="#">“Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP” à la page 384</a> |
| Configuration d'un serveur KDC esclave. | Configure et construit un serveur KDC esclave pour un domaine à l'aide d'un processus automatique, opération appropriée pour les scripts                                         | <a href="#">“Procédure de configuration automatique d'un KDC esclave” à la page 391</a>                             |
|                                         | Configure et construit un serveur KDC esclave pour un domaine à l'aide d'un processus automatique, opération suffisante pour la plupart des installations.                       | <a href="#">“Procédure de configuration interactive d'un KDC esclave” à la page 392</a>                             |
|                                         | Configure et construit le serveur KDC esclave à l'aide d'un processus manuel, opération requise pour les installations plus complexes.                                           | <a href="#">“Procédure de configuration manuelle d'un KDC esclave” à la page 393</a>                                |

TABLEAU 21-1 Configuration de serveurs KDC (liste des tâches) (Suite)

| Tâche                                                  | Description                                                                                     | Voir                                                                                         |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Actualisation des clés principales sur un serveur KDC. | Met à jour la clé de session sur un serveur KDC pour utiliser de nouveaux types de chiffrement. | <a href="#">“Procédure d’actualisation des clés TGS sur un serveur maître” à la page 397</a> |

## ▼ Procédure de configuration automatique d'un KDC maître

Dans la version Oracle Solaris 11, un KDC maître peut être configuré automatiquement à l'aide de la procédure suivante.

- 1 **Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175.](#)

- 2 **Créez le KDC.**

Exécutez l'utilitaire `kdcmgr` pour créer le KDC. Vous devez fournir à la fois le mot de passe de la clé maître et le mot de passe du principal d'administration.

```
kdc1# kdcmgr -a kws/admin -r EXAMPLE.COM create master

Starting server setup
-----

Setting up /etc/krb5/kdc.conf

Setting up /etc/krb5/krb5.conf

Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:      <Type the password>
Re-enter KDC database master key to verify:  <Type it again>

Authenticating as principal root/admin@EXAMPLE.COM with password.
WARNING: no policy specified for kws/admin@EXAMPLE.COM; defaulting to no policy
Enter password for principal "kws/admin@EXAMPLE.COM":      <Type the password>
Re-enter password for principal "kws/admin@EXAMPLE.COM":      <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.

Setting up /etc/krb5/kadm5.acl.

-----
Setup COMPLETE.
```

```
kdc1#
```

## ▼ Procédure de configuration interactive d'un KDC maître

Dans la version Oracle Solaris, un KDC maître peut être configuré de manière interactive à l'aide de la procédure suivante.

- 1 **Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

- 2 **Créez le KDC.**

Exécutez l'utilitaire `kdcmgr` pour créer le KDC. Vous devez fournir à la fois le mot de passe de la clé maître et le mot de passe du principal d'administration.

```
kdc1# kdcmgr create master
```

```
Starting server setup
```

```
-----
Enter the Kerberos realm: EXAMPLE.COM
```

```
Setting up /etc/krb5/kdc.conf
```

```
Setting up /etc/krb5/krb5.conf
```

```
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
```

```
You will be prompted for the database Master Password.
```

```
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key:      <Type the password>
```

```
Re-enter KDC database master key to verify:  <Type it again>
```

```
Enter the krb5 administrative principal to be created: kws/admin
```

```
Authenticating as principal root/admin@EXAMPLE.COM with password.
```

```
WARNING: no policy specified for kws/admin@EXAMPLE.COM; defaulting to no policy
```

```
Enter password for principal "kws/admin@EXAMPLE.COM":      <Type the password>
```

```
Re-enter password for principal "kws/admin@EXAMPLE.COM":    <Type it again>
```

```
Principal "kws/admin@EXAMPLE.COM" created.
```

```
Setting up /etc/krb5/kadm5.acl.
```

```
-----
Setup COMPLETE.
```

kdc1#

### Exemple 21–1 Affichage de l'état d'un serveur KDC

La commande `kdcmgr status` peut être utilisée pour afficher des informations sur un serveur KDC maître ou esclave.

## ▼ Procédure de configuration manuelle d'un KDC maître

Dans cette procédure, la propagation incrémentielle est configurée. En outre, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- admin principal = `kws/admin`
- Aide en ligne URL =  
`http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html`

---

**Remarque** – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "[URL d'aide en ligne dans l'outil d'administration graphique de Kerberos](#)" à la page 373.

---

**Avant de commencer** Cette procédure nécessite que l'hôte soit configuré pour utiliser DNS. Pour obtenir des instructions de nommage spécifiques afin de déterminer si ce maître doit être échangeable, reportez-vous à la section "[Echange d'un KDC maître et d'un KDC esclave](#)" à la page 428.

**1 Connectez-vous en tant que superutilisateur au KDC maître.**

**2 Editez le fichier de configuration Kerberos (`krb5.conf`).**

Vous devez modifier les noms de domaine et les noms de serveurs. Pour une description complète de ce fichier, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
    }
```

```
[domain_realm]
    .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
    kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html
    }
```

Dans cet exemple, les lignes pour `default_realm`, `kdc`, `admin_server` et toutes les entrées `domain_realm` ont été modifiées. En outre, la ligne définissant `help_url` a été modifiée.

---

**Remarque** – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_etypes` ou `default_tgs_etypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “[Utilisation des types de chiffrement Kerberos](#)” à la page 544.

---

### 3 Editez le fichier de configuration KDC (`kdc.conf`).

Vous devez modifier le nom de domaine. Pour une description complète de ce fichier, reportez-vous à la page de manuel [kdc.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
    }
```

Dans cet exemple, la définition du nom de domaine dans la section `realms` a été modifiée. En outre, dans la section `realms`, des lignes ont été ajoutées pour activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal.

**Remarque** – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `permitted_enctypes`, `supported_enctypes` ou `master_key_type`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “[Utilisation des types de chiffrement Kerberos](#)” à la page 544.

---

#### 4 Créez la base de données KDC à l'aide de la commande `kdb5_util`.

La commande `kdb5_util` crée la base de données KDC. En outre, lorsqu'elle est utilisée avec l'option `-s`, cette commande crée un fichier stash utilisé pour authentifier le KDC à lui-même avant le lancement des démons `kadmind` et `krb5kdc`.

```
kdc1 # /usr/sbin/kdb5_util create -s
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:      <Type the key>
Re-enter KDC database master key to verify:  <Type it again>
```

#### 5 Modifiez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC.

```
kws/admin@EXAMPLE.COM *
```

L'entrée donne au principal `kws/admin` du domaine `EXAMPLE.COM` la possibilité de modifier les principaux ou des stratégies dans le KDC. L'installation par défaut comprend un astérisque (\*) pour correspondre à tous les principaux `admin`. Cette valeur par défaut peut constituer un risque de sécurité, il est donc plus sûr d'inclure une liste de tous les principaux `admin`. Pour plus d'informations, reportez-vous à la page de manuel [kadm5.acl\(4\)](#).

#### 6 Démarrez la commande `kadmin.local` et ajoutez les principaux.

Les sous-étapes suivantes créent des principaux utilisés par le service Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

##### a. Ajoutez des principaux d'administration à la base de données.

Vous pouvez ajouter autant de principaux `admin` que nécessaire. Vous devez ajouter au moins un principal `admin` pour terminer le processus de configuration du KDC. Pour cet exemple, un principal `kws/admin` est ajouté. Vous pouvez remplacer `kws` par le nom de principal approprié.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM:  <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM:  <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

**b. Créez les principaux kprop.**

Le principal kprop est utilisé pour autoriser les mises à jour depuis le KDC maître.

```
kadmin.local: addprinc -randkey kprop/kdc1.example.com
Principal "kprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin.local:
```

**c. Quittez kadmin.local.**

Vous avez ajouté toutes les identités requises pour les prochaines étapes.

```
kadmin.local: quit
```

**7 Démarrez les démons Kerberos.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

**8 Démarrez kadmin et ajoutez d'autres principaux.**

A ce stade, vous pouvez ajouter les principaux à l'aide de l'outil d'administration graphique Kerberos. Pour ce faire, vous devez vous connecter avec l'un des noms de principal admin que vous avez précédemment créés dans cette procédure. Cependant, l'exemple de ligne de commande suivant est utilisé par souci de simplicité.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Créez l'host principal du KDC maître.**

L'hôte principal est utilisé par les applications utilisant Kerberos, notamment kprop, pour propager les modifications aux KDC esclaves. Ce principal est également utilisé pour fournir un accès à distance sécurisé au serveur KDC à l'aide d'applications, comme ssh. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. (Facultatif) Créez le principal kclient.**

Ce principal est utilisé par l'utilitaire kclient au cours de l'installation d'un client Kerberos. Si vous n'avez pas l'intention d'utiliser cet utilitaire, vous n'avez pas besoin d'ajouter le principal. Les utilisateurs de l'utilitaire kclient doivent utiliser ce mot de passe.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM: <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

**c. Ajoutez l'host principal au fichier keytab du KDC maître.**

L'ajout de l'hôte principal au fichier keytab autorise ce principal à être utilisé automatiquement par des serveurs d'application tels que sshd.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**d. Quittez kadmin.**

```
kadmin: quit
```

**9 (Facultatif) Synchronisez l'horloge des KDC maître en utilisant NTP ou un autre mécanisme de synchronisation d'horloge.**

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

**10 Configurez les KDC esclaves.**

Pour assurer la redondance, veillez à installer au moins un KDC esclave. Pour obtenir des instructions spécifiques, reportez-vous à la section [“Procédure de configuration manuelle d'un KDC esclave”](#) à la page 393.

## ▼ Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP

Utilisez la procédure ci-dessous pour configurer un KDC pour l'utilisation d'un serveur de données LDAP.

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- Serveur d'annuaire = `dsserver.example.com`
- admin principal = `kws/admin`



- FMRI pour le service LDAP =  
svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1
- Aide en ligne URL =  
[http://download.oracle.com/docs/cd/E23824\\_01/html/821-1456/aadmin-23.html](http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html)

---

**Remarque** – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "[URL d'aide en ligne dans l'outil d'administration graphique de Kerberos](#)" à la page 373.

---

**Avant de commencer**

Cette procédure nécessite également que l'hôte soit configuré pour utiliser DNS. Pour de meilleures performances, installez le KDC et le service d'annuaire LDAP sur le même serveur. En outre, un serveur d'annuaire doit être en cours d'exécution. La procédure ci-dessous fonctionne avec des serveurs utilisant la version Sun Directory Server Enterprise Edition 7.0.

**1 Connectez-vous en tant que superutilisateur au KDC.**

**2 Configurez le KDC maître afin qu'il utilise SSL pour atteindre le serveur d'annuaire.**

Les étapes suivantes permettent de configurer un KDC de la version Oracle Solaris pour qu'il utilise le certificat auto-signé Directory Server. Si le certificat est arrivé à expiration, suivez les instructions de renouvellement de certificat dans la section "[To Manage Self-Signed Certificates](#)".

**a. Sur le serveur d'annuaire, exportez le certificat de serveur d'annuaire auto-signé.**

```
# /export/sun-ds6.1/ds6/bin/dsadm show-cert -F der /export/sun-ds6.1/directory2 \
defaultCert > /tmp/defaultCert.cert.der
```

**b. Sur le KDC maître, importez le certificat du serveur d'annuaire.**

```
# pktool setpin keystore=nss dir=/var/ldap
# chmod a+r /var/ldap/*.db
# pktool import keystore=nss objtype=cert trust="CT" infile=/tmp/defaultCert.certutil.der \
label=defaultCert dir=/var/ldap
```

**c. Sur le KDC maître, vérifiez que SSL fonctionne.**

Cet exemple suppose que l'entrée `cn=directory manager` dispose de privilèges d'administration.

```
/usr/bin/ldapsearch -Z -P /var/ldap -D "cn=directory manager" \
-h dsserver.example.com -b "" -s base objectclass=*
```

```
Subject:
"CN=dsserver.example.com,CN=636,CN=Directory Server,O=Example Corporation
```

Notez que l'entrée `CN=dsserver.example.com` doit inclure le nom d'hôte complet, pas une version abrégée.

**3 Renseignez l'annuaire LDAP, si nécessaire.**

#### 4 Ajoutez le schéma Kerberos pour le schéma existant.

```
# ldapmodify -h dsserver.example.com -D "cn=directory manager" -f /usr/share/lib/ldif/kerberos.ldif
```

#### 5 Créez le conteneur Kerberos dans l'annuaire LDAP.

Ajoutez les entrées suivantes au fichier `krb5.conf`.

##### a. Définissez le type de base de données.

Ajoutez une entrée pour définir le `database_module` sur la section `realms`.

```
database_module = LDAP
```

##### b. Définissez le module de base de données.

```
[dbmodules]
LDAP = {
    ldap_kerberos_container_dn = "cn=krbcontainer,dc=example,dc=com"
    db_library = kldap
    ldap_kdc_dn = "cn=kdc service,ou=profile,dc=example,dc=com"
    ldap_kadmin_dn = "cn=kadmin service,ou=profile,dc=example,dc=com"
    ldap_cert_path = /var/ldap
    ldap_servers = ldaps://dsserver.example.com
}
```

##### c. Créez le KDC dans l'annuaire LDAP.

Cette commande crée `krbcontainer` et plusieurs autres objets. Elle crée également un fichier `stash` de clé principale `/var/krb5/.k5.EXAMPLE.COM`.

```
# kdb5_ldap_util -D "cn=directory manager" create -P abcd1234 -r EXAMPLE.COM -s
```

#### 6 Dissimulez les mots de passe KDC de liaison DN (Distinguished Name, nom distinctif).

Ces mots de passe sont utilisés par le KDC lorsqu'il se connecte au DS. Le KDC utilise des rôles différents en fonction du type d'accès utilisé par le KDC.

```
# kdb5_ldap_util stashsrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
# kdb5_ldap_util stashsrvpw "cn=kadmin service,ou=profile,dc=example,dc=com"
```

#### 7 Ajoutez des rôles de service KDC.

##### a. Créez un fichier `kdc_roles.ldif` avec un contenu comme suit :

```
dn: cn=kdc service,ou=profile,dc=example,dc=com
cn: kdc service
sn: kdc service
objectclass: top
objectclass: person
userpassword: test123

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: test123
```

## b. Créez des entrées de rôle dans l'annuaire LDAP

```
# ldapmodify -a -h dsserver.example.com -D "cn=directory manager" -f kdc_roles.ldif
```

## 8 Définissez les listes de contrôle d'accès (ACL) pour les rôles relatifs au KDC.

```
# cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
# Set kadmin ACL for everything under krbcontainer.
dn: cn=krbcontainer,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///cn=krbcontainer,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
    acl kadmin ACL; allow (all)\
    userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)

# Set kadmin ACL for everything under the people subtree if there are
# mix-in entries for krb princis:
dn: ou=people,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///ou=people,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
    acl kadmin ACL; allow (all)\
    userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)
EOF
```

## 9 Editez le fichier de configuration Kerberos (krb5.conf).

Vous devez modifier les noms de domaine et les noms de serveurs. Pour une description complète de ce fichier, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM

#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
    kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html
    }
```

Dans cet exemple, les lignes pour `default_realm`, `kdc`, `admin_server` et toutes les entrées `domain_realm` ont été modifiées. En outre, la ligne définissant `help_url` a été modifiée.

---

**Remarque** – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_enctypes` ou `default_tgs_enctypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “[Utilisation des types de chiffrement Kerberos](#)” à la page 544.

---

## 10 Editez le fichier de configuration KDC (`kdc.conf`).

Vous devez modifier le nom de domaine. Pour une description complète de ce fichier, reportez-vous à la page de manuel [kdc.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_uologsize = 1000
    }
```

Dans cet exemple, la définition du nom de domaine dans la section `realms` a été modifiée. En outre, dans la section `realms`, des lignes ont été ajoutées pour activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal.

---

**Remarque** – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `permitted_enctypes`, `supported_enctypes` ou `master_key_type`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “[Utilisation des types de chiffrement Kerberos](#)” à la page 544.

---

## 11 Modifiez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC.

```
kws/admin@EXAMPLE.COM *
```

L'entrée donne au principal `kws/admin` du domaine `EXAMPLE.COM` la possibilité de modifier les principaux ou des stratégies dans le KDC. L'installation par défaut comprend un astérisque (\*) pour correspondre à tous les principaux `admin`. Cette valeur par défaut peut constituer un risque de sécurité, il est donc plus sûr d'inclure une liste de tous les principaux `admin`. Pour plus d'informations, reportez-vous à la page de manuel [kadm5.acl\(4\)](#).

## 12 Démarrez la commande `kadmin.local` et ajoutez les principaux.

Les sous-étapes suivantes créent des principaux utilisés par le service Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

### a. Ajoutez des principaux d'administration à la base de données.

Vous pouvez ajouter autant de principaux `admin` que nécessaire. Vous devez ajouter au moins un principal `admin` pour terminer le processus de configuration du KDC. Pour cet exemple, un principal `kws/admin` est ajouté. Vous pouvez remplacer `kws` par le nom de principal approprié.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM: <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

### b. Quittez `kadmin.local`.

Vous avez ajouté toutes les identités requises pour les prochaines étapes.

```
kadmin.local: quit
```

## 13 (Facultatif) Configurez les dépendances LDAP pour les services Kerberos.

Si LDAP et les serveurs KDC sont en cours d'exécution sur le même hôte et que le service LDAP est configuré avec un FMRI SMF, ajoutez une dépendance de service LDAP pour les démons Kerberos. Cette dépendance redémarre le service KDC si le service LDAP est redémarré.

### a. Ajoutez la dépendance au service `krb5kdc`.

```
# svccfg -s security/krb5kdc
svc:/network/security/krb5kdc> addpg dsins1 dependency
svc:/network/security/krb5kdc> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/krb5kdc> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/krb5kdc> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/krb5kdc> setprop dsins1/type = astring: "service"
svc:/network/security/krb5kdc> exit
```

### b. Ajoutez la dépendance au service `kadmin`.

```
# svccfg -s security/kadmin
svc:/network/security/kadmin> addpg dsins1 dependency
svc:/network/security/kadmin> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmin> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/kadmin> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmin> setprop dsins1/type = astring: "service"
svc:/network/security/kadmin> exit
```

## 14 Démarrez les démons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

## 15 Démarrez `kadmin` et ajoutez d'autres principaux.

A ce stade, vous pouvez ajouter les principaux à l'aide de l'outil d'administration graphique Kerberos. Pour ce faire, vous devez vous connecter avec l'un des noms de principal `admin` que vous avez précédemment créés dans cette procédure. Cependant, l'exemple de ligne de commande suivant est utilisé par souci de simplicité.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

### a. Créez l'host principal du KDC maître.

L'host principal est utilisé par les applications utilisant Kerberos, notamment `klist` et `kprop`. Les clients utilisent ce principal lors du montage d'un système de fichiers NFS authentifié. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

### b. (Facultatif) Créez le principal `clnt`.

Ce principal est utilisé par l'utilitaire `clnt` au cours de l'installation d'un client Kerberos. Si vous n'avez pas l'intention d'utiliser cet utilitaire, vous n'avez pas besoin d'ajouter le principal. Les utilisateurs de l'utilitaire `clnt` doivent utiliser ce mot de passe.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

### c. Ajoutez l'hôte principal au fichier `keytab` du KDC maître.

L'ajout de l'hôte principal au fichier `keytab` autorise ce principal à être utilisé de manière automatique.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### d. Quittez `kadmin`.

```
kadmin: quit
```

**16 (Facultatif) Synchronisez l'horloge des KDC maître en utilisant NTP ou un autre mécanisme de synchronisation d'horloge.**

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

**17 Configurez les KDC esclaves.**

Pour assurer la redondance, veillez à installer au moins un KDC esclave. Pour obtenir des instructions spécifiques, reportez-vous à la section [“Procédure de configuration manuelle d'un KDC esclave”](#) à la page 393.

## ▼ Procédure de configuration automatique d'un KDC esclave

Dans la version Oracle Solaris, un KDC esclave peut être configuré automatiquement à l'aide de la procédure suivante.

**1 Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

**2 Créez le KDC.**

Exécutez l'utilitaire `kdcmgr` pour créer le KDC. Vous devez fournir à la fois le mot de passe de la clé maître et le mot de passe du principal d'administration.

```
kdc2# kdcmgr -a kws/admin -r EXAMPLE.COM create -m kdc1 slave
```

```
Starting server setup
```

```
-----
```

```
Setting up /etc/krb5/kdc.conf
```

```
Setting up /etc/krb5/krb5.conf
```

```
Obtaining TGT for kws/admin ...
```

```
Password for kws/admin@EXAMPLE.COM: <Type the password>
```

```
Setting up /etc/krb5/kadm5.acl.
```

```
Setting up /etc/krb5/kpropd.acl.
```

```
Waiting for database from master...
```

```
Waiting for database from master...
```

```
Waiting for database from master...
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
Enter KDC database master key:      <Type the password>

-----
Setup COMPLETE.

kdc2#
```

## ▼ Procédure de configuration interactive d'un KDC esclave

Utilisez la procédure suivante pour configurer un KDC esclave en mode interactif.

- 1 **Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

- 2 **Créez le KDC.**

Exécutez l'utilitaire `kdcmgr` pour créer le KDC. Vous devez fournir à la fois le mot de passe de la clé maître et le mot de passe du principal d'administration.

```
kdc1# kdcmgr create slave

Starting server setup
-----

Enter the Kerberos realm: EXAMPLE.COM
What is the master KDC's host name?: kdc1

Setting up /etc/krb5/kdc.conf

Setting up /etc/krb5/krb5.conf
Obtaining TGT for kws/admin ...
Password for kws/admin@EXAMPLE.COM:      <Type the password>

Setting up /etc/krb5/kadm5.acl.

Setting up /etc/krb5/kpropd.acl.

Waiting for database from master...
Waiting for database from master...
Waiting for database from master...
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
Enter KDC database master key:      <Type the password>
```



```
-----
Setup COMPLETE.
```

```
kdc2#
```

## ▼ Procédure de configuration manuelle d'un KDC esclave

Dans cette procédure, un nouveau KDC esclave nommé `kdc2` est configuré. En outre, la propagation incrémentielle est configurée. Cette procédure utilise les paramètres de configuration ci-dessous :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com`
- `admin principal` = `kws/admin`

### Avant de commencer

Le KDC maître doit être configuré. Pour obtenir des instructions spécifiques afin de déterminer si cet esclave doit être échangeable, reportez-vous à la section [“Echange d'un KDC maître et d'un KDC esclave”](#) à la page 428.

#### 1 Sur le KDC maître, connectez-vous en tant que superutilisateur.

#### 2 Sur le KDC maître, démarrez `kadmin`.

Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lors de la configuration du KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

#### a. Sur le KDC maître, ajoutez des principaux d'hôtes esclaves à la base de données, si ce n'est pas déjà fait.

Pour que l'esclave fonctionne, il doit avoir un hôte principal. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey host/kdc2.example.com
Principal "host/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. Sur le KDC maître, créez le principal kprop.**

Le principal kprop est utilisé pour autoriser la propagation incrémentielle à partir du KDC maître.

```
kadmin: addprinc -randkey kprop/kdc2.example.com
Principal "kprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

**c. Quittez kadmin.**

```
kadmin: quit
```

**3 Sur le KDC maître, modifiez le fichier de configuration Kerberos (krb5.conf).**

Vous devez ajouter une entrée pour chaque esclave. Pour une description complète de ce fichier, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/krb5.conf
.
.
[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
    }
```

**4 Sur le KDC maître, ajoutez une entrée kprop au fichier kadm5.acl.**

Cette entrée permet au KDC maître de recevoir des demandes de propagation incrémentielle pour le serveur kdc2.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kprop/kdc2.example.com@EXAMPLE.COM p
```

**5 Sur le KDC maître, redémarrez kadmind pour utiliser les nouvelles entrées dans le fichier kadm5.acl.**

```
kdc1 # svcadm restart network/security/kadmin
```

**6 Sur tous les KDC esclaves, copiez les fichiers d'administration à partir du serveur KDC maître.**

Cette étape doit être effectuée sur tous les KDC esclaves, car le serveur KDC maître a mis à jour des informations requises par chaque serveur KDC. Vous pouvez utiliser ftp ou tout autre mécanisme de transfert similaire pour extraire des copies des fichiers suivants du KDC maître :

- /etc/krb5/krb5.conf
- /etc/krb5/kdc.conf

**7 Sur tous les KDC esclaves, ajoutez une entrée pour le KDC maître et le KDC esclave dans le fichier de configuration de propagation de base de données, `kpropd.acf`.**

Ces informations doivent être mises à jour sur tous les serveurs KDC esclaves.

```
kdc2 # cat /etc/krb5/kpropd.acf
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

**8 Sur tous les KDC esclaves, assurez-vous que le fichier d'ACL Kerberos, `kadm5.acf`, n'est pas renseigné.**

Un fichier `kadm5.acf` non modifié ressemble à ce qui suit :

```
kdc2 # cat /etc/krb5/kadm5.acf
*/admin@__default_realm__ *
```

Si le fichier contient des entrées `kprop`, supprimez-les.

**9 Sur le nouvel esclave, modifiez une entrée de `kdc.conf`.**

Remplacez l'entrée `sunw_dbprop_master_ologsize` par une entrée définissant `sunw_dbprop_slave_poll`. L'entrée définit la durée d'interrogation sur deux minutes.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acf
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_slave_poll = 2m
    }
```

**10 Sur le nouvel esclave, démarrez la commande `kadmin`.**

Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lors de la configuration du KDC maître.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Ajoutez l'hôte principal de l'esclave au fichier `keytab` de l'esclave en utilisant `kadmin`.**

Cette entrée permet à `kprop` et à d'autres applications utilisant Kerberos de fonctionner.

Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: ktadd host/kdc2.example.com
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

```
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type Triple DES cbc
  mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type ArcFour
  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode
  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**b. Ajoutez le principal kiprop au fichier keytab du KDC esclave.**

L'ajout du principal kiprop au fichier krb5.keytab permet à la commande kpropd de s'authentifier elle-même lors du lancement de la propagation incrémentielle.

```
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
  mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**c. Quittez kadmin.**

```
kadmin: quit
```

**11 Sur le nouvel esclave, démarrez le démon de propagation Kerberos.**

```
kdc2 # svcadm enable network/security/krb5_prop
```

**12 Sur le nouvel esclave, créez un fichier stash à l'aide de kdb5\_util.**

```
kdc2 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key:      <Type the key>
```

**13 (Facultatif) Sur le nouveau KDC esclave, synchronisez l'horloge du KDC maître à l'aide du protocole NTP ou d'un autre mécanisme de synchronisation de l'horloge.**

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

**14 Sur le nouvel esclave, démarrez le démon KDC (krb5kdc).**

```
kdc2 # svcadm enable network/security/krb5kdc
```

## ▼ Procédure d'actualisation des clés TGS sur un serveur maître

Lorsque le principal de TGS (Ticket Granting Service, service d'octroi de tickets) n'a qu'une clé DES, ce qui est le cas pour les serveurs KDC créés avant la version Solaris 10, la clé restreint le type de chiffrement de la clé de session du TGT à DES. Si un KDC est mis à jour pour une version prenant en charge d'autres types de chiffrement renforcés, l'administrateur peut s'attendre à ce que le chiffrement renforcé soit utilisé pour toutes les clés de session générées par le KDC. En revanche, si les clés du principal de TGS ne sont pas actualisées pour inclure les nouveaux types de chiffrement, la clé de session du TGT restera limitée à DES. La procédure suivante actualise la clé afin que d'autres types de chiffrement puissent être utilisés.

### ● Actualisez la clé de principal du TGS.

```
kdc1 % /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

#### Exemple 21–2 Actualisation des clés de principal à partir d'un serveur maître

Si vous n'êtes pas connecté au KDC maître en tant que root, vous pouvez actualiser le principal de TGS à l'aide de la commande suivante :

```
kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
```

## Configuration de l'authentification inter-domaine

Il existe plusieurs manières de relier les domaines pour que les utilisateurs d'un domaine puissent être authentifiés dans un autre domaine. L'authentification inter-domaine est réalisée par la mise en place d'une clé secrète partagée par les deux domaines. La relation entre les domaines peut être hiérarchique ou directionnelle (voir [“Hiérarchie des domaines” à la page 365](#)).

## ▼ Procédure d'établissement de l'authentification inter-domaine hiérarchique

L'exemple de cette procédure utilise deux domaines, ENG.EAST.EXAMPLE.COM et EAST.EXAMPLE.COM. L'authentification inter-domaine est établie dans les deux directions. Cette procédure doit être effectuée sur le KDC maître dans les deux domaines.

### Avant de commencer

Le KDC maître de chaque domaine doit être configuré. Pour tester complètement le processus d'authentification, plusieurs clients Kerberos doivent être configurés.

**1 Connectez-vous en tant que superutilisateur au premier KDC maître.****2 Créez des principaux de service de TGT pour les deux domaines.**

Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lorsque vous avez configuré le KDC maître.

```
# /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM:      <Type password>
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM:      <Type password>
kadmin: quit
```

---

**Remarque** – Le mot de passe que vous avez spécifié pour chaque service de principal doit être identique dans les deux KDC. Par conséquent, le mot de passe pour le service principal `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` doit être le même dans les deux domaines.

---

**3 Ajoutez des entrées dans le fichier de configuration Kerberos (`krb5.conf`) pour définir les noms de domaine pour chaque domaine.**

```
# cat /etc/krb5/krb5.conf
[libdefaults]
.
.
[domain_realm]
    .eng.east.example.com = ENG.EAST.EXAMPLE.COM
    .east.example.com = EAST.EXAMPLE.COM
```

Dans cet exemple, les noms de domaine pour `ENG.EAST.EXAMPLE.COM` et `EAST.EXAMPLE.COM` sont définis. Il est important d'inclure d'abord le sous-domaine, parce que la recherche dans le fichier s'effectue du haut vers le bas.

**4 Copiez le fichier de configuration Kerberos pour tous les clients dans ce domaine.**

Pour que l'authentification inter-domaine fonctionne, la nouvelle version du fichier de configuration Kerberos (`/etc/krb5/krb5.conf`) doit être installée sur tous les systèmes (y compris les KDC esclaves et les autres serveurs).

**5 Répétez toutes ces étapes dans le second domaine.**

## ▼ Procédure d'établissement de l'authentification inter-domaine directe

L'exemple de cette procédure utilise deux domaines, `ENG.EAST.EXAMPLE.COM` et `SALES.WEST.EXAMPLE.COM`. L'authentification inter-domaine est établie dans les deux directions. Cette procédure doit être effectuée sur le KDC maître dans les deux domaines.

**Avant de commencer** Le KDC maître de chaque domaine doit être configuré. Pour tester complètement le processus d'authentification, plusieurs clients Kerberos doivent être configurés.

### 1 Connectez-vous en tant que superutilisateur à l'un des serveurs KDC maîtres.

### 2 Créez des principaux de service de TGT pour les deux domaines.

Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lorsque vous avez configuré le KDC maître.

```
# /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
Enter password for principal
krtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM: <Type the password>
kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal
krtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: <Type the password>
kadmin: quit
```

---

**Remarque** – Le mot de passe que vous avez spécifié pour chaque service de principal doit être identique dans les deux KDC. Par conséquent, le mot de passe pour le service principal `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` doit être identique dans les deux domaines.

---

### 3 Ajoutez des entrées dans le fichier de configuration Kerberos pour définir le chemin d'accès direct au domaine distant.

Cet exemple représente les clients dans le domaine `ENG.EAST.EXAMPLE.COM`. Vous pourriez avoir besoin de changer le nom de domaine pour obtenir les définitions adéquates dans le domaine `SALES.WEST.EXAMPLE.COM`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
.
.
.
[capaths]
ENG.EAST.EXAMPLE.COM = {
    SALES.WEST.EXAMPLE.COM = .
}
```

```
SALES.WEST.EXAMPLE.COM = {  
    ENG.EAST.EXAMPLE.COM = .  
}
```

**4 Copiez le fichier de configuration Kerberos pour tous les clients dans le domaine actuel.**

Pour que l'authentification inter-domaine fonctionne, la nouvelle version du fichier de configuration Kerberos (/etc/krb5/krb5.conf) doit être installée sur tous les systèmes (y compris les KDC esclaves et les autres serveurs).

**5 Répétez toutes ces étapes pour le second domaine.**

## Configuration des serveurs d'application réseau Kerberos

Les serveurs d'application réseau sont des hôtes fournissant un accès à l'aide d'une ou plusieurs applications réseau parmi les suivantes : ftp, rcp, rlogin, rsh, ssh et telnet. Seules quelques étapes sont nécessaires pour activer la version Kerberos de ces commandes sur un serveur.

### ▼ Procédure de configuration d'un serveur d'application réseau Kerberos

Cette procédure utilise les paramètres de configuration ci-dessous :

- Serveur d'application = boston
- admin principal = kws/admin
- Nom de domaine DNS = example.com
- Nom de domaine = EXAMPLE.COM

**Avant de commencer**

Cette procédure nécessite que le KDC maître ait été configuré. Pour tester complètement le processus, plusieurs clients Kerberos doivent être configurés.

**1 Connectez-vous en tant que superutilisateur au serveur**

**2 (Facultatif) Installez le client NTP ou un autre mécanisme de synchronisation d'horloge.**

Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

**3 Ajoutez des principaux pour le nouveau serveur et mettez à jour le fichier keytab du serveur.**

La commande suivante indique l'existence de l'hôte principal :

```
boston # klist -k |grep host  
4 host/boston.example.com@EXAMPLE.COM  
4 host/boston.example.com@EXAMPLE.COM  
4 host/boston.example.com@EXAMPLE.COM  
4 host/boston.example.com@EXAMPLE.COM
```



Si la commande ne renvoie pas de principal, créez de nouveaux comptes utilisateur en suivant les étapes ci-dessous.

L'utilisation de l'outil d'administration graphique Kerberos pour ajouter un principal est expliquée à la section [“Procédure de création d'un principal Kerberos” à la page 486](#). L'exemple dans les étapes suivantes montre comment ajouter les principaux requis à l'aide de la ligne de commande. Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lors de la configuration du KDC maître.

```
boston # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Créez l'host principal du serveur.

L'host principal est utilisé dans les cas suivants :

- Pour authentifier le trafic lors de l'utilisation des commandes à distance, comme rsh et ssh.
- Par pam\_krb5 afin d'empêcher les attaques par mystification de KDC en utilisant l'host principal pour vérifier que les informations d'identification Kerberos d'un utilisateur ont été obtenues auprès d'un KDC de confiance.
- Pour autoriser l'utilisateur root à acquérir automatiquement des informations d'identification Kerberos en l'absence d'un principal root. Cela peut être utile lors d'un montage NFS manuel où le partage requiert des informations d'identification Kerberos.

Ce principal est obligatoire si le trafic qui utilise l'application distante doit être authentifié à l'aide du service Kerberos. Si le serveur a plusieurs noms d'hôte associés, créez un principal pour chaque nom d'hôte sous la forme de nom de domaine complet(FQDN) du nom d'hôte.

```
kadmin: addprinc -randkey host/boston.example.com
Principal "host/boston.example.com" created.
kadmin:
```

#### b. Ajoutez l'host principal du serveur au fichier keytab du serveur.

Si la commande kadmin n'est pas en cours d'exécution, redémarrez-la avec une commande similaire à la suivante : /usr/sbin/kadmin -p kws/admin

Si le serveur a plusieurs noms d'hôte associés, ajoutez un principal au fichier keytab de chaque nom d'hôte.

```
kadmin: ktadd host/boston.example.com
Entry for principal host/boston.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode  
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.

kadmin:

**c. Quittez kadmin.**

kadmin: **quit**

## ▼ Procédure d'utilisation du service de sécurité générique avec Kerberos lors de l'exécution FTP

Le service de sécurité générique (GSS) peut être utilisé sur des applications pour faciliter l'utilisation de Kerberos pour l'authentification, l'intégrité et la confidentialité. Les étapes suivantes montrent comment activer le service GSS pour ProFTPD.

- 1 Connectez-vous en tant que superutilisateur au serveur FTP.**
- 2 Ajoutez des principaux pour le serveur FTP et mettez à jour le fichier keytab du serveur.**

Ces étapes ne sont peut-être pas nécessaires si les modifications ont été effectuées précédemment.

**a. Démarrez la commande kadmin.**

```
ftpserver1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**b. Ajoutez l'hôte principal de service pour le serveur FTP.**

kadmin: **addprinc -randkey host/ftpserver1.example.com**

**c. Ajoutez l'host principal de service au fichier keytab du serveur.**

kadmin: **ktadd host/ftpserver1.example.com**

- 3 Activez GSS pour le serveur FTP.**

Apportez les modifications suivantes au fichier /etc/proftpd.conf .

```
# cat /etc/proftpd.conf
#User      ftp
#Group      ftp

User        root
Group       root

UseIPv6     off

LoadModule  mod_gss.c

GSSEngine   on
GSSKeytab   /etc/krb5/krb5.keytab
```

#### 4 Redémarrez le serveur FTP.

```
# svcadm restart network/ftp
```

## Configuration de serveurs NFS Kerberos

Les services NFS utilisent les ID d'utilisateur (UID) UNIX pour identifier un utilisateur et ne peuvent pas utiliser directement les informations d'identification GSS. Pour traduire les données d'identification en UID, il peut être nécessaire de créer une table mappant les informations d'identification d'utilisateur et les UID UNIX. Pour plus d'informations sur le mappage par défaut des informations d'identification, reportez-vous à la section [“Mappage d'informations d'identification GSS sur des informations d'identification UNIX”](#) à la page 368. Les procédures décrites dans cette section se concentrent sur les tâches nécessaires pour configurer un serveur Kerberos NFS, administrer la table d'informations d'identification Kerberos, et initier des modes de sécurité pour les systèmes de fichiers montés sur NFS. La liste ci-dessous décrit les tâches traitées dans cette section.

TABLEAU 21-2 Configuration de serveurs Kerberos NFS (liste des tâches)

| Tâche                                                                                                                | Description                                                                                                                                                                                      | Voir                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Configuration d'un serveur NFS Kerberos                                                                              | Permet à un serveur de partager un système de fichiers requérant l'authentification Kerberos.                                                                                                    | <a href="#">“Procédure de configuration des serveurs NFS Kerberos”</a> à la page 404                                                 |
| Création d'une table d'informations d'identification                                                                 | Génère une table d'informations d'identification pouvant être utilisée pour assurer le mappage des informations d'identification GSS aux UID UNIX, si le mappage par défaut n'est pas suffisant. | <a href="#">“Procédure de création d'une table d'informations d'identification”</a> à la page 405                                    |
| Modification de la table d'informations d'identification qui mappe les informations d'identification et les UID UNIX | Met à jour les informations de la table d'informations d'identification.                                                                                                                         | <a href="#">“Procédure d'ajout d'une entrée unique à la table d'informations d'identification”</a> à la page 406                     |
| Mappage des informations d'identification entre deux domaines similaires                                             | Fournit des instructions sur la méthode de mappage des UID d'un domaine à un autre si les domaines partagent un fichier de mots de passe.                                                        | <a href="#">“Procédure de mappage d'informations d'identification entre domaines”</a> à la page 407                                  |
| Partage d'un système de fichiers à l'aide de l'authentification Kerberos                                             | Partage un système de fichiers avec des modes de sécurité de sorte que l'authentification Kerberos est requise.                                                                                  | <a href="#">“Procédure de configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos”</a> à la page 408 |

## ▼ Procédure de configuration des serveurs NFS Kerberos

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- Serveur NFS = `denver.example.com`
- `admin principal` = `kws/admin`

### 1 Connectez-vous en tant que superutilisateur au serveur NFS.

### 2 Remplissez les conditions préalables à la configuration d'un serveur Kerberos NFS.

Le KDC maître doit être configuré. Pour tester complètement le processus, vous avez besoin de plusieurs clients.

### 3 (Facultatif) Installez le client NTP ou un autre mécanisme de synchronisation d'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être synchronisée avec l'heure sur le serveur KDC dans une différence maximum définie par la relation `clockskew` dans le fichier `krb5.conf` pour que l'opération d'authentification réussisse. Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos” à la page 427](#).

### 4 Configurez le serveur NFS en tant que client Kerberos.

Suivez les instructions de la section [“Configuration des clients Kerberos” à la page 410](#).

### 5 Démarrez `kadmin`.

Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section [“Procédure de création d'un principal Kerberos” à la page 486](#). Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

#### a. Créez le principal de service NFS du serveur.

Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

Répétez cette étape pour chaque interface unique sur le système susceptible d'être utilisée pour accéder aux données NFS. Si un hôte possède plusieurs interfaces avec des noms uniques, chaque nom unique doit avoir son propre principal de service NFS.

```
kadmin: addprinc -randkey nfs/denver.example.com
Principal "nfs/denver.example.com" created.
kadmin:
```

**b. Ajoutez le principal de service du serveur NFS au fichier keytab du serveur.**

Répétez cette étape pour chaque principal de service dans l'[Étape a.](#)

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**c. Quittez kadmin.**

```
kadmin: quit
```

**6 (Facultatif) Créez les mappages d'informations d'identification GSS spéciaux, si nécessaire.**

Normalement, le service Kerberos génère des mappages appropriés entre les informations d'identification GSS et les UID UNIX. Le mappage par défaut est décrit dans la section [“Mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 368](#). Si le mappage par défaut n'est pas suffisant, reportez-vous à la section [“Procédure de création d'une table d'informations d'identification” à la page 405](#) pour plus d'informations.

**7 Partagez le système de fichiers NFS avec les modes de sécurité Kerberos.**

Pour plus d'informations, reportez-vous à la section [“Procédure de configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos” à la page 408](#).

## ▼ Procédure de création d'une table d'informations d'identification

La table d'informations d'identification `gsscred` est utilisée par un serveur NFS pour mapper les informations d'identification Kerberos à un UID. Par défaut, la première partie du nom du principal est mappée avec un nom de connexion UNIX. Pour que les clients NFS puissent monter des systèmes de fichiers à partir d'un serveur NFS à l'aide de l'authentification Kerberos, ce tableau doit être créé si le mappage par défaut n'est pas suffisant.

**1 Connectez-vous en tant que superutilisateur au serveur NFS.**

**2 Modifiez le fichier `/etc/gss/gsscred.conf` et changez le mécanisme de sécurité.**

Modifiez le mécanisme en `files`.

**3 Créez la table d'informations d'identification à l'aide de la commande `gsscred`.**

```
# gsscred -m kerberos_v5 -a
```

La commande `gsscred` rassemble les informations provenant de l'ensemble des sources répertoriées avec l'entrée `passwd` dans le fichier `svc:/system/name-service/switch:default`. Vous pouvez être amené à supprimer temporairement l'entrée `files`, si vous ne souhaitez pas que les entrées de mot de passe local soient incluses dans la table d'informations d'identification. Pour plus d'informations, reportez-vous à la page de manuel [gsscred\(1M\)](#).

## ▼ Procédure d'ajout d'une entrée unique à la table d'informations d'identification

**Avant de commencer**

Cette procédure nécessite que la table `gsscred` ait déjà été créée sur le serveur NFS. Pour obtenir des instructions, reportez-vous à la section “[Procédure de création d'une table d'informations d'identification](#)” à la page 405.

**1 Connectez-vous en tant que superutilisateur au serveur NFS.****2 Ajoutez une entrée à la table d'informations d'identification à l'aide de la commande `gsscred`.**

```
# gsscred -m mech [ -n name [ -u uid ] ] -a
```

*mech* Définit le mécanisme de sécurité à utiliser.

*name* Définit le nom de principal de l'utilisateur, tel que défini dans le KDC.

*uid* Définit l'UID de l'utilisateur, tel que défini dans la base de données de mots de passe.

*-a* Ajoute l'UID au mappage du nom de principal.

**Exemple 21–3 Ajout d'un principal à composants multiples à la table d'informations d'identification**

Dans l'exemple suivant, l'entrée est ajoutée à un principal appelé `sandy/admin` associé à l'UID 3736.

```
# gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

**Exemple 21-4** Ajout d'un principal à un domaine différent de la table d'informations d'identification

Dans l'exemple suivant, l'entrée est ajoutée à un principal appelé `sandy/admin@EXAMPLE.COM` associé à l'UID 3736.

```
# gsscred -m kerberos_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a
```

## ▼ Procédure de mappage d'informations d'identification entre domaines

Cette procédure assure le mappages d'informations d'identification approprié entre des domaines utilisant le même fichier de mots de passe. Dans cet exemple, les domaines `CORP.EXAMPLE.COM` et `SALES.EXAMPLE.COM` utilisent le même fichier de mots de passe. Les informations d'identification pour `bob@CORP.EXAMPLE.COM` et `bob@SALES.EXAMPLE.COM` sont mappées avec le même UID.

- 1 Connectez-vous au système client en tant que superutilisateur.
- 2 Sur le système client, ajoutez des entrées au fichier `krb5.conf`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = CORP.EXAMPLE.COM
.
[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

**Exemple 21-5** Mappage des informations d'identification entre domaines utilisant le même fichier de mot de passe

Cet exemple illustre le mappage d'informations d'identification approprié entre des domaines qui utilisent le même fichier de mots de passe. Dans cet exemple, les domaines `CORP.EXAMPLE.COM` et `SALES.EXAMPLE.COM` utilisent le même fichier de mots de passe. Les informations d'identification pour `bob@CORP.EXAMPLE.COM` et `bob@SALES.EXAMPLE.COM` sont mappées avec le même UID. Sur le système client, ajoutez des entrées au fichier `krb5.conf`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = CORP.EXAMPLE.COM
.
[realms]
```

```
CORP.EXAMPLE.COM = {  
    .  
    auth_to_local_realm = SALES.EXAMPLE.COM  
    .  
}
```

**Erreurs  
fréquentes**

Pour plus d'information sur le processus de dépannage des problèmes de mappage d'informations d'identification, reportez-vous à la section [“Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX”](#) à la page 473.

## ▼ Procédure de configuration d'un environnement NFS sécurisé avec plusieurs modes de sécurité Kerberos

Cette procédure permet à un serveur NFS de fournir un accès NFS sécurisé à l'aide de différents modes ou variantes de sécurité. Lorsqu'un client négocie une variante de sécurité avec le serveur NFS, la première variante proposée par le serveur auquel le client a accès est utilisée. Cette variante est utilisée pour toutes les demandes de client suivantes du système de fichiers partagé par le serveur NFS.

### 1 Connectez-vous en tant que superutilisateur au serveur NFS.

### 2 Vérifiez que le fichier keytab comporte un principal de service NFS.

La commande `klist` signale s'il existe un fichier keytab et affiche les principaux. Si les résultats indiquent qu'aucun fichier keytab ou principal de service NFS n'existe, vous devez vérifier que toutes les étapes décrites à la section [“Procédure de configuration des serveurs NFS Kerberos”](#) à la page 404 ont bien été effectuées dans leur totalité.

```
# klist -k  
Keytab name: FILE:/etc/krb5/krb5.keytab  
KVNO Principal  
-----  
3 nfs/denver.example.com@EXAMPLE.COM  
3 nfs/denver.example.com@EXAMPLE.COM  
3 nfs/denver.example.com@EXAMPLE.COM  
3 nfs/denver.example.com@EXAMPLE.COM
```

### 3 Activez les modes de sécurité Kerberos dans le fichier `/etc/nfssec.conf`.

Modifiez le fichier `/etc/nfssec.conf` et supprimez le `"#"` placé devant les modes de sécurité Kerberos.

```
# cat /etc/nfssec.conf  
.  
.  
#  
# Uncomment the following lines to use Kerberos V5 with NFS  
#  
krb5          390003  kerberos_v5      default -          # RPCSEC_GSS
```



```
krb5i          390004  kerberos_v5    default integrity    # RPCSEC_GSS
krb5p          390005  kerberos_v5    default privacy      # RPCSEC_GSS
```

#### 4 Partagez les systèmes de fichiers avec les modes de sécurité appropriés.

```
share -F nfs -o sec=mode file-system
```

*mode* Spécifie les modes de sécurité à utiliser lors du partage du système de fichiers. Lorsque plusieurs modes de sécurité sont utilisés, le premier mode figurant dans la liste est utilisé comme valeur par défaut.

*file-system* Définit le chemin d'accès au système de fichiers à partager.

Tous les clients tentant d'accéder à des fichiers dans le système de fichiers nommé requièrent l'authentification Kerberos. Pour accéder aux fichiers, le principal d'utilisateur sur le client NFS doit être authentifié.

#### 5 (Facultatif) Si l'agent de montage automatique est en cours d'utilisation, modifiez la base de données `auto_master` pour sélectionner un mode de sécurité autre que celui par défaut.

Vous n'avez pas besoin de suivre cette procédure si vous n'utilisez pas l'agent de montage automatique pour accéder au système de fichiers ou si la sélection par défaut du mode de sécurité est acceptable.

```
file-system auto_home -nosuid,sec=mode
```

#### 6 (Facultatif) Emettez manuellement la commande `mount` pour accéder au système de fichiers à l'aide d'un autre mode que celui par défaut.

Vous pouvez aussi utiliser la commande `mount` pour spécifier le mode de sécurité, mais cette alternative ne tire pas parti de l'agent de montage automatique.

```
# mount -F nfs -o sec=mode file-system
```

### Exemple 21-6 Partage d'un système de fichiers avec un mode de sécurité Kerberos

Dans cet exemple, l'authentification Kerberos doit aboutir avant que les fichiers puissent être accessibles via le service NFS.

```
# share -F nfs -o sec=krb5 /export/home
```

### Exemple 21-7 Partage d'un système de fichiers avec plusieurs modes de sécurité Kerberos

Dans cet exemple, les trois modes de sécurité Kerberos ont été sélectionnés. Le mode utilisé est négocié entre le client et le serveur NFS. Si le premier mode dans la commande échoue, le mode suivant est essayé. Pour plus d'informations, reportez-vous à la page de manuel [nfssec\(5\)](#).

```
# share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

# Configuration des clients Kerberos

Les clients Kerberos incluent tout hôte qui n'est pas un serveur KDC sur le réseau et qui doit utiliser les services Kerberos. Cette section décrit les procédures d'installation d'un client Kerberos, ainsi que des informations spécifiques sur l'utilisation de l'authentification root pour monter des systèmes de fichiers NFS.

## Configuration des clients Kerberos (liste des tâches)

La liste des tâches ci-dessous comprend toutes les procédures associées à la configuration des clients Kerberos. Chaque ligne comprend un identificateur de tâche, une description de la raison pour laquelle cette tâche doit être effectuée, suivie d'un lien vers la tâche.

| Tâche                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Voir                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Etablissement d'un profil d'installation client Kerberos                                           | Génère un profil d'installation client pouvant être utilisé pour installer automatiquement un client Kerberos.                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">"Procédure de création d'un profil d'installation de client Kerberos" à la page 411</a>                                                                                                                                                                                                                                                                                                                           |
| Configuration d'un client Kerberos                                                                 | <p>Installe manuellement un client Kerberos. Utilisez cette procédure si chaque installation de client requiert des paramètres d'installation uniques.</p> <p>Installe automatiquement un client Kerberos. Utilisez cette procédure si les paramètres d'installation sont identiques pour tous les clients.</p> <p>Installe interactivement un client Kerberos. Utilisez cette procédure si seuls quelques-uns des paramètres d'installation doivent être modifiés.</p> <p>Installe automatiquement un client Kerberos d'un serveur Active Directory.</p> | <p><a href="#">"Procédure de configuration manuelle d'un client Kerberos" à la page 417</a></p> <p><a href="#">"Procédure de configuration automatique d'un client Kerberos" à la page 411</a></p> <p><a href="#">"Procédure de configuration interactive d'un client Kerberos" à la page 413</a></p> <p><a href="#">"Procédure de configuration d'un client Kerberos pour un serveur Active Directory" à la page 416</a></p> |
| Autorisation donnée à un client d'accéder à un système de fichiers NFS en tant qu'utilisateur root | Crée un principal root sur le client, de manière à ce que le client puisse monter un système de fichiers NFS partagé avec accès root. Permet également au client de définir un accès root non interactif au système de fichiers NFS, de manière à ce que les tâches cron puissent s'exécuter.                                                                                                                                                                                                                                                             | <a href="#">"Procédure d'accès à un système de fichiers NFS protégé par Kerberos en tant qu'utilisateur root" à la page 423</a>                                                                                                                                                                                                                                                                                               |
| Désactivation de la vérification du KDC qui a émis un TGT (Ticket Granting Ticket) client          | Permet aux clients ne disposant pas d'un principal d'hôte stocké dans le fichier keytab local d'ignorer le contrôle de sécurité qui vérifie que le KDC ayant émis le TGT est le même serveur que celui ayant émis le principal d'hôte.                                                                                                                                                                                                                                                                                                                    | <a href="#">"Procédure de désactivation de la vérification du ticket d'octroi de tickets" à la page 422</a>                                                                                                                                                                                                                                                                                                                   |

## ▼ Procédure de création d'un profil d'installation de client Kerberos

Cette procédure permet de créer un profil kclient à utiliser lorsque vous installez un client Kerberos. L'utilisation du profil kclient permet de réduire les risques de faute de frappe. En outre, le profil permet de réduire l'intervention de l'utilisateur par rapport au processus interactif.

### 1 Connectez-vous en tant que superutilisateur.

### 2 Créez un profil d'installation kclient.

Un exemple de profil kclient pourrait ressembler à l'exemple suivant :

```
client# cat /net/denver.example.com/export/install/profile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

## ▼ Procédure de configuration automatique d'un client Kerberos

### Avant de commencer

Cette procédure utilise un profil d'installation. Reportez-vous à la section [“Procédure de création d'un profil d'installation de client Kerberos”](#) à la page 411.

### 1 Connectez-vous en tant qu'administrateur ou endosse un rôle ou nom d'utilisateur affecté au profil Kerberos Client Management (gestion de client Kerberos).

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

### 2 Exécutez le script d'installation kclient.

Vous devez fournir le mot de passe pour le principal clntconfig afin de terminer le processus.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile
```

```
Starting client setup
```

```
-----
kdc1.example.com
```

```
Setting up /etc/krb5/krb5.conf.
```

```
Obtaining TGT for clntconfig/admin ...
```

```
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>
```

```
nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

-----
Setup COMPLETE.

client#
```

### Exemple 21-8 Configuration automatique d'un client Kerberos avec des remplacements de ligne de commande

L'exemple suivant remplace les paramètres DNSARG et KDC définis dans le profil d'installation.

```
# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile\
-d dns_fallback -k kdc2.example.com

Starting client setup
-----

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

-----
Setup COMPLETE.

client#
```

## ▼ Procédure de configuration interactive d'un client Kerberos

Cette procédure utilise l'utilitaire d'installation `kcLient` sans profil d'installation. Dans la version Oracle Solaris 11, l'utilitaire `kcLient` a amélioré la facilité d'utilisation et le travail avec les serveurs Active Directory. Reportez-vous à la section “[Procédure de configuration d'un client Kerberos pour un serveur Active Directory](#)” à la page 416 pour plus d'informations. Reportez-vous à l'[Exemple 21–10](#) pour un exemple d'exécution de `kcLient` sur une version précédente.

- 1 **Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Client Management (gestion de client Kerberos).**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

- 2 **Exécutez le script d'installation `kcLient`.**

Vous devez fournir les informations suivantes :

- Nom de domaine Kerberos
- Nom d'hôte KDC maître
- Nom d'hôte KDC esclave
- Domaines à mettre en correspondance avec le domaine local
- Noms de service PAM et options à utiliser pour l'authentification Kerberos

- a. **Indiquez si le serveur KDC n'exécute pas une version d'Oracle Solaris.**

Si ce système est un client d'un serveur KDC qui n'exécute pas une version d'Oracle Solaris vous devez définir le type de serveur qui exécute le KDC. Les serveurs disponibles sont : Microsoft Active Directory, serveur KDC MIT, serveur KDC Heimdal et serveur KDC Shishi.

- b. **Sélectionnez si le DNS doit être utilisé pour les recherches Kerberos.**

Si vous utilisez DNS pour les recherches Kerberos, vous devez saisir l'option de recherche DNS que vous souhaitez utiliser. Les options valides sont `dns_lookup_kdc`, `dns_lookup_realm` et `dns_fallback`. Pour plus d'informations sur ces valeurs, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

- c. **Définissez le nom du domaine Kerberos et le nom d'hôte du KDC maître.**

Ces informations sont ajoutées au fichier de configuration `/etc/krb5/krb5.conf`.

- d. **Indiquez si des KDC esclaves existent.**

S'il existe des KDC esclaves dans le domaine, vous devez entrer les noms d'hôte des KDC esclaves. Ces informations sont utilisées pour créer d'autres entrées KDC dans le fichier de configuration du client.

**e. Indiquez si des clés de service ou d'hôte sont requises.**

Normalement, des clés de service ou d'hôte ne sont pas requise, sauf si le système client héberge des services utilisant Kerberos.

**f. Indiquez si le client est membre d'un cluster.**

Si le client est membre d'un cluster, vous devez fournir le nom logique du cluster. Le nom d'hôte logique est utilisé lorsque vous créez les clés de service, ce qui est requis lors de l'hébergement de services Kerberos de clusters.

**g. Identifiez les domaines ou hôtes à mapper avec le domaine actuel.**

Ce mappage permet à d'autres domaines d'appartenir au domaine par défaut du client.

**h. Indiquez si le client utilisera le NFS utilisant Kerberos.**

Les clés de service NFS doivent être créées si le client héberge des services NFS utilisant Kerberos.

**i. Indiquez si le fichier `/etc/pam.conf` doit être mis à jour.**

Cela vous permet de définir les services PAM utilisant Kerberos pour l'authentification. Vous devez entrer le nom du service et un indicateur indiquant comment l'authentification Kerberos est utilisée. Les options d'indicateur valides sont les suivantes :

- `first` : utilise l'authentification Kerberos en premier, puis utilise uniquement UNIX si l'authentification Kerberos échoue
- `only` : utilise l'authentification Kerberos uniquement
- `optional` : utilise l'authentification Kerberos de manière optionnelle

**j. Indiquez si le fichier maître `/etc/krb5/krb5.conf` doit être copié.**

Cette option permet d'utiliser des informations de configuration spécifiques lorsque les arguments de `kclient` ne sont pas suffisants.

### **Exemple 21–9** Exécution de l'utilitaire d'installation `kclient`

```
client# /usr/sbin/kclient
```

```
Starting client setup
```

```
-----
```

```
Is this a client of a non-Solaris KDC ? [y/n]: n
```

```
No action performed.
```

```
Do you want to use DNS for kerveros lookups ? [y/n]: n
```

```
No action performed.
```

```
Enter the Kerberos realm: EXAMPLE.COM
```

```
Specify the KDC hostname for the above realm: kdc1.example.com
```

Note, this system and the KDC's time must be within 5 minutes of each other for Kerberos to function. Both systems should run some form of time synchronization

```

system like Network Time Protocol (NTP).
Do you have any slave KDC(s) ? [y/n]: y
Enter a comma-separated list of slave KDC host names: kdc2.example.com

Will this client need service keys ? [y/n]: n
    No action performed.
Is this client a member of a cluster that uses a logical host name ? [y/n]: n
    No action performed.
Do you have multiple domains/hosts to map to realm ? [y/n]: y
Enter a comma-separated list of domain/hosts to map to the default realm: engineering.example.com, \
example.com

Setting up /etc/krb5/krb5.conf.

Do you plan on doing Kerberized nfs ? [y/n]: y
Do you want to update /etc/pam.conf ? [y/n]: y
Enter a comma-separated list of PAM service names in the following format:
service:{first|only|optional}: xscreensaver:first
Configuring /etc/pam.conf.

Do you want to copy over the master krb5.conf file ? [y/n]: n
    No action performed.

-----
Setup COMPLETE.

```

### Exemple 21–10 Exécution de l'utilitaire d'installation kclient dans la version Oracle Solaris 10

La sortie suivante indique les résultats de l'exécution de la commande `kclient`.

```

client# /usr/sbin/kclient

Starting client setup
-----

Do you want to use DNS for kerberos lookups ? [y/n]: n
    No action performed.
Enter the Kerberos realm: EXAMPLE.COM
Specify the KDC hostname for the above realm: kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Enter the krb5 administrative principal to be used: clntconfig/admin
Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>
Do you plan on doing Kerberized nfs ? [y/n]: n

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Do you want to copy over the master krb5.conf file ? [y/n]: y
Enter the pathname of the file to be copied: \
/net/denver.example.com/export/install/krb5.conf

Copied /net/denver.example.com/export/install/krb5.conf.

```

```
-----  
Setup COMPLETE !  
#
```

## ▼ Procédure de configuration d'un client Kerberos pour un serveur Active Directory

Cette procédure utilise l'utilitaire d'installation `kcclient` sans profil d'installation.

**1 Connectez-vous en tant que superutilisateur.**

**2 (Facultatif) Activez la création d'enregistrements de ressource DNS pour le client.**

```
client# sharectl set -p ddns_enable=true smb
```

**3 Exécutez l'utilitaire `kcclient`.**

L'option `-T` permet de sélectionner un type de serveur KDC. Dans ce cas, un serveur Active Directory est sélectionné.

```
client# kcclient -T ms_ad
```

Par défaut, vous devez fournir le mot de passe pour le principal d'administration.

### Exemple 21–11 Configuration d'un client Kerberos pour un serveur Active Directory à l'aide de `kcclient`

La sortie suivante indique les résultats de l'exécution de la commande `kcclient` à l'aide de l'argument de type de serveur `ms_ad` (Microsoft Active Directory). Le client sera joint au domaine Active Directory appelé `EXAMPLE.COM`.

```
client# /usr/sbin/kcclient -T ms_ad  
  
Starting client setup  
-----  
  
Attempting to join 'CLIENT' to the 'EXAMPLE.COM' domain.  
Password for Administrator@EXAMPLE.COM: <Type the password>  
Forest name found: example.com  
Looking for local KDCs, DCs and global catalog servers (SVR RRs).  
  
Setting up /etc/krb5/krb5.conf  
  
Creating the machine account in AD via LDAP.  
-----  
Setup COMPLETE.  
#
```



## ▼ Procédure de configuration manuelle d'un client Kerberos

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- Nom de domaine DNS = `example.com`
- KDC maître = `kdc1.example.com`
- KDC esclave = `kdc2.example.com`
- Serveur NFS = `denver.example.com`
- Client = `client.example.com`
- admin principal = `kws/admin`
- Utilisateur principal = `mre`
- Aide en ligne URL =  
`http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html`

---

**Remarque** – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "[URL d'aide en ligne dans l'outil d'administration graphique de Kerberos](#)" à la page 373.

---

### 1 Connectez-vous en tant que superutilisateur.

### 2 Editez le fichier de configuration Kerberos (`krb5.conf`).

Pour modifier le fichier de version Kerberos par défaut, vous devez modifier les noms de domaine et les noms de serveur. Vous devez également identifier le chemin d'accès aux fichiers d'aide pour `gkadmin`.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
```

```
kdc = FILE:/var/krb5/kdc.log

[appdefaults]
  gkadmin = {
    help_url = http://download.oracle.com/docs/cd/E23824\_01/html/821-1456/aadmin-23.html
```

---

**Remarque** – Si vous voulez limiter les types de chiffrement, vous pouvez définir les lignes `default_tkt_enctypes` ou `default_tgs_enctypes`. Pour une description des problèmes liés à la restriction des types de chiffrement, reportez-vous à la section “[Utilisation des types de chiffrement Kerberos](#)” à la page 544.

---

### 3 (Facultatif) Modifiez le processus utilisé pour localiser les KDC.

Par défaut, le domaine Kerberos pour le mappage KDC est effectué dans l'ordre suivant :

- Définition de la section `realms` dans `krb5.conf`.
- Recherche des enregistrements SRV dans le DNS.

Vous pouvez modifier ce comportement en ajoutant `dns_lookup_kdc` ou `dns_fallback` à la section `libdefaults` du fichier `krb5.conf`. Pour plus d'informations, reportez-vous à la page de manuel [krb5.conf\(4\)](#). Notez que les références sont toujours tentées en premier.

### 4 (Facultatif) Modifiez le processus utilisé pour déterminer le domaine d'un hôte.

Par défaut, le mappage de l'hôte au domaine est déterminé dans l'ordre suivant :

- Si le KDC prend en charge les références, le KDC peut indiquer au client le domaine auquel appartient l'hôte.
- Par la définition de `domain_realm` dans le fichier `krb5.conf`.
- Le nom de domaine DNS de l'hôte.
- Le domaine par défaut.

Vous pouvez modifier ce comportement en ajoutant `dns_lookup_kdc` ou `dns_fallback` à la section `libdefaults` du fichier `krb5.conf`. Pour plus d'informations, reportez-vous à la page de manuel [krb5.conf\(4\)](#). Notez que les références sont toujours tentées en premier.

### 5 (Facultatif) Synchronisez l'horloge du client avec l'horloge du KDC maître à l'aide de NTP ou d'un autre mécanisme de synchronisation d'horloge.

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être synchronisée avec l'heure sur le serveur KDC dans une différence maximum définie par la relation `clockskew` dans le fichier `krb5.conf` pour que l'opération d'authentification réussisse. Pour plus d'informations sur le protocole NTP, reportez-vous à la section “[Synchronisation des horloges entre les KDC et les clients Kerberos](#)” à la page 427.

## 6 Démarrez kadmin.

Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section [“Procédure de création d'un principal Kerberos”](#) à la page 486. Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

### a. (Facultatif) Créez un principal d'utilisateur s'il n'en existe pas déjà.

Vous devez créer un principal d'utilisateur uniquement si aucun principal n'est affecté à l'utilisateur associé à cet hôte.

```
kadmin: addprinc mre
Enter password for principal mre@EXAMPLE.COM:      <Type the password>
Re-enter password for principal mre@EXAMPLE.COM:    <Type it again>
kadmin:
```

### b. (Facultatif) Créez un principal root et ajoutez le principal au fichier keytab du serveur.

Cette étape est nécessaire pour que le client dispose d'un accès root aux systèmes de fichiers montés à l'aide du service NFS. Cette étape est également requise si l'accès root non interactif est nécessaire, par exemple pour l'exécution des tâches cron en tant que root.

Vous pouvez ignorer cette étape si le client ne nécessite pas l'accès root à un système de fichiers distant monté à l'aide du service NFS. Le principal de root doit être un principal à deux composants, avec pour second composant le nom d'hôte du système du client Kerberos, pour éviter la création d'un principal root à l'échelle du domaine. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**c. Créez un principal host et ajoutez le principal au fichier keytab du serveur.**

Le principal host est utilisé par les services d'accès à distance pour fournir l'authentification. L'identité permet à root d'acquérir des informations d'identification, s'il n'en existe pas déjà dans le fichier keytab.

```
kadmin: addprinc -randkey host/denver.example.com
Principal "host/denver.example.com@EXAMPLE.COM" created.
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**d. (Facultatif) Ajoutez le principal de service du serveur NFS au fichier keytab du serveur.**

Cette étape n'est requise que si le client a besoin d'accéder aux systèmes de fichiers NFS à l'aide de l'authentification Kerberos.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**e. Quittez kadmin.**

```
kadmin: quit
```

**7 (Facultatif) Activez Kerberos avec NFS.****a. Activez les modes de sécurité Kerberos dans le fichier /etc/nfssec.conf.**

Modifiez le fichier /etc/nfssec.conf et supprimez le "#" placé devant les modes de sécurité Kerberos.

```
# cat /etc/nfssec.conf
.
.
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5          390003  kerberos_v5    default -          # RPCSEC_GSS
krb5i         390004  kerberos_v5    default integrity  # RPCSEC_GSS
krb5p         390005  kerberos_v5    default privacy    # RPCSEC_GSS
```

**b. Activez DNS.**

Si le service `svc:/network/dns/client:default` n'est pas activé, activez-le. Pour plus d'informations, reportez-vous à la page de manuel [resolv.conf\(4\)](#).

**c. Redémarrez le service gssd.**

```
# svcadm restart network/rpc/gssd
```

- 8** Si vous souhaitez que le client renouvelle automatiquement le TGT ou qu'il avertisse les utilisateurs de l'expiration du ticket Kerberos, créez une entrée dans le fichier `/etc/krb5/warn.conf`.

Pour plus d'informations, reportez-vous à la page de manuel [warn.conf\(4\)](#).

**Exemple 21-12** Configuration d'un client Kerberos à l'aide d'un KDC non Solaris

Un client Kerberos peut être configuré pour fonctionner avec un KDC non Solaris. Dans ce cas, une ligne doit être incluse dans le fichier `/etc/krb5/krb5.conf` à la section `realms`. Cette ligne change le protocole utilisé lorsque le client est en cours de communication avec le serveur de changement de mot de passe Kerberos. Le format de cette ligne est le suivant.

```
[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
        kpasswd_protocol = SET_CHANGE
    }
```

**Exemple 21-13** Enregistrements DNS TXT pour le mappage de l'hôte et du nom de domaine au domaine Kerberos

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
    1989020501 ;serial
    10800      ;refresh
    3600       ;retry
    3600000    ;expire
    86400      ;minimum

    kdc1      IN      NS      kdc1.example.com.
    kdc1      IN      A        192.146.86.20
    kdc2      IN      A        192.146.86.21

    _kerberos.example.com.      IN      TXT      "EXAMPLE.COM"
    _kerberos.kdc1.example.com. IN      TXT      "EXAMPLE.COM"
    _kerberos.kdc2.example.com. IN      TXT      "EXAMPLE.COM"
```

**Exemple 21-14** Enregistrements DNS SRV pour les emplacements de serveur Kerberos

Cet exemple définit les enregistrements pour l'emplacement des KDC, du serveur `admin` et du serveur `kpasswd`, respectivement.

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
    1989020501 ;serial
    10800      ;refresh
    3600       ;retry
    3600000    ;expire
    86400      ;minimum

    IN NS      kdc1.example.com.
kdc1  IN A      192.146.86.20
kdc2  IN A      192.146.86.21

_kerberos._udp.EXAMPLE.COM IN SRV 0 0 88 kdc2.example.com
_kerberos._tcp.EXAMPLE.COM IN SRV 0 0 88 kdc2.example.com
_kerberos._udp.EXAMPLE.COM IN SRV 1 0 88 kdc1.example.com
_kerberos._tcp.EXAMPLE.COM IN SRV 1 0 88 kdc1.example.com
_kerberos-adm._tcp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com
```

## ▼ Procédure de désactivation de la vérification du ticket d'octroi de tickets

Cette procédure permet de désactiver le contrôle de sécurité qui vérifie que le KDC de l'hôte principal stocké dans le fichier `/etc/krb5/krb5.keytab` local est le même KDC qui a émis le ticket d'octroi de tickets. Cette vérification permet d'empêcher les attaques par usurpation de DNS. Cependant, pour certaines configurations client, l'hôte principal peut ne pas être disponible, et cette vérification doit alors être désactivée pour que le client puisse fonctionner. Voici les configurations requérant que cette vérification soit désactivée :

- L'adresse IP du client est affectée de manière dynamique. Par exemple, un client DHCP.
- Le client n'est pas configuré pour héberger les services, de sorte qu'aucun hôte principal n'a été créé.
- La clé d'hôte n'est pas stockée sur le client.

**1 Connectez-vous en tant que superutilisateur.**

**2 Modifiez le fichier `krb5.conf`.**

Si l'option `verify_ap_req_nofail` est définie sur `false`, le processus de vérification du TGT n'est pas activé. Pour plus d'informations sur cette option, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

```
client # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM
    verify_ap_req_nofail = false
...
```

---

**Remarque** – L'option `verify_ap_req_nofail` peut être saisie dans la section `[libdefaults]` ou `[realms]` du fichier `krb5.conf`. Si la valeur de l'option est dans la section `[libdefaults]`, le paramètre est utilisé pour tous les domaines. Si la valeur de l'option est dans la section `[realms]`, le paramètre s'applique uniquement au domaine défini.

---

## ▼ Procédure d'accès à un système de fichiers NFS protégé par Kerberos en tant qu'utilisateur root

Cette procédure permet à un client d'accéder à un système de fichiers NFS requérant l'authentification Kerberos avec le privilège d'ID `root`, en particulier lorsque le système de fichiers NFS est partagé avec des options comme `-o sec=krb5, root=client1.sun.com`.

### ● Démarrez `kadmin`.

Vous pouvez utiliser l'outil d'administration graphique Kerberos pour ajouter un principal, comme expliqué dans la section “[Procédure de création d'un principal Kerberos](#)” à la page 486. Pour ce faire, vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créés lorsque vous avez configuré le KDC maître. Toutefois, l'exemple ci-après montre comment ajouter les principaux requis à l'aide de la ligne de commande.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Créez un principal `root` pour le client NFS.

Ce principal permet de fournir un accès équivalent à `root` aux systèmes de fichiers montés NFS requérant l'authentification Kerberos. Le principal `root` doit être un principal à deux composants, avec pour second composant le nom d'hôte du système du client Kerberos, pour éviter la création d'un principal `root` à l'échelle du domaine. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin:
```

#### b. Ajoutez le principal `root` au fichier `keytab` du serveur.

Cette étape est nécessaire si vous avez ajouté un principal `root` afin que le client puisse avoir l'accès `root` aux systèmes de fichiers montés à l'aide du service NFS. Cette étape est également requise si l'accès `root` non interactif est nécessaire, par exemple pour l'exécution des tâches `cron` en tant que `root`.

```
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
```

```
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.  
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc  
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.  
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour  
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode  
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  
kadmin:
```

**c. Quittez kadmin.**

```
kadmin: quit
```

## ▼ Procédure de configuration de la migration automatique des utilisateurs dans un domaine Kerberos

Les utilisateurs ne disposant pas d'un principal Kerberos peuvent être automatiquement migrés vers un domaine Kerberos existant. La migration s'effectue à l'aide de la structure PAM pour le service en cours d'utilisation par l'empilage du module `pam_krb5_migrate` dans la pile d'authentification du service dans `/etc/pam.conf`.

Dans cet exemple, les noms de services PAM `gdm` et `other` sont configurés pour utiliser la migration automatique. Les paramètres de configuration suivants sont utilisés :

- Nom de domaine = `EXAMPLE.COM`
- KDC maître = `kdc1.example.com`
- Machine hébergeant le service de migration = `server1.example.com`
- Principal du service de migration = `host/server1.example.com`

**Avant de commencer**

Configurez `server1` en tant que client Kerberos du domaine `EXAMPLE.COM`. Pour plus d'informations, reportez-vous à la section [“Configuration des clients Kerberos”](#) à la page 410.

- 1 Connectez-vous en tant que superutilisateur.**
- 2 Vérifiez si un hôte principal de service existe pour `server1`.**

L'hôte principal de service dans le fichier `keytab` de `server1` est utilisé pour authentifier le serveur auprès du KDC maître.

```
server1 # klist -k  
Keytab name: FILE:/etc/krb5/krb5.keytab  
KVNO Principal  
-----  
3 host/server1.example.com@EXAMPLE.COM  
3 host/server1.example.com@EXAMPLE.COM  
3 host/server1.example.com@EXAMPLE.COM  
3 host/server1.example.com@EXAMPLE.COM
```



### 3 Apportez des modifications au fichier de configuration PAM.

#### a. Ajoutez des entrées pour le service gdm.

```
# cat /etc/pam.conf
.
.
#
# gdm service
#
gdm      auth requisite      pam_authtok_get.so.1
gdm      auth required       pam_dhkeys.so.1
gdm      auth required       pam_unix_cred.so.1
gdm      auth sufficient     pam_krb5.so.1
gdm      auth requisite      pam_unix_auth.so.1
gdm      auth optional       pam_krb5_migrate.so.1
```

#### b. (Facultatif) Forcez une modification immédiate du mot de passe, si nécessaire.

Il est possible de définir le délai d'expiration du mot de passe des nouveaux comptes Kerberos sur l'heure actuelle (maintenant), afin de forcer la modification immédiate du mot de passe Kerberos. Pour définir l'heure d'expiration sur l'heure actuelle, ajoutez l'option `expire_pw` aux lignes utilisant le module `pam_krb5_migrate`. Pour plus d'informations, reportez-vous à la page de manuel [pam\\_krb5\\_migrate\(5\)](#).

```
# cat /etc/pam.conf
.
.
#
gdm      auth optional       pam_krb5_migrate.so.1 expire_pw
```

#### c. Ajoutez le module `pam_krb5` à la pile de compte.

Cet ajout prévoit l'expiration du mot de passe de Kerberos afin de bloquer l'accès.

```
# cat /etc/pam.conf
.
.
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other    account requisite    pam_roles.so.1
other    account required     pam_krb5.so.1
other    account required     pam_unix_account.so.1
```

#### d. Ajoutez le module `pam_krb5` à la pile de mot de passe.

Cet ajout permet la mise à jour des mots de passe lorsque ceux-ci expirent.

```
# cat /etc/pam.conf
.
.
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password management
#
other    password required     pam_dhkeys.so.1
other    password requisite     pam_authtok_get.so.1
```

|       |                     |                        |
|-------|---------------------|------------------------|
| other | password requisite  | pam_authtok_check.so.1 |
| other | password sufficient | pam_krb5.so.1          |
| other | password required   | pam_authtok_store.so.1 |

#### 4 Sur le KDC maître, mettez à jour le fichier de contrôle d'accès.

Les entrées suivantes accordent des privilèges de migration et de consultation au principal de service `host/server1.example.com` pour tous les utilisateurs, excepté l'utilisateur `root`. Il est important que les utilisateurs qui ne doivent pas être migrés soient répertoriés dans le fichier `kadm5.acl` à l'aide du privilège `U`. Ces entrées doivent figurer avant l'entrée `"permit all"` ou `ui`. Pour plus d'informations, reportez-vous à la page de manuel [kadm5.acl\(4\)](#).

```
kdc1 # cat /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

#### 5 Sur le KDC maître, redémarrez le démon d'administration Kerberos.

Cette étape permet au démon `kadmind` d'utiliser les nouvelles entrées `kadm5.acl`.

```
kdc1 # svcadm restart network/security/kadmin
```

#### 6 Sur le KDC maître, ajoutez les entrées au fichier `pam.conf`.

Les entrées suivantes permettent au démon `kadmind` d'utiliser le service PAM `k5migrate` pour valider le mot de passe utilisateur UNIX pour les comptes qui nécessitent une migration.

```
# grep k5migrate /etc/pam.conf
k5migrate      auth      required      pam_unix_auth.so.1
k5migrate      account   required      pam_unix_account.so.1
```

## ▼ Procédure de configuration du verrouillage de compte

### ● Démarrez `kadmin`.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

#### a. Créez une stratégie avec des paramètres de verrouillage de compte.

Dans l'exemple suivant, la sous-commande `add_policy` est utilisée pour créer une stratégie nommée `default`. Trois échecs d'authentification en l'espace de 300 secondes déclenchera un verrouillage de compte de 900 secondes.

```
kadmin: add_policy -maxfailure 3 -failurecountinterval "300 seconds" \
-lockoutduration "900 seconds" default
```

#### b. Quittez `kadmin`.

```
kadmin: quit
```

**Exemple 21–15** Déverrouillage d'un principal verrouillé

Dans l'exemple suivant, un principal d'utilisateur est déverrouillé :

```
# kadmin  
kadmin: add_policy -unlock principal
```

## Synchronisation des horloges entre les KDC et les clients Kerberos

Tous les hôtes participant au système d'authentification Kerberos doivent avoir leurs horloges internes synchronisées dans une quantité maximale de temps spécifiée (appelée *écart d'horloge*). Cette exigence constitue un autre contrôle de sécurité Kerberos. Si l'écart d'horloge est dépassé entre des hôtes participants, les demandes du client sont rejetées.

L'écart d'horloge détermine également la durée pendant laquelle les serveurs d'application doivent assurer le suivi de tous les messages du protocole Kerberos, afin de reconnaître et de rejeter les demandes rediffusées. Ainsi, plus l'écart d'horloge est élevé, plus les serveurs d'application doivent collecter d'informations.

La valeur par défaut pour l'écart d'horloge maximal est de 300 secondes (5 minutes). Vous pouvez modifier cette valeur par défaut dans la section `libdefaults` du fichier `krb5.conf`.

---

**Remarque** – Pour des raisons de sécurité, l'écart d'horloge ne doit pas dépasser 300 secondes.

---

Dans la mesure où il est important de conserver la synchronisation des horloges entre le KDC et les clients Kerberos, vous devez utiliser le logiciel NTP (Network Time Protocol) pour les synchroniser. Le logiciel NTP du domaine public de l'Université du Delaware est inclus dans le logiciel Oracle Solaris.

---

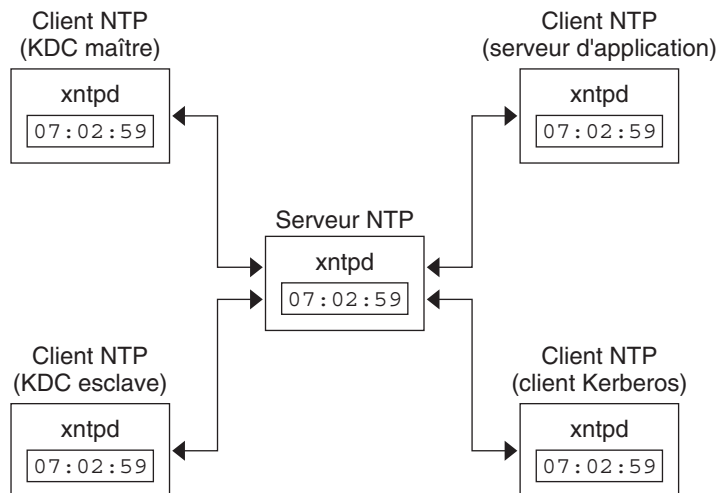
**Remarque** – Un autre moyen de synchroniser les horloges consiste à utiliser la commande `rdate` et les tâches `cron` ; ce processus peut être moins complexe que l'utilisation du protocole NTP. Toutefois, cette section se concentre sur l'utilisation du protocole NTP. En outre, si vous utilisez le réseau pour synchroniser les horloges, le protocole de synchronisation de l'horloge doit lui-même être sécurisé.

---

NTP vous permet de gérer avec précision la synchronisation de l'heure ou de l'horloge du réseau, ou les deux, dans un environnement réseau. NTP est fondamentalement une implémentation serveur-client. Sélectionnez le système qui sera l'horloge principale (serveur NTP). Ensuite, définissez tous les autres systèmes (clients NTP) de sorte qu'ils synchronisent leurs horloges avec l'horloge principale.

Pour synchroniser les horloges, NTP utilise le démon `xntpd` qui définit et actualise l'heure du jour d'un système UNIX en accord avec les serveurs de temps standard Internet. L'exemple suivant montre un exemple de cette implémentation serveur-client NTP.

FIGURE 21-1 Synchronisation des horloges à l'aide de NTP



S'assurer que les KDC et les clients Kerberos maintiennent leurs horloges synchronisées implique la mise en oeuvre des étapes suivantes :

1. Configuration d'un serveur NTP sur votre réseau. Ce serveur peut être n'importe quel système, à l'exception du KDC maître. Reportez-vous à la section [“Gestion du protocole NTP \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : Services réseau* pour connaître les tâches de serveur NTP.
2. Lorsque vous configurez les clients KDC et Kerberos sur le réseau, définissez-les de sorte qu'ils soient des clients NTP sur le serveur NTP. Reportez-vous à la section [“Gestion du protocole NTP \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : Services réseau* pour connaître les tâches de client NTP.

## Echange d'un KDC maître et d'un KDC esclave

Vous devez utiliser les procédures décrites dans cette section pour faciliter l'échange d'un KDC maître et d'un KDC esclave. Vous devez remplacer le KDC maître par un KDC esclave uniquement si le serveur du KDC maître est en panne pour une raison quelconque, ou si le KDC maître doit être réinstallé (par exemple, en cas d'installation de nouveau matériel).

## ▼ Procédure de configuration d'un KDC échangeable

Effectuez cette procédure sur le serveur KDC esclave que vous souhaitez libérer pour devenir le KDC maître. Cette procédure suppose que vous utilisez la propagation incrémentielle.

### 1 Utilisez les noms d'alias pour le KDC maître et le KDC esclave échangeable pendant l'installation du KDC.

Lorsque vous définissez les noms d'hôte des KDC, assurez-vous que chaque système possède un alias inclus dans le DNS. Vous pouvez également utiliser les noms d'alias lorsque vous définissez les hôtes dans le fichier `/etc/krb5/krb5.conf`.

### 2 Effectuez les étapes suivantes pour installer un KDC esclave.

Avant tout échange, ce serveur doit fonctionner comme n'importe quel autre KDC esclave dans le domaine. Reportez-vous à la section [“Procédure de configuration manuelle d'un KDC esclave” à la page 393](#) pour obtenir des instructions.

### 3 Déplacez les commandes de KDC maître.

Pour empêcher les commandes du KDC maître d'être exécutées à partir de ce KDC esclave, déplacez les commandes `kprop`, `kadmind` et `kadmin.local` à un endroit réservé.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc4 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
```

## ▼ Procédure d'échange d'un KDC maître et d'un KDC esclave

Dans cette procédure, le serveur de KDC maître échangé est appelé `kdc1`. Le KDC esclave qui devient le nouveau KDC maître est appelé `kdc4`. Cette procédure suppose que vous utilisez la propagation incrémentielle.

### Avant de commencer

Cette procédure nécessite que le serveur de KDC esclave ait été défini en tant qu'esclave échangeable. Pour plus d'informations, reportez-vous à la section [“Procédure de configuration d'un KDC échangeable” à la page 429](#).

### 1 Connectez-vous en tant que superutilisateur.

**2 Sur le nouveau KDC maître, démarrez kadmin.**

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Créez de nouveaux principaux pour le service kadmind.**

L'exemple suivant montre la première commande `addprinc` sur deux lignes, mais elle doit être saisie sur une seule ligne.

```
kadmin: addprinc -randkey -allow_tgs_req +password_changing_service -clearpolicy \
changepw/kdc4.example.com
Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. Quittez kadmin.**

```
kadmin: quit
```

**3 Sur le nouveau KDC maître, forcez la synchronisation.**

Les étapes suivantes forcent une mise à jour complète de KDC sur le serveur esclave.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**4 Sur le nouveau KDC maître, vérifiez que la mise à jour est terminée.**

```
kdc4 # /usr/sbin/kproplog -h
```

**5 Sur le nouveau KDC maître, redémarrez le service KDC.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

**6 Sur le nouveau KDC maître, effacez le journal de mise à jour.**

Ces étapes réinitialisent le journal de mise à jour pour le nouveau serveur KDC maître.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**7 Sur l'ancien KDC maître, arrêtez les processus kadmind et krb5kdc.**

Lorsque vous interrompez le processus `kadmind`, vous empêchez toute modification apportée à la base de données KDC.

```
kdc1 # svcadm disable network/security/kadmin
kdc1 # svcadm disable network/security/krb5kdc
```

**8 Sur l'ancien KDC maître, spécifiez la durée d'interrogation pour demander les propagations.**

Mettez en commentaire l'entrée `sunw_dbprop_master_ologsize` du fichier `/etc/krb5/kdc.conf` et ajoutez une entrée définissant `sunw_dbprop_slave_poll`. L'entrée définit la durée d'interrogation sur deux minutes.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
```

```

kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
        sunw_dbprop_slave_poll = 2m
    }

```

### 9 Sur l'ancien KDC maître, déplacez les commandes de KDC maître et le fichier `kadm5.acl`.

Pour empêcher l'exécution des commandes de KDC maître, déplacez les commandes `kprop`, `kadmind` et `kadmin.local` à une place réservée.

```

kdc1 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc1 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc1 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
kdc1 # mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save

```

### 10 Sur le serveur DNS, modifiez les noms d'alias du KDC maître.

Pour changer de serveurs, modifiez le fichier de zone `example.com` et modifiez l'entrée pour `masterkdc`.

```
masterkdc IN CNAME kdc4
```

### 11 Sur le serveur DNS, redémarrez le serveur de nom de domaine Internet.

Exécutez la commande suivante pour recharger les nouvelles informations d'alias :

```
# svcadm refresh network/dns/server
```

### 12 Sur le nouveau KDC maître, déplacez les commandes de KDC maître et le fichier esclave `kpropd.acl`.

```

kdc4 # mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop
kdc4 # mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind
kdc4 # mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local
kdc4 # mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save

```

### 13 Sur le nouveau KDC maître, créez le fichier d'ACL Kerberos (`kadm5.acl`).

Une fois renseigné, le fichier `/etc/krb5/kadm5.acl` doit contenir tous les noms de principaux autorisés à administrer le KDC. Ce fichier doit également répertorier tous les esclaves qui émettent des requêtes de propagation incrémentielle. Pour plus d'informations, reportez-vous à la page de manuel [kadm5.acl\(4\)](#).

```

kdc4 # cat /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM *
kiprop/kdc1.example.com@EXAMPLE.COM p

```

**14 Sur le nouveau KDC maître, spécifiez la taille de journal de mise à jour dans le fichier `kdc.conf`.**

Mettez en commentaire l'entrée `sunw_dbprop_slave_poll` et ajoutez une entrée définissant `sunw_dbprop_master_ulogsize`. L'entrée définit la taille du journal à 1000 entrées.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
#        sunw_dbprop_slave_poll = 2m
        sunw_dbprop_master_ulogsize = 1000
    }
```

**15 Sur le nouveau KDC maître, démarrez `kadmind` et `krb5kdc`.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmind
```

**16 Sur l'ancien KDC maître, ajoutez le principal de service `kiprop`.**

L'ajout du principal `kiprop` au fichier `krb5.keytab` permet au démon `kpropd` de s'authentifier auprès du service de propagation incrémentielle.

```
kdc1 # /usr/sbin/kadmind -p kws/admin
Authenticating as principal kws/admin@EXAMPLE.COM with password.
Enter password: <Type kws/admin password>
kadmind: ktadd kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmind: quit
```

**17 Sur l'ancien KDC maître, ajoutez une entrée pour chaque KDC répertorié dans `krb5.conf` au fichier de configuration de propagation, `kpropd.acl`.**

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
host/kdc4.example.com@EXAMPLE.COM
```



**18 Sur l'ancien KDC maître, démarrez kpropd et krb5kdc.**

```
kdc1 # svcadm enable -r network/security/krb5_prop
kdc1 # svcadm enable -r network/security/krb5kdc
```

## Administration de la base de données Kerberos

La base de données Kerberos est l'épine dorsale de Kerberos et sa maintenance doit s'effectuer correctement. Cette section présente certaines procédures d'administration de la base de données Kerberos, telles que la sauvegarde et la restauration de la base de données, la définition de la propagation incrémentielle ou parallèle, ainsi que l'administration du fichier stash. Les étapes de configuration initiale de la base de données sont détaillées dans la section [“Procédure de configuration manuelle d'un KDC maître” à la page 380](#).

### Sauvegarde et propagation de la base de données Kerberos

La propagation de la base de données Kerberos du KDC maître aux KDC esclaves est l'une des tâches de configuration les plus importantes. Si la propagation n'est pas suffisamment fréquente, la synchronisation entre le KDC maître et les KDC esclaves est perdue. Par conséquent, en cas de défaillance du KDC maître, les KDC esclaves n'auront pas les informations de base de données les plus récentes. En outre, si un KDC esclave a été configuré en tant que KDC maître à des fins d'équilibrage de charge, les clients qui utilisent le KDC esclave en tant que KDC maître ne disposeront pas des dernières informations. Par conséquent, vous devez vous assurer que la propagation est suffisamment fréquente ou configurer les serveurs pour une propagation incrémentielle, en fonction de la fréquence à laquelle vous modifiez la base de données Kerberos. La propagation incrémentielle est préférable à une propagation manuelle parce qu'elle élimine les frais d'administration liés à la propagation manuelle de la base de données. En outre, une propagation complète de la base de données n'est pas totalement efficace.

Lorsque vous configurez le KDC maître, vous configurez la commande `kprop_script` dans une tâche `cron` pour sauvegarder automatiquement la base de données Kerberos dans le fichier `dump /var/krb5/slave_data.tans` et la propager vers les KDC esclaves. Mais, comme avec n'importe quel fichier, la base de données Kerberos peut être corrompue. Si la corruption de données se produit sur un KDC esclave, il se peut que vous ne le remarquiez pas, dans la mesure où la propagation automatique suivante de la base de données permet d'installer une nouvelle copie. Toutefois, si la corruption se produit sur le KDC maître, la base de données corrompue est propagée à l'ensemble des KDC esclaves pendant la propagation suivante. Et, la sauvegarde corrompue écrase le fichier de sauvegarde non altéré précédent sur le KDC maître.

Parce qu'il n'y a pas de copie de sauvegarde "sûre" dans ce scénario, vous devez également définir une tâche `cron` pour copier, à intervalles réguliers, le fichier `dump slave_data.tans`

dans un autre emplacement ou pour créer une autre copie de sauvegarde à l'aide de la commande `dump de kdb5_util`. Puis, si votre base de données est endommagée, vous pouvez restaurer la sauvegarde la plus récente sur le KDC maître en utilisant la commande `load de kdb5_util`.

Autre remarque importante : puisque le fichier dump de la base de données contient les clés de principal, vous devez protéger le fichier de tout accès par des utilisateurs non autorisés. Par défaut, la base de données du fichier de vidage dispose d'autorisations de lecture et d'écriture uniquement en tant que `root`. Afin de les protéger contre tout accès non autorisé, utilisez uniquement la commande `kprop` pour propager la base de données du fichier de vidage, qui chiffre les données en cours de transfert. En outre, `kprop` propage les données uniquement aux KDC esclaves, ce qui réduit les risques d'envoi par inadvertance du fichier dump de la base de données à des hôtes non autorisés.



---

**Attention** – Si la base de données Kerberos est mise à jour après sa propagation et que la base de données est ensuite corrompue avant la propagation suivante, les KDC esclaves ne contiennent pas les mises à jour. Les mises à jour seront perdues. Pour cette raison, si vous ajoutez des mises à jour importantes de la base de données Kerberos avant une propagation programmée, vous devez propager manuellement la base de données afin d'éviter toute perte de données.

---

## Fichier `kpropd.acl`

Le fichier `kpropd.acl` sur un KDC esclave fournit une liste de noms d'hôte principal, un nom par ligne, qui spécifie les systèmes à partir desquels le KDC peut recevoir une base de données mise à jour par la propagation. Si le KDC maître est utilisé pour propager tous les KDC esclaves, le fichier `kpropd.acl` sur chaque esclave doit contenir uniquement le nom d'hôte principal du KDC maître.

Toutefois, l'installation de Kerberos et les étapes de configuration dans ce manuel vous indiquent que vous devez ajouter le même fichier `kpropd.acl` sur le KDC maître et les KDC esclaves. Ce fichier contient tous les noms de principaux d'hôtes KDC. Cette configuration vous permet de propager à partir de n'importe quel KDC, dans le cas où la propagation des KDC serait temporairement indisponible. De plus, en conservant une copie identique sur tous les KDC, la configuration est plus facile à gérer.

## Commande `kprop_script`

La commande `kprop_script` utilise la commande `kprop` pour propager la base de données Kerberos à d'autres KDC. Si la commande `kprop_script` est exécutée sur un KDC esclave, elle se propage à la copie de la base de données Kerberos du KDC esclave vers d'autres KDC. La commande `kprop_script` accepte une liste de noms d'hôte pour les arguments, séparés par des espaces, qui indiquent les KDC à propager.

Quand `kprop_script` est exécutée, elle crée une copie de sauvegarde de la base de données Kerberos pour le fichier `/var/krb5/slave_data/tran` et copie le fichier dans les KDC spécifiés. La base de données Kerberos est verrouillée jusqu'à ce que la propagation soit terminée.

## ▼ Procédure de sauvegarde de la base de données Kerberos

- 1 Connectez-vous en tant qu'administrateur ou endossez un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

- 2 Sauvegardez la base de données Kerberos à l'aide de la commande `dump` de la commande `kdb5_util`.

```
# /usr/sbin/kdb5_util dump [-verbose] [-d dbname] [filename [principals...]]
```

`-verbose` Imprime le nom de chaque principal et stratégie en cours de sauvegarde.

`dbname` Définit le nom de la base de données à sauvegarder. Notez que vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si l'option `-d` n'est pas spécifiée, le nom de la base de données par défaut est `/var/krb5/principal`.

`filename` Définit le fichier utilisé pour sauvegarder la base de données. Vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si vous ne spécifiez pas un fichier, la base de données est transférée vers la sortie standard.

`principals` Définit une liste d'un ou plusieurs principaux (séparés par un espace) à sauvegarder. Vous devez utiliser des noms de principaux entièrement qualifiés. Si vous ne spécifiez aucun principal, l'intégralité de la base de données est sauvegardée.

### Exemple 21–16 Sauvegarde de la base de données Kerberos

Dans l'exemple suivant, la base de données Kerberos est sauvegardée dans un fichier appelé `dumpfile`. Dans la mesure où l'option `-verbose` est spécifiée, chaque principal est imprimé lorsqu'il est sauvegardé.

```
# kdb5_util dump -verbose dumpfile
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/ENG.EXAMPLE.COM@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

Dans l'exemple suivant, les principaux `pak` et `pak/admin` de la base de données Kerberos sont sauvegardés.

```
# kdb5_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
```

## ▼ Procédure de restauration de la base de données Kerberos

- 1 Connectez-vous en tant que superutilisateur au KDC maître.

- 2 Sur le serveur maître, arrêtez les démons KDC.

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

- 3 Restaurez la base de données Kerberos à l'aide de la commande `load` de la commande `kdb_util`.

```
# /usr/sbin/kdb5_util load [-verbose] [-d dbname] [-update] [filename]
```

`-verbose` Imprime le nom de chaque principal et stratégie en cours de restauration.

`dbname` Définit le nom de la base de données à restaurer. Notez que vous pouvez spécifier un chemin d'accès absolu pour le fichier. Si l'option `-d` n'est pas spécifiée, le nom de la base de données par défaut est `/var/krb5/principal`.

`-update` Met à jour la base de données existante. Dans le cas contraire, une nouvelle base de données est créée ou la base de données existante est écrasée.

`filename` Définit le fichier à partir duquel restaurer la base de données. Vous pouvez spécifier un chemin d'accès absolu pour le fichier.

- 4 Démarrez les démons KDC.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

### Exemple 21-17 Restauration de la base de données Kerberos

Dans l'exemple suivant, la base de données appelée `database1` est restaurée dans le répertoire courant à partir du fichier `dumpfile`. Comme l'option `-update` n'est pas spécifiée, la restauration crée une nouvelle base de données.

```
# kdb5_util load -d database1 dumpfile
```

## ▼ Procédure de conversion d'une base de données Kerberos après une mise à niveau du serveur

Si votre base de données KDC a été créée sur un serveur exécutant la version Solaris 8 ou Solaris 9, la conversion de la base de données vous permet de tirer parti du format de base de données amélioré.

**Avant de commencer**

Assurez-vous que la base de données utilise un format ancien.

**1 Sur le serveur maître, arrêtez les démons KDC.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

**2 Créez un répertoire pour stocker une copie temporaire de la base de données.**

```
kdc1 # mkdir /var/krb5/tmp
kdc1 # chmod 700 /var/krb5/tmp
```

**3 Videz la base de données KDC.**

```
kdc1 # kdb5_util dump /var/krb5/tmp/prdb.txt
```

**4 Enregistrez des copies des fichiers de la base de données actuelle.**

```
kdc1 # cd /var/krb5
kdc1 # mv princ* tmp/
```

**5 Chargez la base de données.**

```
kdc1 # kdb5_util load /var/krb5/tmp/prdb.txt
```

**6 Démarrez les démons KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

## ▼ Procédure de reconfiguration d'un KDC maître pour l'utilisation de la propagation incrémentielle

Les étapes de cette procédure peuvent être utilisées pour reconfigurer un KDC maître pour qu'il utilise la propagation incrémentielle. Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Nom de domaine = EXAMPLE.COM
- Nom de domaine DNS = example.com
- KDC maître = kdc1.example.com
- KDC esclave = kdc2.example.com
- admin principal = kws/admin

**1 Connectez-vous en tant que superutilisateur.**

## 2 Ajoutez des entrées à `kdc.conf`.

Vous devez activer la propagation incrémentielle et sélectionner le nombre de mises à jour que le KDC maître conserve dans le journal. Pour plus d'informations, reportez-vous à la page de manuel [kdc.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ologsize = 1000
    }
```

## 3 Créez le principal `kiprop`.

Le principal `kiprop` est utilisé pour authentifier le serveur KDC maître et autoriser les mises à jour depuis le KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

## 4 Sur le KDC maître, ajoutez une entrée `kiprop` au fichier `kadm5.acl`.

Cette entrée permet au KDC maître de recevoir des demandes de propagation incrémentielle du serveur `kdc2`.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

## 5 Mettez en commentaire la ligne `kprop` dans le fichier `crontab root`.

Cette étape permet d'éviter que le KDC maître ne propage sa copie de la base de données KDC.

```
kdc1 # crontab -e
#ident "@(#)root 1.20 01/11/06 SMI"
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * * /usr/sbin/logadm
```

```
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
#10 3 * * * /usr/lib/krb5kprop_script kdc2.example.sun.com #SUNWkr5ma
```

## 6 Redémarrez kadmind.

```
kdc1 # svcadm restart network/security/kadmin
```

## 7 Reconfigurez tous les serveurs KDC esclaves qui utilisent la propagation incrémentielle.

Reportez-vous à la section “[Procédure de reconfiguration d'un KDC esclave pour l'utilisation de la propagation incrémentielle](#)” à la page 439 pour obtenir des instructions complètes.

# ▼ Procédure de reconfiguration d'un KDC esclave pour l'utilisation de la propagation incrémentielle

## 1 Connectez-vous en tant que superutilisateur.

## 2 Ajoutez des entrées à kdc.conf.

La première nouvelle entrée permet active la propagation incrémentielle. La deuxième nouvelle entrée définit la durée d'interrogation sur deux minutes.

```
kdc2 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_slave_poll = 2m
    }
```

## 3 Ajoutez le principal kprop au fichier krb5.keytab.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: ktadd kprop/kdc2.example.com
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

```
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

#### 4 Redémarrez kpropd.

```
kdc2 # svcadm restart network/security/krb5_prop
```

## ▼ Procédure de configuration d'un KDC esclave pour l'utilisation de la propagation complète

Cette procédure montre comment reconfigurer un serveur KDC esclave exécutant la version Solaris 10 pour qu'il utilise la propagation complète. Normalement, la procédure est utilisée uniquement si le serveur KDC maître exécute la version Solaris 9 ou une version antérieure. Dans ce cas, le serveur KDC maître ne prend pas en charge la propagation incrémentielle, de sorte que le serveur esclave doit être configuré pour que la propagation fonctionne.

Dans cette procédure, un KDC esclave nommé kdc3 est configuré. Cette procédure utilise les paramètres de configuration ci-dessous :

- Nom de domaine = EXAMPLE.COM
- Nom de domaine DNS = example.com
- KDC maître = kdc1.example.com
- KDC esclave = kdc2.example.com et kdc3.example.com
- admin principal = kws/admin
- Aide en ligne URL =  
[http://download.oracle.com/docs/cd/E23824\\_01/html/821-1456/aadmin-23.html](http://download.oracle.com/docs/cd/E23824_01/html/821-1456/aadmin-23.html)

---

**Remarque** – Réglez l'URL pour qu'elle pointe vers la section "Outil d'administration graphique Kerberos", comme décrit dans la section "[URL d'aide en ligne dans l'outil d'administration graphique de Kerberos](#)" à la page 373.

---

#### Avant de commencer

Le KDC maître doit être configuré. Pour obtenir des instructions spécifiques afin de déterminer si cet esclave doit être échangeable, reportez-vous à la section "[Echange d'un KDC maître et d'un KDC esclave](#)" à la page 428.

#### 1 Sur le KDC maître, connectez-vous en tant que superutilisateur.



**2 Sur le KDC maître, démarrez kadmin.**

Vous devez vous connecter à l'aide de l'un des noms de principal admin que vous avez créé lors de la configuration du KDC maître.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Sur le KDC maître, ajoutez des principaux d'hôtes esclaves à la base de données, si ce n'est pas déjà fait.**

Pour que l'esclave fonctionne, il doit avoir un hôte principal. Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: addprinc -randkey host/kdc3.example.com
Principal "host/kdc3@EXAMPLE.COM" created.
kadmin:
```

**b. Quittez kadmin.**

```
kadmin: quit
```

**3 Sur le KDC maître, modifiez le fichier de configuration Kerberos (krb5.conf).**

Vous devez ajouter une entrée pour chaque esclave. Pour une description complète de ce fichier, reportez-vous à la page de manuel [krb5.conf\(4\)](#).

```
kdc1 # cat /etc/krb5/krb5.conf
.
.
[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        kdc = kdc3.example.com
        admin_server = kdc1.example.com
    }
```

**4 Sur le KDC maître, ajoutez une entrée pour le KDC maître et chaque KDC esclave dans le fichier kpropd.acl.**

Reportez-vous à la page de manuel [kprop\(1M\)](#) pour obtenir une description complète de ce fichier.

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
```

**5 Sur tous les KDC esclaves, copiez les fichiers d'administration à partir du serveur KDC maître.**

Cette étape doit être effectuée sur tous les KDC esclaves, car le serveur KDC maître a mis à jour des informations requises par chaque serveur KDC. Vous pouvez utiliser ftp ou tout autre mécanisme de transfert similaire pour extraire des copies des fichiers suivants du KDC maître :

- /etc/krb5/krb5.conf
- /etc/krb5/kdc.conf
- /etc/krb5/kpropd.acl

**6 Sur tous les KDC esclaves, assurez-vous que le fichier d'ACL Kerberos, `kadm5.acl`, n'est pas renseigné.**

Un fichier `kadm5.acl` non modifié ressemble à ce qui suit :

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Si le fichier contient des entrées `kprop`, supprimez-les.

**7 Sur le nouvel esclave, démarrez la commande `kadmin`.**

Vous devez vous connecter à l'aide de l'un des noms de principal `admin` que vous avez créé lors de la configuration du KDC maître.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

**a. Ajoutez le principal host de l'esclave au fichier keytab de ce dernier en utilisant `kadmin`.**

Cette entrée permet à `kprop` et à d'autres applications utilisant Kerberos de fonctionner.

Notez que lorsque l'instance de principal est un nom d'hôte, le nom de domaine complet (FQDN) doit être spécifié en minuscules, quelle que soit la casse du nom de domaine dans le service de noms.

```
kadmin: ktadd host/kdc3.example.com
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**b. Quittez `kadmin`.**

```
kadmin: quit
```

- 8 Sur le KDC maître, ajoutez le nom du KDC esclave à la tâche cron, qui exécute automatiquement les sauvegardes, en exécutant `crontab -e`.**

Ajoutez le nom de chaque serveur KDC esclave à la fin de la ligne `kprop_script`.

```
10 3 * * * /usr/lib/krb5/kprop_script kdc2.example.com kdc3.example.com
```

Vous pouvez aussi modifier l'heure des sauvegardes. Cette entrée démarre le processus de sauvegarde tous les jours à 3h10.

- 9 Sur le nouvel esclave, démarrez le démon de propagation Kerberos.**

```
kdc3 # svcadm enable network/security/krb5_prop
```

- 10 Sur le KDC maître, sauvegardez et propagez la base de données à l'aide de `kprop_script`.**

Si une copie de sauvegarde de la base de données est déjà disponible, il n'est pas nécessaire d'effectuer une autre sauvegarde. Reportez-vous à la section [“Procédure de propagation manuelle de la base de données Kerberos aux KDC esclaves”](#) à la page 445 pour obtenir des instructions.

```
kdc1 # /usr/lib/krb5/kprop_script kdc3.example.com
Database propagation to kdc3.example.com: SUCCEEDED
```

- 11 Sur le nouvel esclave, créez un fichier stash à l'aide de `kdb5_util`.**

```
kdc3 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key:      <Type the key>
```

- 12 (Facultatif) Sur le nouveau KDC esclave, synchronisez l'horloge du KDC maître à l'aide du protocole NTP ou d'un autre mécanisme de synchronisation de l'horloge.**

L'installation et l'utilisation du protocole NTP (Network Time Protocol) ne sont pas requises. Cependant, chaque horloge doit être réglée sur l'heure par défaut définie dans la section `libdefaults` du fichier `krb5.conf` pour que l'authentification s'exécute correctement. Pour plus d'informations sur le protocole NTP, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

- 13 Sur le nouvel esclave, démarrez le démon KDC (`krb5kdc`).**

```
kdc3 # svcadm enable network/security/krb5kdc
```

## ▼ Procédure de vérification de la synchronisation des serveurs KDC

Si la propagation incrémentielle a été configurée, cette procédure permet de s'assurer que les informations sur le KDC esclave ont été mises à jour.

- 1 **Connectez-vous en tant que superutilisateur.**
- 2 **Sur le serveur KDC maître, exécutez la commande kproplog.**  
`kdc1 # /usr/sbin/kproplog -h`
- 3 **Sur un serveur KDC esclave, exécutez la commande kproplog.**  
`kdc2 # /usr/sbin/kproplog -h`
- 4 **Vérifiez que les valeurs du dernier numéro de série et du dernier horodatage correspondent.**

### Exemple 21–18 Vérification de la synchronisation des serveurs KDC

L'exemple suivant est un exemple des résultats de l'exécution de la commande kproplog sur le serveur KDC maître.

```
kdc1 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
  Log version #: 1
  Log state: Stable
  Entry block size: 2048
  Number of entries: 2500
  First serial #: 137966
  Last serial #: 140465
  First time stamp: Fri Nov 28 00:59:27 2004
  Last time stamp: Fri Nov 28 01:06:13 2004
```

L'exemple suivant est un exemple des résultats de l'exécution de la commande kproplog sur le serveur KDC esclave.

```
kdc2 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
  Log version #: 1
  Log state: Stable
  Entry block size: 2048
  Number of entries: 0
  First serial #: None
  Last serial #: 140465
  First time stamp: None
  Last time stamp: Fri Nov 28 01:06:13 2004
```

Notez que les valeurs pour le dernier numéro de série et le dernier horodatage sont identiques, ce qui indique que l'esclave est synchronisé avec le serveur KDC maître.

Dans la sortie du serveur KDC esclave, notez qu'aucune entrée de mise à jour n'existe dans le journal de mise à jour du serveur KDC esclave. Il n'y a pas d'entrées dans la mesure où le serveur KDC esclave ne conserve pas de jeu de mises à jour, à l'inverse du serveur KDC maître. En

outre, le serveur KDC esclave n'inclut pas d'informations sur le premier numéro de série ou le premier horodatage car il ne s'agit pas d'informations pertinentes.

## ▼ Procédure de propagation manuelle de la base de données Kerberos aux KDC esclaves

Cette procédure vous indique comment propager la base de données Kerberos à l'aide de la commande `kprop`. Utilisez cette procédure si vous avez besoin de synchroniser un KDC esclave avec le KDC maître à l'extérieur de la tâche périodique `cron`. A la différence de `kprop_script`, vous pouvez utiliser `kprop` pour propager uniquement la sauvegarde actuelle de la base de données sans nouvelle sauvegarde préalable de la base de données Kerberos.

---

**Remarque** – N'utilisez pas cette procédure si vous utilisez la propagation incrémentielle.

---

- 1 **Connectez-vous en tant qu'administrateur ou endosse un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).**

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

- 2 **Connectez-vous en tant que superutilisateur au KDC maître.**
- 3 **(Facultatif) Sauvegardez la base de données à l'aide de la commande `kdb5_util`.**

```
# /usr/sbin/kdb5_util dump /var/krb5/slave_datatrans
```

- 4 **Propagez la base de données à un KDC esclave en utilisant la commande `kprop`.**

```
# /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC
```

### Exemple 21–19 Propagation manuelle de la base de données Kerberos au KDC esclave à l'aide de `kprop_script`

Si vous souhaitez sauvegarder la base de données et la propager à un KDC esclave à l'extérieur de la tâche périodique `cron`, vous pouvez également utiliser la commande `kprop_script` comme suit :

```
# /usr/lib/krb5/kprop_script slave-KDC
```

## Configuration d'une propagation parallèle

Dans la plupart des cas, le KDC maître est utilisé exclusivement pour propager sa base de données Kerberos aux KDC esclaves. Cependant, si votre site comporte beaucoup de KDC esclaves, vous pouvez envisager le partage de la charge du processus de propagation, aussi appelé *propagation parallèle*.

---

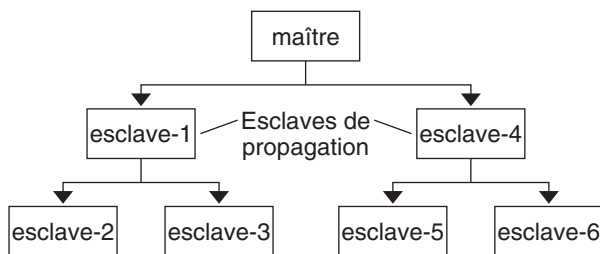
**Remarque** – N'utilisez pas cette procédure si vous utilisez la propagation incrémentielle.

---

La propagation parallèle autorise des KDC esclaves spécifiques à partager les fonctions de propagation avec le KDC maître. Ce partage permet à la propagation de s'effectuer plus rapidement et d'alléger la charge du KDC maître.

Par exemple, supposons que votre site dispose d'un KDC maître et de six KDC esclaves (illustrés dans la [Figure 21-2](#)), où *slave-1* jusqu'à *slave-3* correspond à un regroupement logique et *slave-4* jusqu'à *slave-6* correspond à un autre regroupement logique. Pour configurer une propagation parallèle, vous pouvez faire en sorte que le KDC maître propage la base de données à *slave-1* et *slave-4*. A leur tour, ces KDC esclaves pourraient propager la base de données aux KDC esclaves dans leur groupe.

FIGURE 21-2 Exemple de configuration de propagation parallèle



## Étapes de configuration d'une propagation parallèle

Ce qui suit n'est pas une procédure détaillée étape par étape, mais une liste de haut niveau des étapes de configuration permettant d'activer la propagation parallèle. Ces étapes impliquent ce qui suit :

1. Sur le KDC maître, modification de l'entrée `kprop_script` dans sa tâche `cron` afin d'inclure les arguments uniquement pour les KDC esclaves qui effectueront la propagation suivante (les *esclaves de propagation*).

2. Sur chaque esclave de propagation, l'ajout d'une entrée `kprop_script` dans sa tâche `cron`, qui doit inclure les arguments pour que les esclaves réalisent la propagation. Pour que la propagation parallèle s'effectue, la tâche `cron` doit être configurée de sorte qu'elle s'exécute après que la nouvelle base de données Kerberos soit propagée à l'esclave de propagation.

---

**Remarque** – Le temps que prend un esclave de propagation à se propager dépend de facteurs tels que la bande passante du réseau et la taille de la base de données Kerberos.

---

3. Sur chaque KDC esclave, configurez les autorisations appropriées à propager. Cette étape s'effectue en ajoutant le nom de l'hôte principal de son KDC de propagation à son fichier `kpropd.acl`.

**EXEMPLE 21-20** Configuration d'une propagation parallèle

Dans la [Figure 21-2](#), l'entrée `kprop_script` du KDC maître doit ressembler à ce qui suit :

```
0 3 * * * /usr/lib/krb5/kprop_script slave-1.example.com slave-4.example.com
```

L'entrée `kprop_script` du `slave-1` doit ressembler à ce qui suit :

```
0 4 * * * /usr/lib/krb5/kprop_script slave-2.example.com slave-3.example.com
```

Notez que la propagation sur l'esclave démarre une heure après sa propagation par le maître.

Le fichier `kpropd.acl` sur les esclaves de propagation doit contenir l'entrée suivante :

```
host/master.example.com@EXAMPLE.COM
```

Le fichier `kpropd.acl` sur les KDC esclaves propagés par `slave-1` contient l'entrée suivante :

```
host/slave-1.example.com@EXAMPLE.COM
```

## Administration du fichier stash

Le *fichier stash* contient la clé principale de la base de données Kerberos, qui est créée automatiquement lorsque vous créez une base de données Kerberos. Si le fichier *stash* est corrompu, vous pouvez utiliser la commande `stash` de l'utilitaire `kdb5_util` pour remplacer le fichier corrompu. Le seul moment où vous devez supprimer un fichier *stash* est après la suppression de la base de données Kerberos avec la commande `destroy` de `kdb5_util`. Dans la mesure où le fichier *stash* n'est pas automatiquement supprimé avec la base de données, vous devez d'abord supprimer le fichier *stash* pour terminer le nettoyage.

## ▼ Procédure de suppression d'un fichier stash

- 1 Connectez-vous en tant que superutilisateur au KDC contenant le fichier stash.

- 2 Supprimez le fichier stash.

```
# rm stash-file
```

Où *stash-file* est le chemin d'accès du fichier stash. Par défaut, le fichier stash est situé dans `/var/krb5/.k5.realm`.

---

**Remarque** – Si vous devez recréer le fichier stash, vous pouvez utiliser l'option `-f` de la commande `kdb5_util`.

---

## ▼ Procédure d'utilisation d'une nouvelle clé principale

- 1 Connectez-vous en tant qu'administrateur ou endosse un rôle ou nom d'utilisateur affecté au profil Kerberos Server Management (gestion de serveur Kerberos).

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

- 2 Créez une nouvelle clé principale.

Cette commande ajoute une nouvelle clé principale, générée de façon aléatoire. L'option `-s` requiert que la nouvelle clé principale soit stockée dans le fichier keytab par défaut.

```
# kdb5_util add_mkey -s
```

```
Creating new master key for master key principal 'K/M@EXAMPLE.COM'
You will be prompted for a new database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:      <Type the password>
Re-enter KDC database master key to verify:  <Type it again>
```

- 3 Vérifiez que la nouvelle clé principale existe.

```
# kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, No activate time set
KNVO: 1, Enctype: DES cbc mode with RSA-MD5, Active on: Wed Dec 31 18:00:00 CST 2001 *
```

L'astérisque dans cette sortie identifie la clé principale actuellement active.

- 4 Définissez le moment auquel la nouvelle clé principale deviendra active.

```
# date
Fri Jul 1 17:57:00 CDT 2011
# kdb5_util use_mkey 2 'now+2days'
```



**# kdb5\_util list\_mkeys**

Master keys for Principal: K/M@EXAMPLE.COM

KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, Active on: Sun Jul 03 17:57:15 CDT 2011

KNVO: 1, Enctype: DES cbc mode with RSA-MD5, Active on: Wed Dec 31 18:00:00 CST 2001 \*

Dans cet exemple, la date est définie deux jours plus tard pour laisser le temps à la nouvelle clé principale de se propager à tous les KDC. Ajustez la date selon les besoins de votre environnement.

## 5 (Facultatif) Après la création d'un nouveau principal, vérifiez que la nouvelle clé principale est en cours d'utilisation.

```
# kadmin.local -q 'getprinc jimf' | egrep 'Principal|MKey'
```

Authenticating as principal root/admin@EXAMPLE.COM with password.

Principal: jimf@EXAMPLE.COM

MKey: vno 2

Dans cet exemple, MKey: vno 2 indique que la clé secrète du principal est protégée par la nouvelle clé principale 2.

## 6 Re-chiffrez les clés secrètes de l'utilisateur principal avec la nouvelle clé principale.

Si vous ajoutez un argument de modèle à la fin de la commande, les principaux qui correspondent au modèle seront mis à jour. Ajoutez l'option -n à la syntaxe de cette commande afin d'identifier les principaux qui seront mis à jour.

```
# kdb5_util update_princ_encryption -f -v
```

Principals whose keys WOULD BE re-encrypted to master key vno 2:

updating: host/kdc1.example.com@EXAMPLE.COM

skipping: jimf@EXAMPLE.COM

updating: kadmin/changepw@EXAMPLE.COM

updating: kadmin/history@EXAMPLE.COM

updating: kdc/admin@EXAMPLE.COM

updating: host/kdc2.example.com@EXAMPLE.COM

6 principals processed: 5 updated, 1 already current

## 7 Purgez l'ancienne clé principale.

Lorsqu'une clé principale n'est plus utilisée pour protéger les clés secrètes des principaux, elle peut être purgée du principal de la clé principale. Cette commande ne purge pas la clé si celle-ci est encore utilisée par des principaux. Ajoutez l'option -n à cette commande pour vérifier que la clé principale appropriée sera purgée.

```
# kdb5_util purge_mkeys -f -v
```

Purging the following master key(s) from K/M@EXAMPLE.COM:

KNVO: 1

1 key(s) purged.

## 8 Vérifiez que l'ancienne clé principale a été purgée.

**# kdb5\_util list\_mkeys**

Master keys for Principal: K/M@EXAMPLE.COM

KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, Active on: Sun Jul 03 17:57:15 CDT 2011 \*

9 Mettez à jour le fichier stash.

```
# kdb5_util stash
Using existing stashed keys to update stash file.
```

10 Vérifiez que le fichier stash a été mis à jour.

```
# klist -kt /var/krb5/.k5.EXAMPLE.COM
Keytab name: FILE:.k5.EXAMPLE.COM
KVNO Timestamp Principal
-----
2 05/07/2011 15:08 K/M@EXAMPLE.COM
```

Gestion d'un KDC sur un serveur d'annuaire LDAP

La plupart des tâches d'administration du KDC qui utilisent un serveur d'annuaire LDAP sont identiques à celles du serveur DB2. Il existe quelques nouvelles tâches spécifiques à l'utilisation de LDAP.

TABLEAU 21-3 Configuration des serveurs KDC pour l'utilisation de LDAP (liste des tâches)

| Tâche                                                                                    | Description                                                                                                                                         | Voir                                                                                                                                     |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration d'un KDC maître.                                                           | Configure et construit le serveur KDC maître et une base de données pour un domaine à l'aide d'un processus manuel et à l'aide de LDAP pour le KDC. | <a href="#">"Procédure de configuration d'un KDC pour l'utilisation d'un serveur de données LDAP" à la page 384</a>                      |
| Association des attributs de principaux Kerberos aux types de classe objet non Kerberos. | Permet de partager les informations stockées avec les enregistrements Kerberos avec d'autres bases de données LDAP.                                 | <a href="#">"Procédure d'association des attributs de principaux Kerberos dans un type de classe d'objet non Kerberos" à la page 450</a> |
| Destruction d'un domaine.                                                                | Supprime toutes les données associées à un domaine.                                                                                                 | <a href="#">"Procédure de suppression d'un domaine d'un serveur d'annuaire LDAP" à la page 451</a>                                       |

▼ Procédure d'association des attributs de principaux Kerberos dans un type de classe d'objet non Kerberos

Cette procédure permet aux attributs de principaux Kerberos d'être associés aux types de classe d'objet non Kerberos. Dans cette procédure, les attributs `krbprincipalaux`, `krbTicketPolicyAux` et `krbPrincipalName` sont associés à la classe d'objet "personnes".

Dans cette procédure, les paramètres de configuration suivants sont utilisés :

- Serveur d'annuaire = `dsserver.example.com`
- Principal d'utilisateur = `willf@EXAMPLE.COM`

**1 Connectez-vous en tant que superutilisateur.****2 Préparez chaque entrée dans les classes d'objet personnes.**

Répétez cette étape pour chaque entrée.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
dn: uid=willf,ou=people,dc=example,dc=com
changetype: modify
objectClass: krbprincipalaux
objectClass: krbTicketPolicyAux
krbPrincipalName: willf@EXAMPLE.COM
EOF
```

**3 Ajoutez un attribut de sous-arborescence pour le conteneur de domaine.**

Cette étape permet d'effectuer des recherches d'entrées de principal dans le conteneur `ou=people,dc=example,dc=com`, ainsi que dans le conteneur `EXAMPLE.COM` par défaut.

```
# kdb5_ldap_util -D "cn=directory manager" modify \
    -subtrees 'ou=people,dc=example,dc=com' -r EXAMPLE.COM
```

**4 (Facultatif) Si les enregistrements de KDC sont stockés dans DB2, migrez les entrées DB2.****a. Videz les entrées DB2.**

```
# kdb5_util dump > dumpfile
```

**b. Chargez la base de données dans le serveur LDAP.**

```
# kdb5_util load -update dumpfile
```

**5 (Facultatif) Ajoutez les attributs de principal au KDC.**

```
# kadmin.local -q 'addprinc willf'
```

## ▼ Procédure de suppression d'un domaine d'un serveur d'annuaire LDAP

Cette procédure peut être utilisée si un autre serveur d'annuaire LDAP a été configuré pour gérer un domaine.

**1 Connectez-vous en tant que superutilisateur.****2 Supprimez le domaine.**

```
# kdb5_ldap_util -D "cn=directory manager" destroy
```

# Renforcement de la sécurité des serveurs Kerberos

Suivez les étapes ci-dessous pour accroître la sécurité des serveurs d'application Kerberos et des serveurs KDC.

TABLEAU 21-4 Renforcement de la sécurité des serveurs Kerberos (liste des tâches)

| Tâche                                                                              | Description                                                                                                                  | Voir                                                                                                                         |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Activation de l'accès à l'aide de l'authentification Kerberos.                     | Limitez l'accès réseau à un serveur pour permettre l'authentification Kerberos uniquement                                    | <a href="#">"Procédure d'activation des applications utilisant Kerberos uniquement" à la page 452</a>                        |
| Restriction de l'accès aux serveurs KDC.                                           | Améliorez la sécurité des serveurs KDC et de leurs données.                                                                  | <a href="#">"Procédure de restriction de l'accès aux serveurs KDC" à la page 453</a>                                         |
| Amélioration de la sécurité du mot de passe à l'aide d'un fichier de dictionnaire. | Augmentez la sécurité de tous les nouveaux mots de passe en vérifiant le nouveau mot de passe par rapport à un dictionnaire. | <a href="#">"Procédure d'utilisation d'un fichier dictionnaire pour augmenter la sécurité de mot de passe" à la page 453</a> |

## ▼ Procédure d'activation des applications utilisant Kerberos uniquement

Cette procédure restreint l'accès réseau au serveur qui exécute telnet, ftp, rcp, rsh et rlogin pour utiliser des transactions authentifiées par Kerberos uniquement.

- 1
- Connectez-vous en tant que superutilisateur.
- 2
- Modifiez la propriété `exec` pour le service `telnet`.  
Ajoutez l'option `-a user` à la propriété `exec` pour `telnet` pour limiter l'accès aux utilisateurs capables de fournir des informations d'authentification valides.  
`# inetadm -m svc:/network/telnet:default exec="/usr/sbin/in.telnetd -a user"`
- 3
- (Facultatif) Si elle n'est pas déjà configurée, modifiez la propriété `exec` pour le service `telnet`.  
Ajoutez l'option `-a` à la propriété `exec` pour que `ftp` autorise uniquement les connexions authentifiées par Kerberos.  
`# inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a"`
- 4
- Désactivez les autres services.  
Les démons `in.rshd` et `in.rlogind` doivent être désactivés.  
`# svcadm disable network/shell`  
`# svcadm disable network/login:rlogin`

## ▼ Procédure de restriction de l'accès aux serveurs KDC

Les serveurs KDC maîtres et esclaves disposent de copies de la base de données KDC stockées localement. La restriction de l'accès à ces serveurs pour sécuriser les bases de données est importante pour la sécurité globale de l'installation Kerberos.

### 1 Connectez-vous en tant que superutilisateur.

### 2 Désactivez les services distants, en fonction des besoins.

Pour fournir un serveur KDC sécurisé, tous les services réseau non essentiels doivent être désactivés. Selon votre configuration, certains de ces services sont peut-être déjà désactivés. Vérifiez le statut du service avec la commande `svcs`. Dans la plupart des cas, les seuls services devant s'exécuter sont `krb5kdc` et `krdb5_kprop` si KDC est un esclave ou uniquement `kadmin` si le KDC est un maître. En outre, tous les services utilisant l'interface de transport loopback (`ticlts`, `ticotsord` et `ticots`) peuvent rester activés.

```
# svcadm disable network/comsat
# svcadm disable network/dtspc/tcp
# svcadm disable network/finger
# svcadm disable network/login:rlogin
# svcadm disable network/rexec
# svcadm disable network/shell
# svcadm disable network/talk
# svcadm disable network/tname
# svcadm disable network/uucp
# svcadm disable network/rpc_100068_2-5/rpc_udp
```

### 3 Restreignez l'accès au matériel prenant en charge le KDC.

Pour limiter l'accès physique, assurez-vous que le serveur KDC et son moniteur se trouvent dans un site sécurisé. Les utilisateurs ne doivent pas être en mesure d'accéder à ce serveur d'une façon ou d'une autre.

### 4 Stockez les sauvegardes de la base de données KDC sur des disques locaux ou les KDC esclaves.

Réalisez des sauvegardes sur bande de votre KDC uniquement si les bandes sont stockées en toute sécurité. Suivez la même pratique pour les copies de fichiers `keytab`. Il serait préférable de stocker ces fichiers sur un système de fichiers local non partagé avec d'autres systèmes. Le système de stockage de fichiers peut être le serveur KDC maître ou n'importe lequel des KDC esclaves.

## ▼ Procédure d'utilisation d'un fichier dictionnaire pour augmenter la sécurité de mot de passe

Un fichier dictionnaire peut être utilisé par le service Kerberos pour éviter qu'un mot dans le dictionnaire soit utilisé en tant que mot de passe lors de la création de nouvelles informations d'identification. Pour rendre plus difficile le fait de deviner un mot de passe, il est judicieux

d'éviter l'utilisation de mots du dictionnaire en tant que mots de passe. Par défaut, le fichier `/var/krb5/kadm5.dict` est utilisé, mais il est vide.

### 1 Connectez-vous en tant que superutilisateur au KDC maître.

### 2 Editez le fichier de configuration KDC (`kdc.conf`).

Vous devez ajouter une ligne afin d'informer le service d'utiliser un fichier dictionnaire. Dans cet exemple, le dictionnaire utilisé est celui inclus dans l'utilitaire `spell`. Reportez-vous à la page de manuel [kdc.conf\(4\)](#) pour obtenir une description complète du fichier de configuration.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
        dict_file = /usr/share/lib/dict/words
    }
```

### 3 Redémarrez les démons Kerberos.

```
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

## Messages d'erreur et dépannage de Kerberos

---

Ce chapitre fournit les solutions aux messages d'erreur que vous pouvez recevoir lorsque vous utilisez le service Kerberos. Ce chapitre fournit également quelques conseils de dépannage pour différents problèmes. La liste suivante répertorie les informations fournies dans ce chapitre :

- “Messages d'erreur de l'outil SEAM” à la page 455
- “Messages d'erreur Kerberos courants (A-M)” à la page 456
- “Messages d'erreur Kerberos courants (N-Z)” à la page 466
- “Problèmes avec le format du fichier `krb5.conf`” à la page 471
- “Problèmes de propagation de la base de données Kerberos” à la page 471
- “Problèmes de montage d'un système de fichiers NFS utilisant Kerberos” à la page 472
- “Problèmes liés à l'authentification en tant qu'utilisateur `root`” à la page 473
- “Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX” à la page 473

## Messages d'erreur Kerberos

Cette section fournit des informations sur les messages d'erreur Kerberos, y compris la raison de chaque erreur et une façon de corriger la corriger.

### Messages d'erreur de l'outil SEAM

Unable to view the list of principals or policies; use the Name field.

**Origine :** Le principal admin avec lequel vous vous êtes connecté n'a pas de privilège de liste (l) dans le fichier ACL de Kerberos (`kadm5.ac1`). Par conséquent, vous ne pouvez pas afficher la liste des principaux ou la liste des stratégies.

**Solution :** Vous devez saisir les noms des principaux et des stratégies dans le champ de nom pour travailler sur ces derniers, ou vous devez vous connecter à l'aide d'un principal qui dispose des privilèges appropriés.

JNI: Java array creation failed  
JNI: Java class lookup failed  
JNI: Java field lookup failed  
JNI: Java method lookup failed  
JNI: Java object lookup failed  
JNI: Java object field lookup failed  
JNI: Java string access failed  
JNI: Java string creation failed

**Origine :** Un grave problème existe avec l'interface native Java utilisée par l'outil SEAM (gkadmin).

**Solution :** Quittez gkadmin et redémarrez-le. Si le problème persiste, veuillez signaler un bogue.

## Messages d'erreur Kerberos courants (A-M)

Cette section fournit une liste alphabétique (A-M) des messages d'erreur courants pour les commandes Kerberos, les démons Kerberos, la structure PAM, l'interface GSS, le service NFS et la bibliothèque Kerberos.

All authentication systems disabled; connection refused

**Origine :** Cette version de rlogind ne prend pas en charge de mécanisme d'authentification.

**Solution :** Vérifiez que la commande rlogind est appelée avec l'option -k.

Another authentication mechanism must be used to access this host

**Origine :** L'authentification n'a pas pu être effectuée.

**Solution :** Assurez-vous que le client utilise le mécanisme Kerberos V5 pour l'authentification.

Authentication negotiation has failed, which is required for encryption. Good bye.

**Origine :** L'authentification n'a pas pu être négociée avec le serveur.

**Solution :** Lancez le débogage d'authentification en appelant la commande telnet avec la commande toggle authdebug et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

Bad krb5 admin server hostname while initializing kadmin interface

**Origine :** Un nom d'hôte non valide est configuré pour admin\_server dans le fichier krb5.conf.



**Solution :** Assurez-vous que le nom d'hôte correct pour le KDC maître est indiqué sur la ligne `admin_server` du fichier `krb5.conf`.

Bad lifetime value

**Origine :** La valeur de durée de vie fournie n'est pas valide ou incorrectement formatée.

**Solution :** Assurez-vous que la valeur fournie est cohérente avec la section des formats d'heure de la page de manuel [kinit\(1\)](#).

Bad start time value

**Origine :** La valeur d'heure de démarrage fournie n'est pas valide ou incorrectement formatée.

**Solution :** Assurez-vous que la valeur fournie est cohérente avec la section des formats d'heure de la page de manuel [kinit\(1\)](#).

Cannot contact any KDC for requested realm

**Origine :** Aucun KDC n'a répondu dans le domaine demandé.

**Solution :** Assurez-vous qu'au moins un KDC (maître ou esclave) est accessible ou que le démon `krb5kdc` est en cours d'exécution sur les KDC. Consultez le fichier `/etc/krb5/krb5.conf` pour la liste de KDC configurés (`kdc = kdc-name`).

Cannot determine realm for host: host is '*hostname*'

**Origine :** Kerberos n'est pas en mesure de déterminer le nom de domaine de l'hôte.

**Solution :** Assurez-vous qu'il y a un nom de domaine par défaut ou que les mappages de nom de domaine sont définis dans le fichier de configuration Kerberos (`krb5.conf`).

Cannot find a kadmin KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find a kpassword KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find a master KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find any KDC entries in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

**Origine :** Le fichier `krb5.conf` ou l'enregistrement du serveur DNS n'est pas correctement configuré.

**Solution :** Assurez-vous que le fichier de configuration Kerberos (`/etc/krb5/krb5.conf`) ou les enregistrements du serveur DNS pour le KDC sont correctement configurés.

Cannot find address for '*hostname*': '*error-string*'

**Origine :** Aucune adresse n'a été trouvée dans les enregistrements du DNS pour le nom d'hôte donné.

**Solution :** Corrigez l'enregistrement d'hôte dans le DNS ou corrigez l'erreur dans la recherche DNS.

Cannot find KDC for requested realm

**Origine :** Aucun KDC n'a été trouvé dans le domaine demandé.

**Solution :** Assurez-vous que le fichier de configuration Kerberos (`krb5.conf`) indique un KDC dans la section `realm`.

cannot initialize realm *realm-name*

**Origine :** Le KDC n'a peut-être pas de fichier stash.

**Solution :** Assurez-vous que le KDC dispose d'un fichier stash. Si tel n'est pas le cas, créez un fichier stash en utilisant la commande `kdb5_util` et essayez de redémarrer la commande `krb5kdc`.

Cannot resolve KDC for requested realm

**Origine :** Kerberos n'est pas en mesure de déterminer un KDC pour le domaine.

**Solution :** Assurez-vous que le fichier de configuration Kerberos (`krb5.conf`) indique un KDC dans la section `realm`.

Cannot resolve network address for KDCs '*hostname*' discovered via DNS Service Location records for realm '*realm-name*'

Cannot resolve network address for KDCs '*hostname*' specified in `krb5.conf(4)` for realm '*realm-name*'

**Origine :** Le fichier `krb5.conf` ou l'enregistrement du serveur DNS n'est pas configuré correctement.

**Solution :** Assurez-vous que le fichier de configuration Kerberos (`/etc/krb5/krb5.conf`) et les enregistrements du serveur DNS pour le KDC sont correctement configurés.

Cannot reuse password

**Origine :** Le mot de passe que vous avez spécifié a déjà été utilisé par ce principal.

**Solution :** Choisissez un mot de passe qui n'a pas été choisi avant, ou du moins qui ne fait pas partie des mots de passe qui sont conservés dans la base de données KDC pour chaque principal. Cette stratégie est appliquée par la stratégie du principal.

Can't get forwarded credentials

**Origine :** Le transfert de données d'identification n'a pas pu être établi.

**Solution :** Assurez-vous que le principal dispose d'informations d'identification transmissibles.

Can't open/find Kerberos configuration file

**Origine :** Le fichier de configuration Kerberos (`krb5.conf`) n'était pas disponible.

**Solution :** Assurez-vous que le `krb5.conf` est disponible au bon emplacement et qu'il dispose des autorisations nécessaires. Ce fichier doit être accessible en écriture par root et lisible par tout le monde.

Client '*principal*' not found in Kerberos database

**Origine :** Le principal est absent de la base de données Kerberos.

**Solution :** Ajoutez le principal de client à la base de données Kerberos.

Client '*principal*' pre-authentication failed

**Origine :** L'authentification du principal a échoué.

**Solution :** Assurez-vous que l'utilisateur utilise le mot de passe correct.

Client did not supply required checksum--connection rejected

**Origine :** L'authentification avec somme de contrôle n'a pas été négociée avec le client. Le client utilise peut-être un ancien protocole Kerberos V5 qui ne prend pas en charge la prise en charge de connexion initiale.

**Solution :** Assurez-vous que le client utilise un protocole Kerberos V5 qui prend en charge la prise en charge de connexion initiale.

Client/server realm mismatch in initial ticket request: '*client-principal*' requesting ticket '*service-principal*'

**Origine :** Un conflit de domaine entre le client et le serveur s'est produit dans la requête de ticket initiale.

**Solution :** Assurez-vous que le serveur avec lequel vous communiquez est dans le même domaine que le client, ou que les configurations du domaine sont correctes.

Client or server has a null key

**Origine :** Le principal a une clé nulle.

**Solution :** Modifiez le principal afin qu'il dispose d'une clé non nulle en utilisant la commande `cpw de kadmin`.

Clock skew too great: '*client*' requesting ticket '*service-principal*' from KDC '*KDC-hostname*' (KDC-time). Skew is *value*

Clock skew too great: '*client*' AP request with ticket for '*service-principal*'. Skew is *value* (allowable *value*)

**Origine :** La différence entre l'heure signalée sur le client et le serveur KDC ou le serveur d'application est trop grande.

**Solution :** Configurez le protocole NTP (Network Time Protocol) pour conserver la synchronisation des horloges. Pour plus d'informations, reportez-vous à la section [“Synchronisation des horloges entre les KDC et les clients Kerberos”](#) à la page 427.

Communication failure with server while initializing kadmin interface

**Origine :** Le démon kadmind n'était pas en cours d'exécution sur l'hôte qui a été spécifié pour le serveur d'administration, également appelé KDC maître.

**Solution :** Assurez-vous d'avoir spécifié le nom d'hôte correct pour le KDC maître. Si vous avez spécifié le nom d'hôte correct, assurez-vous que kadmind est en cours d'exécution sur le KDC maître que vous avez spécifié.

Credentials cache file permissions incorrect

**Origine :** Vous ne disposez pas des autorisations de lecture ou d'écriture sur le cache d'informations d'identification (/tmp/krb5cc\_*uid*).

**Solution :** Assurez-vous que vous disposez des autorisations de lecture ou d'écriture sur le cache d'informations d'identification.

Credentials cache I/O operation failed XXX

**Origine :** Kerberos a rencontré un problème lors de l'écriture dans le cache d'informations d'identification du système (/tmp/krb5cc\_*uid*).

**Solution :** Assurez-vous que le cache d'informations d'identification n'a pas été supprimé et qu'il reste de l'espace sur le périphérique en utilisant la commande `df`.

Decrypt integrity check failed

**Origine :** Vous avez peut-être un ticket non valide.

**Solution :** Vérifiez les deux conditions suivantes :

- Assurez-vous que vos informations d'identification sont valides. Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.
- Assurez-vous que l'hôte cible dispose d'un fichier keytab avec la version correcte de la clé du service. Utilisez `kadmin` pour afficher le numéro de version de la clé du principal service (par exemple, `host/FQDN-hostname`) dans la base de données Kerberos. Utilisez également `klist -k` sur l'hôte cible pour vérifier qu'il a le même numéro de version de clé.

Decrypt integrity check failed for client 'principal' and server 'hostname'

**Origine :** Vous avez peut-être un ticket non valide.

**Solution :** Assurez-vous que vos informations d'identification sont valides. Détruisez vos tickets avec la commande `kdestroy`, puis créez de nouveaux tickets avec la commande `kinit`.

Encryption could not be enabled. Goodbye.

**Origine :** Le chiffrement n'a pas pu être négocié avec le serveur.

**Solution :** Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle encdebug` et consultez les messages de débogage pour en savoir plus.

Failed to find realm for *principal* in keytab

**Origine :** Le nom de domaine inclus dans le *principal* ne correspond pas au nom de domaine dans le principal stocké dans le fichier keytab.

**Solution :** Assurez-vous que les principaux utilisent le domaine correct.

failed to obtain credentials cache

**Origine :** Pendant l'initialisation de `kadmin`, une panne s'est produite lorsque `kadmin` a essayé afin d'obtenir des informations d'identification pour le principal `admin`.

**Solution :** Assurez-vous que vous avez utilisé le bon principal et le bon mot de passe lorsque vous avez exécuté `kadmin`.

Field is too long for this implementation

**Origine :** Le message qui a été envoyé par une application utilisant Kerberos était trop long. Cette erreur peut être générée si le protocole de transport est UDP, dont la taille maximale de message par défaut est 65535 octets. En outre, il existe des limites sur les champs individuels dans un message de protocole qui est envoyé par le service Kerberos.

**Solution :** Vérifiez que vous n'avez pas restreint le transport à UDP dans le fichier `/etc/krb5/kdc.conf` du serveur KDC.

GSS-API (or Kerberos) error

**Origine :** Ce message est un message d'erreur GSS-API ou Kerberos générique pouvant être causé par divers problèmes.

**Solution :** Vérifiez le fichier `/var/krb5/kdc.log` pour trouver le message d'erreur plus spécifique qui a été enregistré lorsque l'erreur s'est produite.

Hostname cannot be canonicalized for '*hostname*': '*error-string*'

**Origine :** Le client Kerberos ne peut pas trouver le nom d'hôte complet pour le serveur.

**Solution :** Assurez-vous que le nom d'hôte du serveur est défini dans le DNS et que les mappages adresse sur nom d'hôte et nom d'hôte sur adresse sont cohérents.

Illegal cross-realm ticket

**Origine :** Le ticket envoyé n'a pas les bons inter-domaines. Les domaines n'ont peut-être pas les bonnes relations d'approbation configurées.

**Solution :** Assurez-vous que les domaines que vous utilisez ont les bonnes relations d'approbation.

Improper format of Kerberos configuration file

**Origine :** Le fichier de configuration Kerberos a des entrées non valides.

**Solution :** Assurez-vous que toutes les relations dans le fichier `krb5.conf` sont suivies du signe “=” et d'une valeur. En outre, vérifiez que les crochets sont présents dans les paires pour chaque sous-section.

Inappropriate type of checksum in message

**Origine :** Le message contient une somme de contrôle non valide.

**Solution :** Vérifiez quels types de somme de contrôle valides sont indiqués dans les fichiers `krb5.conf` et `kdc.conf`.

Incorrect net address

**Origine :** Une incohérence s'est produite dans l'adresse réseau. L'adresse réseau dans le ticket qui a été transmis est différente de l'adresse réseau où le ticket a été traité. Ce message peut se produire lorsque des tickets sont transmis.

**Solution :** Assurez-vous que les adresses réseau sont correctes. Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.

Invalid credential was supplied

Service key not available

**Origine :** Le ticket de service du cache d'informations d'identification est peut-être incorrect.

**Solution :** Détruisez le cache d'informations d'identification actuel et exécutez de nouveau `kinit` avant d'essayer d'utiliser ce service.

Invalid flag for file lock mode

**Origine :** Une erreur Kerberos interne s'est produite.

**Solution :** Veuillez signaler un bogue.

Invalid message type specified for encoding

**Origine :** Kerberos n'a pas pu reconnaître le type de message qui a été envoyé par l'application utilisant Kerberos.

**Solution :** Si vous utilisez une application utilisant Kerberos qui a été développé par votre site ou un fournisseur, assurez-vous qu'elle utilise Kerberos correctement.

Invalid number of character classes

**Origine :** Le mot de passe que vous avez spécifié pour le principal ne contient pas suffisamment de classes de mot de passe, tel qu'appliqué par la stratégie du principal.

**Solution :** Assurez-vous que vous avez spécifié un mot de passe avec le nombre minimal de classes de mot de passe requis par la stratégie.

KADM err: Memory allocation failure

**Origine :** Il n'y a pas suffisamment de mémoire pour exécuter kadmin.

**Solution :** Libérez de la mémoire et essayez d'exécuter kadmin à nouveau.

kadmin: Bad encryption type while changing host/*FQDN*'s key

**Origine :** Plusieurs types de chiffrement par défaut sont inclus dans la version de base après la version Solaris 10 8/07. Les clients peuvent demander des types de chiffrement qui ne sont peut-être pas pris en charge par un KDC exécuté sur une version antérieure du logiciel.

**Solution :** Plusieurs solutions existent pour résoudre ce problème. La plus facile à mettre en oeuvre est donnée en premier :

1. Ajoutez les packages SUNWcry et SUNWcryr sur le serveur KDC. Ceci permet d'augmenter le nombre de types de chiffrement pris en charge par le KDC.
2. Définissez `permitted_ectypes` dans `krb5.conf` sur le client pour que le type de chiffrement `aes256` ne soit pas inclus. Cette étape doit être effectuée sur chaque nouveau client.

KDC can't fulfill requested option

**Origine :** Le KDC n'a pas autorisé l'option demandée. Il est possible que des options `postdatables` ou `transmissibles` soient demandées et que le KDC refuse. Un autre problème peut être une demande de renouvellement d'un TGT, sans avoir de TGT renouvelable.

**Solution :** Déterminez si vous demandez une option que le KDC n'autorise pas ou un type de ticket qui n'est pas disponible.

KDC policy rejects request

**Origine :** La stratégie du KDC n'a pas autorisé la demande. Par exemple, la demande au KDC n'a pas d'adresse IP. Ou une transmission a été demandée, mais le KDC ne l'a pas autorisée.

**Solution :** Assurez-vous que vous utilisez `kinit` avec les options appropriées. Si nécessaire, vous pouvez modifier la stratégie associée au principal ou modifier les attributs du principal afin d'autoriser la demande. Vous pouvez modifier la stratégie ou le principal en utilisant `kadmin`.

KDC reply did not match expectation: KDC not found. Probably got an unexpected realm referral

**Origine :** La réponse du KDC ne contient pas le nom de principal attendu ou d'autres valeurs dans la réponse n'étaient pas correctes.

**Solution :** Assurez-vous que le KDC avec lequel vous communiquez est conforme à RFC4120, que la demande envoyée est une demande Kerberos V5 ou que le KDC est disponible.

kdestroy: Could not obtain principal name from cache

**Origine :** Le cache d'informations d'identification est manquant ou endommagé.

**Solution :** Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via kinit, si nécessaire.

kdestroy: No credentials cache file found while destroying cache

**Origine :** Le cache d'informations d'identification (/tmp/krb5c\_*uid*) est manquant ou endommagé.

**Solution :** Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via kinit, si nécessaire.

kdestroy: TGT expire warning NOT deleted

**Origine :** Le cache d'informations d'identification est manquant ou endommagé.

**Solution :** Vérifiez que l'emplacement du cache fourni est correct. Supprimez et obtenez un nouveau TGT via kinit, si nécessaire.

Kerberos authentication failed

**Origine :** Le mot de passe Kerberos est incorrect ou ne peut pas être synchronisé avec le mot de passe UNIX.

**Solution :** Si les mots de passe ne sont pas synchronisés, vous devez spécifier un mot de passe différent pour terminer l'authentification Kerberos. Il est possible que l'utilisateur ait oublié son mot de passe d'origine.

Kerberos V5 refuses authentication

**Origine :** L'authentification n'a pas pu être négociée avec le serveur.

**Solution :** Lancez le débogage d'authentification en appelant la commande telnet avec la commande toggle authdebug et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

Key table entry not found

**Origine :** Il n'existe aucune entrée pour le principal de service dans le fichier keytab du serveur d'application réseau.

**Solution :** Ajouter le principal de service approprié au fichier keytab du serveur afin de pouvoir fournir le service utilisant Kerberos.

Key table file '*filename*' not found

**Origine :** Le fichier de table de clés nommé n'existe pas.

**Solution :** Créez le fichier de table de clés.



Key version *number* is not available for principal *principal*

**Origine :** La version des clés ne correspond pas à la version des clés sur le serveur d'application.

**Solution :** Vérifiez la version des clés sur le serveur d'application à l'aide de la commande `klist -k`.

Key version number for principal in key table is incorrect

**Origine :** La version de clé d'un principal dans le fichier keytab est différente de la version dans la base de données Kerberos. Soit la clé d'un service a été modifiée, soit vous utilisez un ancien ticket de service.

**Solution :** Si la clé d'un service a été modifiée (par exemple, en utilisant `kadmin`), vous devez extraire la nouvelle clé et la stocker dans le fichier keytab de l'hôte où le service est en cours d'exécution.

Sinon, vous utilisez peut-être un ancien ticket de service qui a une ancienne clé. Vous aurez peut-être besoin d'exécuter la commande `kdestroy`, puis la commande `kinit` à nouveau.

`kinit: gethostname failed`

**Origine :** Une erreur dans la configuration réseau local provoque l'échec de `kinit`.

**Solution :** Assurez-vous que l'hôte est correctement configuré.

`login: load_modules: can not open module /usr/lib/security/pam_krb5.so.1`

**Origine :** Le module PAM de Kerberos est manquant ou il ne s'agit pas d'un binaire exécutable valide.

**Solution :** Assurez-vous que le module PAM de Kerberos est dans les `/usr/lib/security` Directory et qu'il s'agit d'un fichier exécutable valide binaire. Assurez-vous également que le `/etc/pam.conf` contient le chemin d'accès correct à `pam_krb5.so.1`.

Looping detected getting initial creds: '*client-principal*' requesting ticket '*service-principal*'. Max loops is *value*. Make sure a KDC is available.

**Origine :** Kerberos a tenté à plusieurs reprises d'obtenir les tickets initiaux mais n'a pas réussi.

**Solution :** Assurez-vous qu'au moins un KDC répond aux demandes d'authentification.

Master key does not match database

**Origine :** Le vidage de base de données chargé n'a pas été créé à partir d'une base de données qui contient la clé principale. La clé principale est située dans `/var/krb5/.k5.REALM`.

**Solution :** Assurez-vous que la clé principale dans le vidage de base de données chargé correspond à la clé principale qui se trouve dans `/var/krb5/.k5.REALM`.

`Matching credential not found`

**Origine :** Les informations d'identification correspondant à votre demande n'ont pas été trouvées. Votre demande exige l'utilisation d'informations d'authentification qui ne sont pas disponibles dans le cache d'informations d'identification.

**Solution :** Détruisez vos tickets avec `kdest roy` et créez de nouveaux tickets avec `kinit`.

`Message out of order`

**Origine :** Les messages qui ont été envoyés à l'aide d'une confidentialité à ordre séquentielle ont été livrés sans tenir compte de l'ordre. Certains messages ont peut-être été perdus dans le processus.

**Solution :** Vous devez réinitialiser la session Kerberos.

`Message stream modified`

**Origine :** Un conflit est survenu entre la somme de contrôle calculée et la somme de contrôle du message. Le message a peut-être été modifié pendant la transmission, ce qui peut indiquer un problème de sécurité.

**Solution :** Assurez-vous que les messages sont envoyés sur le réseau correctement. Etant donné que ce message peut également indiquer la possible altération des messages pendant qu'ils sont en cours d'envoi, détruisez vos tickets à l'aide de `kdest roy` et réinitialisez les services Kerberos que vous êtes en train d'utiliser.

## Messages d'erreur Kerberos courants (N-Z)

Cette section fournit une liste alphabétique (N-Z) des messages d'erreur courants pour les commandes Kerberos, les démons Kerberos, la structure PAM, l'interface GSS, le service NFS et la bibliothèque Kerberos.

`No credentials cache file found`

**Origine :** Kerberos n'a pas trouvé le cache d'informations d'identification (`/tmp/krb5cc_uid`).

**Solution :** Assurez-vous que le fichier d'informations d'identification existe et qu'il est lisible. Si ce n'est pas le cas, essayez d'exécuter `kinit` une nouvelle fois.

`No credentials were supplied, or the credentials were unavailable or inaccessible`

`No credential cache found`

**Origine :** Le cache d'informations d'identification de l'utilisateur est incorrect ou n'existe pas.

**Solution :** L'utilisateur doit exécuter `kinit` avant d'essayer de démarrer le service.

No credentials were supplied, or the credentials were unavailable or inaccessible

No principal in keytab (' *filename* ') matches desired name *principal*

**Origine :** Une erreur s'est produite au cours d'une tentative d'authentification du serveur.

**Solution :** Assurez-vous que l'hôte ou le principal de service est dans le fichier keytab du serveur.

Operation requires "*privilege*" privilege

**Origine :** Le principal admin qui était en cours d'utilisation n'a pas les privilèges appropriés configurés dans le fichier `kadm5.acf`.

**Solution :** Utilisez une identité qui dispose des privilèges appropriés. Vous pouvez également configurer le principal qui a été utilisé afin qu'il dispose des privilèges appropriés en modifiant le fichier `kadm5.acf`. Généralement, un principal contenant `/admin` dans son nom est doté des privilèges appropriés.

PAM-KRB5 (auth): krb5\_verify\_init\_creds failed: Key table entry not found

**Origine :** L'application distante a tenté de lire le principal de service de l'hôte dans le fichier `/etc/krb5/krb5.keytab` local, mais il n'existe pas.

**Solution :** Ajoutez le principal de service de l'hôte au fichier keytab du serveur.

Password is in the password dictionary

**Origine :** Le mot de passe que vous avez spécifié se trouve dans un dictionnaire de mots de passe en cours d'utilisation. Votre mot de passe n'est pas un bon choix.

**Solution :** Choisissez un mot de passe qui mélange plusieurs classes de mot de passe.

Permission denied in replay cache code

**Origine :** Le cache de rediffusion du système n'a pas pu être ouvert. Votre serveur peut avoir été exécuté pour la première fois sous un ID utilisateur différent de votre ID d'utilisateur actuel.

**Solution :** Assurez-vous que le cache de rediffusion possède les autorisations appropriées. Le cache de rediffusion est stocké sur l'hôte sur lequel l'application de serveur utilisant Kerberos est en cours d'exécution. Le fichier du cache de rediffusion est appelé `/var/krb5/rcache/rc_service_name_uid` pour les utilisateurs non root. Pour les utilisateurs root le fichier du cache de rediffusion est appelé `/var/krb5/rcache/root/rc_service_name`.

Protocol version mismatch

**Origine :** Une demande Kerberos V4 a probablement été envoyée au KDC. Le service Kerberos ne prend en charge que le protocole Kerberos V5.

**Solution :** Assurez-vous que vos applications utilisent le protocole Kerberos V5.

Request is a replay

**Origine :** La demande a déjà été envoyée à ce serveur et traitée. Les tickets ont peut-être été volés et quelqu'un d'autre essaie de les réutiliser.

**Solution :** Attendez quelques minutes et relancez la demande.

Requested principal and ticket don't match: Requested principal is '*service-principal*' and TGT principal is '*TGT-principal*'

**Origine :** Le principal de service auquel vous vous connectez et le ticket de service que vous avez ne correspondent pas.

**Solution :** Assurez-vous que le service DNS fonctionne correctement. Si vous utilisez un logiciel d'un autre fabricant, assurez-vous qu'il utilise correctement les noms de principaux.

Requested protocol version not supported

**Origine :** Une demande Kerberos V4 a probablement été envoyée au KDC. Le service Kerberos ne prend en charge que le protocole Kerberos V5.

**Solution :** Assurez-vous que vos applications utilisent le protocole Kerberos V5.

Service key *service-principal* not available

**Origine :** Le principal de service nommé ne se trouve pas dans le fichier keytab sur le serveur d'application.

**Solution :** Assurez-vous que le principal de service est inclus dans le fichier keytab sur le serveur d'application ou lui correspond.

Server refused to negotiate authentication, which is required for encryption.  
Good bye.

**Origine :** L'application distante n'est pas capable ou a été configuré de manière à ne pas accepter l'authentification Kerberos du client.

**Solution :** Fournissez une application distante qui peut négocier l'authentification ou configurez l'application pour qu'elle utilise les indicateurs appropriés pour activer l'authentification.

Server refused to negotiate encryption. Good bye.

**Origine :** Le chiffrement n'a pas pu être négocié avec le serveur.

**Solution :** Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle encdebug` et consultez les messages de débogage pour en savoir plus.

Server rejected authentication (during sendauth exchange)

**Origine :** Le serveur avec lequel vous tentez de communiquer a rejeté l'authentification. La plupart du temps, cette erreur se produit pendant la propagation de base de données kerberos. Certaines causes courantes peuvent être des problèmes avec le fichier `kpropd.ac1`, DNS ou le fichier `keytab`.

**Solution :** Si vous recevez ce message d'erreur lorsque vous exécutez des applications autres que kprop, cherchez à savoir si le fichier keytab du serveur est correct.

Server *service-principal* not found in Kerberos database

**Origine :** Le principal de service n'est pas correct ou manque dans la base de données du principal.

**Solution :** Assurez-vous que le principal de service est correct et qu'il se trouve dans la base de données.

Target name principal '*principal*' does not match *service-principal*

**Origine :** Le principal de service en cours d'utilisation ne correspond pas au principal de service utilisé par le serveur d'application.

**Solution :** Sur le serveur d'application, veillez à ce que le principal de service soit inclus dans le fichier keytab. Pour le client, assurez-vous que le principal de service correct est utilisé.

The ticket isn't for us

Ticket/authenticator don't match

**Origine :** Un conflit est survenu entre le ticket et l'authentificateur. Le nom du principal de la demande peut ne pas correspondre au nom du principal de service. Soit le ticket a été envoyé avec un nom FQDN du principal alors que le service attendait un autre nom, soit le service attendait un FQDN et a reçu un autre nom.

**Solution :** Si vous recevez ce message d'erreur lorsque vous exécutez des applications autres que kprop, cherchez à savoir si le fichier keytab du serveur est correct.

Ticket expired

**Origine :** Votre ticket a expiré.

**Solution :** Détruisez vos tickets avec `kdestroy` et créez de nouveaux tickets avec `kinit`.

Ticket is ineligible for postdating

**Origine :** Le principal n'autorise pas ses tickets à être postdatés.

**Solution :** Modifier le principal avec `kadmin` pour l'autoriser.

Ticket not yet valid: '*client-principal*' requesting ticket '*service-principal*' from '*kdc-hostname*' (*time*). TGT start time is *time*.

**Origine :** Le ticket postdaté n'est pas encore valide.

**Solution :** Créez un nouveau ticket avec la date correcte ou attendez que le ticket actuel soit valide.

Truncated input file detected

**Origine :** Le fichier de vidage de base de données qui a été utilisé dans l'opération n'est pas un fichier de vidage complet.

**Solution :** Recréez le fichier de vidage ou utilisez-en un autre.

Unable to securely authenticate user ... exit

**Origine :** L'authentification n'a pas pu être négociée avec le serveur.

**Solution :** Lancez le débogage d'authentification en appelant la commande `telnet` avec la commande `toggle authdebug` et consultez les messages de débogage pour en savoir plus. En outre, assurez-vous que vous avez des informations d'identification valides.

Unknown encryption type: *name*

**Origine :** Le type de chiffrement inclus avec les informations d'identification ne peut pas être utilisé.

**Solution :** Déterminez les types de chiffrement utilisés par le client à l'aide de la commande `klist -e`. Assurez-vous que le serveur d'application prend en charge au moins l'un des types de chiffrement.

Wrong principal in request

**Origine :** Le ticket contenait un nom de principal non valide. Cette erreur peut indiquer un problème de DNS ou de FQDN.

**Solution :** Assurez-vous que le principal du service correspond au principal du ticket.

## Dépannage de Kerberos

Cette section fournit des informations de dépannage pour le logiciel Kerberos.

### ▼ Identification des problèmes liés aux numéros de version de clé

Parfois, le numéro de version de clé (KVNO) utilisé par le KDC et les clés du principal de service stockées dans le fichier `/etc/krb5/krb5.keytab` pour les services hébergés sur le système ne correspondent pas. Le KVNO peut être désynchronisé lors de la création d'un nouvel ensemble de clés sur le KDC sans mettre à jour le fichier de table de clés avec les nouvelles clés. Ce problème peut être diagnostiqué à l'aide de la procédure suivante.

**1 Répertoriez les entrées keytab.**

Notez que le KVNO pour chaque principal est inclus dans la liste.

```
# klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
-----
2 host/denver.example.com@EXAMPLE.COM
2 host/denver.example.com@EXAMPLE.COM
2 host/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
```

**2 Faites l'acquisition d'autorisations initiales à l'aide de la clé host.**

```
# kinit -k
```

**3 Déterminez le KVNO utilisé par le KDC.**

```
# kvno nfs/denver.example.com
nfs/denver.example.com@EXAMPLE.COM: kvno = 3
```

Notez que le KVNO répertorié ici est 3 au lieu de 2.

## Problèmes avec le format du fichier krb5.conf

Si le fichier `krb5.conf` n'est pas formaté correctement, le message d'erreur suivant peut s'afficher dans une fenêtre de terminal ou être enregistrée dans le fichier journal :

```
Improper format of Kerberos configuration file while initializing krb5 library
```

S'il y a un problème avec le format du fichier `krb5.conf`, les services associés sont vulnérables aux attaques. Vous devez résoudre le problème avant d'autoriser l'utilisation des fonctions de Kerberos.

## Problèmes de propagation de la base de données Kerberos

Si la propagation de base de données Kerberos échoue, essayez `/usr/bin/rlogin -x` entre le KDC esclave et le KDC maître, et depuis le KDC maître vers le serveur KDC esclave.

Si les KDC ont été configurés de façon à restreindre l'accès, `rlogin` est désactivé et ne peut pas être utilisé pour résoudre ce problème. Pour activer `rlogin` sur un KDC, vous devez activer le service `eklogin`.

```
# svcadm enable svc:/network/login:eklogin
```

Une fois que vous avez résolu le problème, vous devez désactiver le service `eklogin`.

Si `rlogin` ne fonctionne pas, les problèmes proviennent probablement des fichiers `keytab` des KDC. Si `rlogin` ne fonctionne pas, le problème ne provient pas du fichier `keytab` ou du service de noms, car `rlogin` et le logiciel de propagation utilisent le même principal `host/host-name`. Dans ce cas, assurez-vous que le fichier `kpropd.acf` est correct.

## Problèmes de montage d'un système de fichiers NFS utilisant Kerberos

- Si un montage de système de fichiers NFS utilisant Kerberos échoue, assurez-vous que le fichier `/var/ncache/root` existe sur le serveur NFS. Si le système de fichiers n'est pas détenu par `root`, supprimez-le et essayez de le monter une nouvelle fois.
- Si vous avez un problème d'accès à un système de fichiers NFS utilisant Kerberos, assurez-vous que le service `gssd` est activé sur votre système et le serveur NFS.
- Si vous voyez le message d'erreur `invalid argument` ou `bad directory` lorsque vous tentez d'accéder à un système de fichiers NFS utilisant Kerberos, le problème est peut-être que vous n'utilisez pas un nom DNS complet lorsque vous essayez de monter le système de fichiers NFS. L'hôte qui est en cours de montage n'est pas le même que le composant du nom de l'hôte du principal de service dans le fichier `keytab` du serveur.

Ce problème peut également se produire si votre serveur dispose de plusieurs interfaces Ethernet, et que vous avez configuré DNS pour qu'il utilise un plan de type "nom par interface" au lieu de "plusieurs enregistrements d'adresses par hôte". Pour le service Kerberos, vous devez configurer plusieurs enregistrements d'adresses par hôte comme suit<sup>1</sup> :

```
my.host.name.      A      1.2.3.4
                   A      1.2.4.4
                   A      1.2.5.4

my-en0.host.name.  A      1.2.3.4
my-en1.host.name.  A      1.2.4.4
my-en2.host.name.  A      1.2.5.4

4.3.2.1            PTR    my.host.name.
4.4.2.1            PTR    my.host.name.
4.5.2.1            PTR    my.host.name.
```

Dans cet exemple, la configuration autorise une référence pour les différentes interfaces et un seul principal de service au lieu de trois principaux de service dans le fichier `keytab` du serveur.

---

<sup>1</sup> Ken Hornstein, "FAQ Kerberos," [<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#kerbdns>], consulté le 10 mars 2010.



## Problèmes liés à l'authentification en tant qu'utilisateur root

En cas d'échec de l'authentification lorsque vous essayez de vous connecter en tant que superutilisateur sur votre système et que vous avez déjà ajouté le principal root au fichier keytab de votre hôte, il y a deux problèmes potentiels à vérifier. Tout d'abord, assurez-vous que le principal root dans le fichier keytab a un nom d'hôte complet comme instance. Si c'est le cas, vérifiez le fichier `/etc/resolv.conf` pour vous assurer que le système est correctement configuré en tant que client DNS.

## Observation du mappage d'informations d'identification GSS sur des informations d'identification UNIX

Pour être en mesure de contrôler les correspondances d'informations d'identification, commencez par décommenter cette ligne du fichier `/etc/gss/gsscred.conf`.

```
SYSLOG_UID_MAPPING=yes
```

Ensuite demandez au service `gssd` d'obtenir des informations depuis le fichier `/etc/gss/gsscred.conf`.

```
# pkill -HUP gssd
```

Maintenant, vous devez être en mesure de contrôler les mappages d'informations d'identification quand `gssd` les demande. Les mappages sont enregistrés par `syslogd`, si le fichier `syslog.conf` est configuré pour l'utilitaire système `auth` avec le niveau de gravité `debug`.

## Utilisation de DTrace avec le service Kerberos

Dans cet exemple, vous souhaitez savoir si la pré-authentification est requise par un KDC, et, le cas échéant, quels types de pré-authentification sont pris en charge. Tout d'abord, en tant qu'utilisateur privilégié, créez un fichier source du programme D semblable au suivant :

```
# cat kerberos_preauth.d
kerberos$target::krb_error-read
{
    self->preauth = args[1]->kerror_error_code ==
        "KDC_ERR_PREAUTH_REQUIRED(25)" ? "required" : "not required";

    printf(" - Preauthentication is %s for this KDC.\n", self->preauth);
}
```

```
kerberos$target:::krb_error-read
/ self->preauth == "required" /
{
    printf(" - This KDC supports the following preauth types: %s.",
        args[1]->error_e_data);
}
```

Ensuite, compilez le fichier source `preauth.d` pour obtenir votre réponse.

```
# dtrace -qs kerberos_preauth.d -c "kinit -k"
- Preauthentication is required for this KDC.
- This KDC supports the following preauth types: ENC_TIMESTAMP(2)
FX_FAST(136) PK_ETYPE_INFO2(19) SAM_RESPONSE(13) FX_COOKIE(133).
```

Pour plus d'informations sur les divers types de pré-authentification, consultez la page [RFC 4120](#).

## Administration des principaux et des stratégies Kerberos (tâches)

---

Ce chapitre décrit les procédures d'administration des principaux et des stratégies qui leur sont associées. Ce chapitre indique également comment administrer un fichier keytab d'hôte.

Ce chapitre est destiné à tous ceux qui ont besoin d'administrer des principaux et des stratégies. Avant d'utiliser ce chapitre, vous devez vous familiariser avec les principaux et les stratégies, y compris les considérations de planification. Reportez-vous au [Chapitre 19, “Introduction au service Kerberos”](#) et au [Chapitre 20, “Planification du service Kerberos”](#), respectivement.

La liste suivante répertorie les informations fournies dans ce chapitre :

- “Méthodes d'administration des principaux et des stratégies Kerberos” à la page 475
- “outil SEAM” à la page 476
- “Gestion des principaux de Kerberos” à la page 480
- “Administration des stratégies Kerberos” à la page 494
- “Référence de l'outil SEAM” à la page 503
- “Administration des fichiers keytab” à la page 508

## Méthodes d'administration des principaux et des stratégies Kerberos

La base de données Kerberos sur le KDC maître contient tous les principaux Kerberos du domaine, leurs mots de passe, les stratégies et d'autres informations administratives. Pour créer et supprimer des principaux et pour modifier leurs attributs, vous pouvez utiliser les commandes `kadmin` ou `gkadmin`.

La commande `kadmin` fournit une interface de ligne de commande interactive qui permet de mettre à jour les principaux, les stratégies et les fichiers `keytab` de Kerberos. Il existe deux versions de la commande `kadmin` :

- `kadmin` : utilise l'authentification Kerberos pour fonctionner en toute sécurité de n'importe où sur le réseau
- `kadmin.local` : doit être exécutée directement sur le KDC maître

Outre le fait que `kadmin` utilise Kerberos pour authentifier l'utilisateur, les capacités de ces deux versions sont identiques. La version locale est nécessaire pour vous permettre de configurer suffisamment de la base de données pour pouvoir utiliser la version distante.

De plus, la version Oracle Solaris fournit l'outil SEAM, `gkadmin`, une interface utilisateur graphique interactive, qui propose globalement les mêmes possibilités que la commande `kadmin`. Pour plus d'informations, reportez-vous à la section “[outil SEAM](#)” à la page 476.

## outil SEAM

L'outil SEAM (`gkadmin`) est une interface graphique interactive qui permet de mettre à jour les principaux et les stratégies de Kerberos. Cet outil fournit globalement les mêmes fonctions que la commande `kadmin`. Toutefois, il ne prend pas en charge la gestion des fichiers `keytab`. Vous devez utiliser la commande `kadmin` pour gérer les fichiers `keytab`, comme décrit dans la section “[Administration des fichiers keytab](#)” à la page 508.

Similaire à la commande `kadmin`, l'outil SEAM utilise l'authentification Kerberos et le RPC chiffré pour fonctionner en toute sécurité depuis n'importe quel point du réseau. L'outil SEAM permet d'effectuer les opérations suivantes :

- Créer des principaux basés sur les valeurs par défaut ou des principaux existants.
- Créer des stratégies basées sur des stratégies existantes.
- Ajouter des commentaires pour les principaux.
- Définir des valeurs par défaut pour la création de principaux.
- Se connecter en tant qu'un autre principal sans quitter l'outil.
- Imprimer ou enregistrer des listes de principaux et des listes de stratégies.
- Afficher ou rechercher des listes de principaux et des listes de stratégies.

L'outil SEAM fournit également une aide contextuelle et une aide en ligne générale.

La liste des tâches suivante fournit des indications sur les différentes tâches réalisables avec l'outil SEAM :

- “[Gestion des principaux de Kerberos \(liste des tâches\)](#)” à la page 480
- “[Administration des stratégies Kerberos \(liste des tâches\)](#)” à la page 494

En outre, reportez-vous à la section “[Descriptions des panneaux de l'outil SEAM](#)” à la page 503 pour obtenir les descriptions de tous les attributs de principaux et de stratégies que vous pouvez spécifier ou afficher dans l'outil SEAM.

## Equivalents de ligne de commande de l'outil SEAM

Cette section répertorie les commandes `kadmin` qui fournissent les mêmes fonctionnalités que l'outil SEAM. Ces commandes peuvent être utilisées sans exécuter un système X Window System. Même si la plupart des procédures de ce chapitre utilisent l'outil SEAM, plusieurs procédures fournissent également des exemples qui utilisent les équivalents de ligne de commande.

TABLEAU 23-1 Equivalents de ligne de commande de l'outil SEAM

| Procédure outil SEAM                                              | Equivalent de la commande <code>kadmin</code>                 |
|-------------------------------------------------------------------|---------------------------------------------------------------|
| Affichage de la liste de principaux.                              | <code>list_principals</code> ou <code>get_principals</code>   |
| Affichage des attributs d'un principal.                           | <code>get_principal</code>                                    |
| Création d'un principal.                                          | <code>add_principal</code>                                    |
| Duplication d'un principal.                                       | Pas d'équivalent de ligne de commande                         |
| Modification d'un principal.                                      | <code>modify_principal</code> ou <code>change_password</code> |
| Suppression d'un principal.                                       | <code>delete_principal</code>                                 |
| Définition des valeurs par défaut pour la création de principaux. | Pas d'équivalent de ligne de commande                         |
| Affichage de la liste des stratégies.                             | <code>list_policies</code> ou <code>get_policies</code>       |
| Affichage des attributs d'une stratégie.                          | <code>get_policy</code>                                       |
| Création d'une stratégie.                                         | <code>add_policy</code>                                       |
| Duplication d'une stratégie.                                      | Pas d'équivalent de ligne de commande                         |
| Modification d'une stratégie.                                     | <code>modify_policy</code>                                    |
| Suppression d'une stratégie.                                      | <code>delete_policy</code>                                    |

## Seul fichier modifié par l'outil SEAM

Le seul fichier modifié par l'outil SEAM est le fichier `$HOME/.gkadmin`. Ce fichier contient les valeurs par défaut pour la création de principaux. Vous pouvez mettre à jour ce fichier en choisissant Properties (Propriétés) dans le menu Edit (Edition).

## Fonctions d'impression et d'aide en ligne de l'outil SEAM

L'outil SEAM fournit des fonctions d'impression et d'aide en ligne. Depuis le menu Print (Imprimer), vous pouvez envoyer les éléments suivants vers une imprimante ou un fichier :

- Liste des principaux disponibles sur le KDC maître spécifié
- Liste des stratégies disponibles sur le KDC maître spécifié
- Principal actuellement sélectionné ou chargé
- Stratégie actuellement sélectionnée ou chargée

Dans le menu d'aide, vous pouvez accéder à l'aide contextuelle et à l'aide générale. Lorsque vous choisissez l'option d'aide contextuelle dans le menu d'aide, la fenêtre d'aide contextuelle s'affiche et l'outil passe en mode d'aide. En mode d'aide, lorsque vous cliquez sur les champs, les étiquettes ou les boutons de la fenêtre, l'aide de ces éléments est affichée dans la fenêtre d'aide. Pour revenir au mode normal, cliquez sur Dismiss (Fermer) dans la fenêtre d'aide.

Vous pouvez également utiliser le sommaire de l'aide, qui s'ouvre dans un navigateur HTML et fournit des indications sur la présentation générale et des informations sur les tâches de ce chapitre.

## Utilisation de grandes listes dans l'outil SEAM

Quand votre site commence à accumuler un grand nombre de principaux et de stratégies, le temps qu'il faut à l'outil SEAM pour charger et afficher les listes de principaux et de stratégies s'allonge. Par conséquent, votre productivité avec l'outil baisse. Il existe plusieurs façons de remédier à ce problème.

Tout d'abord, vous pouvez éliminer totalement le temps de chargement des listes en empêchant l'outil SEAM de les charger. Pour définir cette option, choisissez Propriétés dans le menu Edit, puis désactivez l'option Show Lists (Afficher les listes). Bien entendu, lorsque l'outil ne charge pas les listes, il ne peut pas les afficher et vous ne pouvez plus utiliser les panneaux de listes pour sélectionner des principaux et des stratégies. Au lieu de cela, vous devez saisir un nom de principal ou de stratégie dans le nouveau champ de nom qui est fourni, puis sélectionner l'opération que vous souhaitez effectuer. Dans les faits, la saisie d'un nom est équivalente à la sélection d'un élément dans la liste.

Une autre façon de travailler avec de grandes listes est de les mettre en cache. En fait, la mise en cache des listes pour une période limitée est définie comme le comportement par défaut pour l'outil SEAM. L'outil SEAM doit toujours initialement charger les listes dans le cache. Mais après cela, l'outil peut utiliser le cache plutôt que d'extraire les listes à nouveau. Cette option supprime la nécessité de continuer à charger les listes à partir du serveur, ce qui est très long.

Vous pouvez paramétrer la mise en cache de listes en sélectionnant **Propriétés** dans le menu **Edit**. Il existe deux paramètres de mise en cache. Vous pouvez choisir de mettre en cache la liste indéfiniment ou de spécifier une limite dans le temps lorsque l'outil doit recharger les listes à partir du serveur dans le cache.

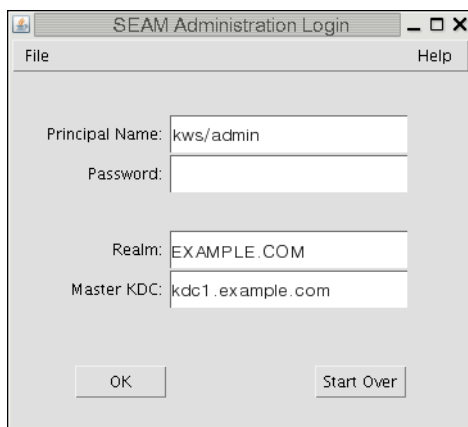
La mise en cache des listes vous permet toujours d'utiliser les panneaux de listes pour sélectionner des principaux et des stratégies, de sorte qu'il n'y a pas d'incidence sur la manière dont vous utilisez l'outil SEAM comme avec la première option. En outre, même si la mise cache ne vous permet pas de voir les modifications d'autres utilisateurs, vous pouvez toujours voir les dernières informations relatives à la liste en fonction de vos modifications, car celles-ci mettent à jour les listes sur le serveur et dans le cache. Et, si vous souhaitez mettre à jour le cache pour voir d'autres modifications et récupérer la dernière copie des listes, vous pouvez utiliser le menu **Refresh (Actualiser)** chaque fois que vous le souhaitez pour actualiser le cache depuis le serveur.

## ▼ Procédure de démarrage de l'outil SEAM

### 1 Démarrez l'outil SEAM en utilisant la commande `gkadmin`.

```
$ /usr/sbin/gkadmin
```

La fenêtre de connexion d'administration SEAM s'affiche.



### 2 Si vous ne souhaitez pas utiliser les valeurs par défaut, spécifiez de nouvelles valeurs par défaut.

La fenêtre est automatiquement renseignée avec des valeurs par défaut. Le nom de principal par défaut est déterminé en prenant votre identité en cours à partir de la variable d'environnement `USER` et en lui ajoutant `/admin` (`username/admin`). Les champs de domaine et de KDC maître par défaut sont sélectionnés à partir du fichier `/etc/krb5/krb5.conf`. Si vous souhaitez récupérer les valeurs par défaut, cliquez sur **Start Over (Recommencer)**.

**Remarque** – Les opérations d'administration que chaque nom de principal peut effectuer sont déterminées par le fichier ACL Kerberos, /etc/krb5/kadm5.ac1. Pour plus d'informations sur les privilèges limités, reportez-vous à la section [“Utilisation de l'outil SEAM avec privilèges d'administration Kerberos limités”](#) à la page 506.

- 3 Saisissez un mot de passe pour le nom de principal spécifié.
- 4 Cliquez sur OK.  
Une fenêtre contenant tous les principaux s'affiche.

## Gestion des principaux de Kerberos

Cette section fournit des instructions détaillées permettant d'administrer les principaux à l'aide de l'outil SEAM. Elle fournit également des exemples d'équivalents de lignes de commande, le cas échéant.

### Gestion des principaux de Kerberos (liste des tâches)

| Tâche                                   | Description                                                                                                                                                                                                                                                                                                                                     | Voir                                                                                        |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Affichage de la liste de principaux.    | Affichez la liste des principaux en cliquant sur l'onglet Principals (Principaux).                                                                                                                                                                                                                                                              | <a href="#">“Procédure d'affichage de la liste des principaux Kerberos”</a> à la page 482   |
| Affichage des attributs d'un principal. | Affichez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier).                                                                                                                                                                                                       | <a href="#">“Procédure d'affichage des attributs d'un principal Kerberos”</a> à la page 484 |
| Création d'un principal.                | Créez un principal en cliquant sur le bouton Create New (Créer) dans le panneau Principal List (Liste de principaux).                                                                                                                                                                                                                           | <a href="#">“Procédure de création d'un principal Kerberos”</a> à la page 486               |
| Duplication d'un principal.             | Dupliquez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Duplicate (Dupliquer).                                                                                                                                                                                                  | <a href="#">“Procédure de duplication d'un principal Kerberos”</a> à la page 489            |
| Modification d'un principal.            | Modifiez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier).<br><br>Notez que vous ne pouvez pas modifier le nom d'un principal. Pour renommer un principal, vous devez le dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancien principal. | <a href="#">“Procédure de modification d'un principal Kerberos”</a> à la page 490           |



| Tâche                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                        | Voir                                                                                                                    |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Suppression d'un principal.                                                              | Supprimez les attributs d'un principal en le sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Delete (Supprimer).                                                                                                                                                                                                                        | <a href="#">“Procédure de suppression d'un principal Kerberos” à la page 491</a>                                        |
| Définition des valeurs par défaut pour la création de principaux.                        | Définissez des valeurs par défaut pour la création de principaux en sélectionnant Properties (Propriétés) dans le menu Edit (Edition).                                                                                                                                                                                                                             | <a href="#">“Procédure de paramétrage des valeurs par défaut pour la création de principaux Kerberos” à la page 492</a> |
| Modification des privilèges d'administration Kerberos (fichier <code>kadm5.ac1</code> ). | <i>Ligne de commande uniquement.</i> Les privilèges d'administration Kerberos déterminent les opérations qu'un principal peut effectuer sur la base de données Kerberos, tels que l'ajout et la modification.<br><br>Vous devez modifier le fichier <code>/etc/krb5/kadm5.ac1</code> pour modifier les privilèges d'administration Kerberos pour chaque principal. | <a href="#">“Procédure de modification des privilèges d'administration Kerberos” à la page 493</a>                      |

## Automatisation de la création de principaux Kerberos

Même si l'outil SEAM offre une certaine facilité d'utilisation, il ne propose pas de moyen d'automatiser la création de principaux. L'automatisation est particulièrement utile si vous avez besoin d'ajouter 10 ou même 100 nouveaux principaux dans un court laps de temps. Vous pouvez toutefois automatiser la création de principaux en utilisant la commande `kadmin.local` dans un script shell Bourne.

La ligne de script shell suivante illustre une manière d'automatiser la création de nouveaux principaux :

```
awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |
time /usr/sbin/kadmin.local> /dev/null
```

Cet exemple est réparti sur deux lignes pour une meilleure lisibilité. Le script lit un fichier appelé `princnames` contenant les noms de principaux et leurs mots de passe, et les ajoute à la base de données Kerberos. Vous devez créer le fichier `princnames` contenant un nom de principal et son mot de passe sur chaque ligne, séparés par un ou plusieurs espaces. L'option `+needchange` configure le principal de manière à ce que l'utilisateur soit invité à saisir un nouveau mot de passe lors de la première connexion au principal. Cette pratique permet de s'assurer que les mots de passe dans le fichier `princnames` ne représentent pas un risque pour la sécurité.

Vous pouvez construire des scripts plus élaborés. Par exemple, le script peut utiliser les informations contenues dans le service de noms pour obtenir la liste des noms d'utilisateur pour les noms de principaux. Ce que vous faites et la manière dont vous le faites est déterminé par les besoins de votre site et votre expérience en script.

## ▼ Procédure d'affichage de la liste des principaux Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

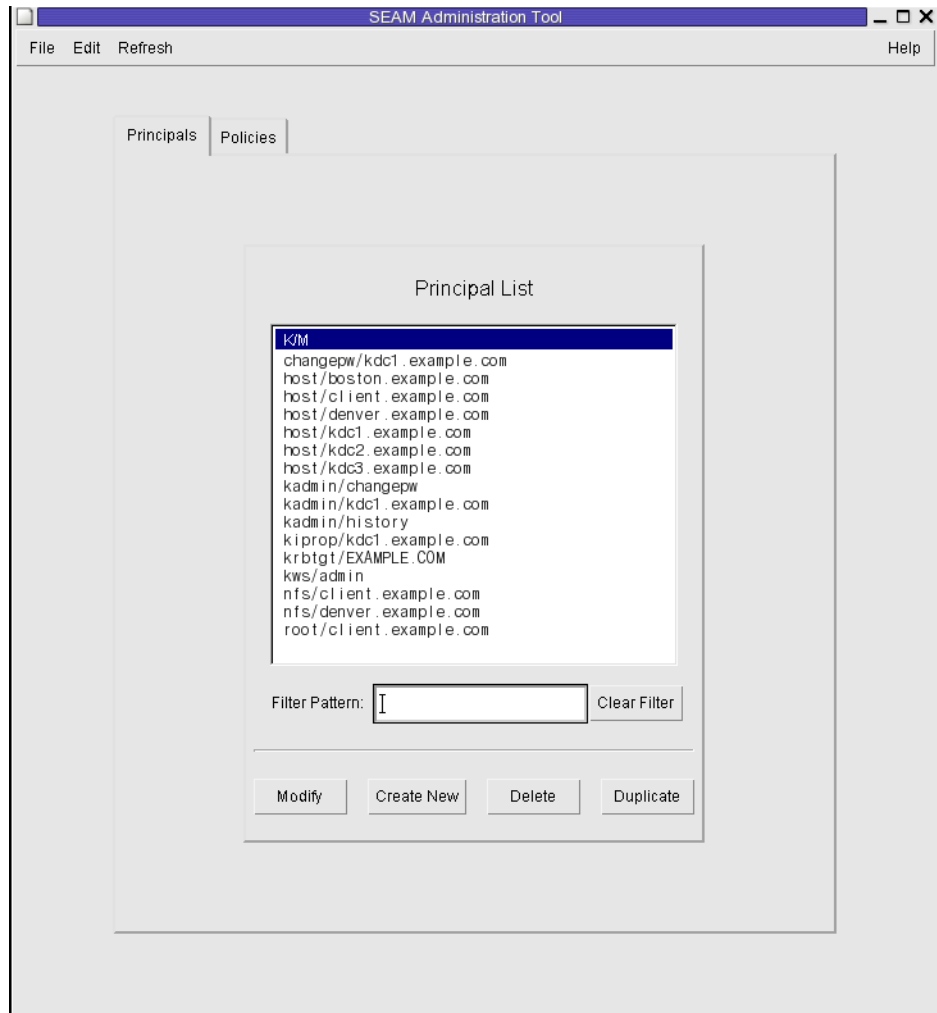
### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM”](#) à la page 479.

```
$ /usr/sbin/gkadmin
```

## 2 Cliquez sur l'onglet Principals (Principaux).

La liste de principaux s'affiche.



## 3 Affichez un principal spécifique ou une sous-liste de principaux.

Saisissez une chaîne dans le champ de filtre et appuyez sur la touche Entrée. Si le filtre fonctionne, la liste de principaux qui lui correspond s'affiche.

La chaîne du filtre doit être composée d'un ou plusieurs caractères. Notez bien que le mécanisme de filtrage respecte la casse et qu'il vous faut utiliser les majuscules et minuscules appropriées. Par exemple, si vous entrez la chaîne de filtrage `ge`, le mécanisme de filtrage affiche uniquement les principaux contenant la chaîne `ge` (`george` ou `edge` par exemple).

Si vous souhaitez afficher l'intégralité de la liste de principaux, cliquez sur Clear Filter (Supprimer le filtre).

### Exemple 23–1 Affichage de la liste de principaux Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `list_principals` de `kadmin` est utilisée pour obtenir la liste de tous les principaux correspondant à `kadmin*`. Les caractères génériques peuvent être utilisés avec la commande `list_principals`.

```
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.con@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
kadmin: quit
```

## ▼ Procédure d'affichage des attributs d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Principals (Principaux).

### 3 Sélectionnez le principal dans la liste que vous souhaitez afficher, puis cliquez sur Modify (Modifier).

Le panneau Principal Basics (Informations de base du principal) contenant certains attributs du principal s'affiche.

### 4 Continuez à cliquer sur Next (Suivant) pour afficher tous les attributs du principal.

Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section [“Descriptions des panneaux de l'outil SEAM” à la page 503](#).

### 5 Lorsque vous avez fini de consulter ces informations, cliquez sur Cancel (Annuler).

**Exemple 23-2** Affichage des attributs d'un principal Kerberos

L'exemple suivant montre la première fenêtre lorsque vous visualisez le principal `jdb/admin`.

The screenshot shows the 'SEAM Administration Tool' window with the 'Principals' tab selected. The 'Principal Basics' dialog is open, displaying the following fields and values:

- Principal Name:** `jdb/admin`
- Password:** (empty text box)
- Generate Random Password:** (button)
- Encryption Key Types:** `aes256-cts-hmac-sha1-96:no` (with a dropdown arrow)
- Policy:** `(no policy)` (with a dropdown arrow)
- Account Expires:** `Never` (with a dropdown arrow)
- Admin History:**
  - Last Principal Change:** Sep 28, 2009 1:32:23 PM
  - Last Changed By:** `host/admin@EXAMPLE.COM`
  - Comments:** (empty text box)

At the bottom of the dialog are buttons for **Save**, **Previous**, **Next**, and **Cancel**. The main window title is 'Modify Principal'.

**Exemple 23-3** Affichage des attributs d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `get_principal` de `kadmin` est utilisée pour afficher les attributs du principal `jdb/admin`.

```
kadmin: getprinc jdb/admin
Principal: jdb/admin@EXAMPLE.COM

Expiration date: [never]
Last password change: [never]

Password expiration date: Wed Apr 14 11:53:10 PDT 2011
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
Last modified: Mon Sep 28 13:32:23 PST 2009 (host/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 1
Key: vno 1, AES-256 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, AES-128 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, Triple DES with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

## ▼ Procédure de création d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

---

**Remarque** – Si vous voulez créer un principal susceptible de requérir une nouvelle stratégie, vous devez d'abord créer cette stratégie. Reportez-vous à la section [“Procédure de création d'une stratégie Kerberos” à la page 499](#).

---

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Principals (Principaux).

### 3 Cliquez sur New (Nouveau).

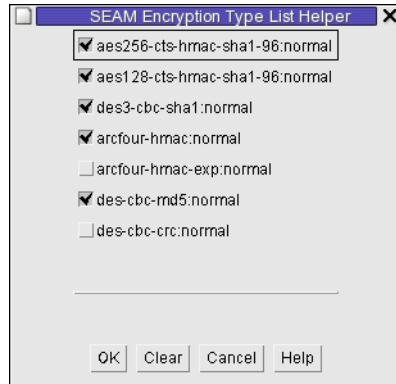
Le panneau Principal Basics (Informations de base du principal) contenant certains attributs du principal s'affiche.

### 4 Indiquez un nom de principal et un mot de passe.

Les deux sont obligatoires.

### 5 Spécifiez les types de chiffrement pour le principal.

Cliquez sur la boîte située à droite du champ de type de clé de chiffrement pour ouvrir une nouvelle fenêtre qui affiche l'ensemble des types de clés de chiffrement disponibles. Cliquez sur OK après avoir sélectionné les types de chiffrement requis.



### 6 Spécifiez la stratégie pour le principal.

### 7 Spécifiez des valeurs pour les attributs du principal et continuez d'appuyer sur Next (Suivant) pour en spécifier d'autres.

Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section [“Descriptions des panneaux de l'outil SEAM”](#) à la page 503.

### 8 Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.

### 9 Si nécessaire, configurez les privilèges d'administration de Kerberos pour le nouveau principal dans le fichier `/etc/krb5/kadm5.acl`.

Pour plus d'informations, reportez-vous à la section [“Procédure de modification des privilèges d'administration Kerberos”](#) à la page 493.

## Exemple 23–4 Création d'un principal Kerberos

L'exemple suivant montre le panneau Principal Basics (Informations de base du principal) lorsqu'un principal appelée pak est créé. La stratégie est définie sur testuser.

The screenshot shows the SEAM Administration Tool window with the 'Principals' tab selected. The 'Principal Basics' form is displayed, containing the following fields and controls:

- Principal Name:** A text box containing 'pak'.
- Password:** A text box with masked characters (asterisks).
- Generate Random Password:** A button.
- Encryption Key Types:** A dropdown menu showing 'aes256-cts-hmac-sha1-96:...' with a selection icon.
- Policy:** A dropdown menu showing 'testuser' with a selection icon.
- Account Expires:** A date/time picker showing 'Oct 8, 2010 10:49:40 AM'.
- Admin History:** A section containing:
  - Last Principal Change:** Oct 8, 2009 11:35:10 AM
  - Last Changed By:** kathys
  - Comments:** A text box.
- Buttons:** 'Save', 'Previous', 'Next', and 'Cancel' at the bottom.

At the bottom of the window, it says 'Create New Principal- \*CHANGES\*'.

### Exemple 23–5 Création d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `add_principal` de `kadmin` est utilisée pour créer un principal appelé `pak`. La stratégie du principal est définie sur `testuser`.

```
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": <Type the password>
Re-enter password for principal "pak@EXAMPLE.COM": <Type the password again>
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```



## ▼ Procédure de duplication d'un principal Kerberos

Cette procédure explique comment utiliser tout ou partie des attributs d'un principal existant pour en créer un nouveau. Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Principals (Principaux).

### 3 Sélectionnez le principal dans la liste que vous souhaitez dupliquer, puis cliquez sur Duplicate (Dupliquer).

Le panneau Principal Basics (Informations de base du principal) s'affiche. Tous les attributs du principal sélectionné sont dupliqués, sauf les champs de nom et de mot de passe, qui sont vides.

### 4 Indiquez un nom de principal et un mot de passe.

Les deux sont obligatoires. Pour effectuer une copie exacte du principal que vous avez sélectionné, cliquez sur Save et passez à l'[Étape 7](#).

### 5 Spécifiez des valeurs différentes pour les attributs du principal et continuez d'appuyer sur Next (Suivant) pour en spécifier d'autres.

Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section [“Descriptions des panneaux de l'outil SEAM” à la page 503](#).

### 6 Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.

### 7 Si nécessaire, configurez les privilèges d'administration de Kerberos pour le principal dans le fichier `/etc/krb5/kadm5.acl`.

Pour plus d'informations, reportez-vous à la section [“Procédure de modification des privilèges d'administration Kerberos” à la page 493](#).

## ▼ Procédure de modification d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

**1 Si nécessaire, démarrez l'outil SEAM.**

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

**2 Cliquez sur l'onglet Principals (Principaux).**

**3 Sélectionnez le principal dans la liste que vous souhaitez modifier, puis cliquez sur Modify (Modifier).**

Le panneau Principal Basics (Informations de base du principal) contenant certains attributs du principal s'affiche.

**4 Modifiez les attributs du principal et continuez d'appuyer sur Next pour en modifier d'autres.**

Trois fenêtres contiennent les informations sur les attributs. Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre. Ou, pour toutes les descriptions d'attributs de principaux, reportez-vous à la section [“Descriptions des panneaux de l'outil SEAM” à la page 503](#).

---

**Remarque** – Vous ne pouvez pas modifier le nom d'un principal. Pour renommer un principal, vous devez le dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancien principal.

---

**5 Cliquez sur Save (Enregistrer) pour enregistrer le principal ou cliquez sur Done (Terminé) dans le dernier panneau.**

**6 Modifiez les privilèges d'administration Kerberos pour le principal dans le fichier /etc/krb5/kadm5.acl.**

Pour plus d'informations, reportez-vous à la section [“Procédure de modification des privilèges d'administration Kerberos” à la page 493](#).

### **Exemple 23–6** Modification du mot de passe d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `change_password` de `kadmin` est utilisée pour modifier le mot de passe du principal `jdb`. La commande `change_password` ne vous permet pas de réutiliser un mot de passe qui se trouve dans l'historique des mots de passe du principal.

```
kadmin: change_password jdb
Enter password for principal "jdb": <Type the new password>
Re-enter password for principal "jdb": <Type the password again>
```

```
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Pour modifier d'autres attributs d'un principal, vous devez utiliser la commande `modify_principal` de `kadmin`.

## ▼ Procédure de suppression d'un principal Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Principals (Principaux).

### 3 Sélectionnez le principal dans la liste que vous souhaitez supprimer, puis cliquez sur Delete.

Après avoir confirmé la suppression, le principal est supprimé.

### 4 Supprimez le principal du fichier de liste de contrôle d'accès (ACL) de Kerberos, `/etc/krb5/kadm5.acl`.

Pour plus d'informations, reportez-vous à la section [“Procédure de modification des privilèges d'administration Kerberos” à la page 493](#).

## Exemple 23–7 Suppression d'un principal Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `delete_principal` de `kadmin` est utilisée pour supprimer le principal `jdb`.

```
kadmin: delete_principal pak
Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): yes
Principal "pak@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
kadmin: quit
```

## ▼ Procédure de paramétrage des valeurs par défaut pour la création de principaux Kerberos

Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

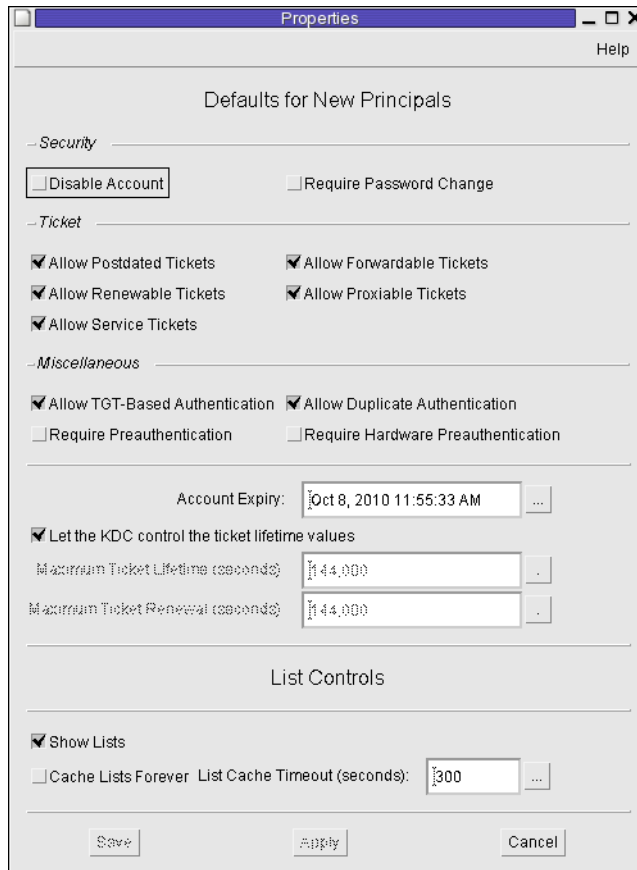
### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section “[Procédure de démarrage de l'outil SEAM](#)” à la page 479.

```
$ /usr/sbin/gkadmin
```

### 2 Choisissez Properties (Propriétés) dans le menu Edit (Editer).

La fenêtre Properties s'affiche.



3    **Sélectionnez les valeurs par défaut que vous souhaitez utiliser lorsque vous créez des principaux.**

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans chaque fenêtre.

4    **Cliquez sur Enregistrer.**

▼    **Procédure de modification des privilèges d'administration Kerberos**

Même si votre site dispose probablement de nombreux principaux d'utilisateurs, en général, vous souhaitez que seul un petit nombre d'utilisateurs soit capable d'administrer la base de données Kerberos. Les privilèges d'administration de la base de données Kerberos sont déterminés par le fichier ACL de Kerberos, `kadm5.ac1`. Le fichier `kadm5.ac1` vous permet d'autoriser ou d'interdire l'ajout de privilèges aux principaux individuels. Ou bien, vous pouvez utiliser le caractère générique "\*" dans le nom du principal pour spécifier les privilèges pour les groupes de principaux.

1    **Connectez-vous en tant que superutilisateur au KDC maître.**

2    **Modifiez le fichier `/etc/krb5/kadm5.ac1`.**

Une entrée dans le fichier `kadm5.ac1` doit avoir le format suivant :

*principal privileges [principal-target]*

*principal*

Spécifie le principal auquel les privilèges sont accordés. N'importe quelle partie du nom du principal peut inclure le caractère générique "\*", ce qui est utile pour fournir les mêmes privilèges pour un groupe de principaux. Par exemple, si vous voulez spécifier tous les principaux avec l'instance `admin`, vous devez utiliser `*/admin@realm`.

Notez qu'une utilisation commune d'une instance `admin` consiste à accorder des privilèges séparés (tels que l'accès à l'administration de la base de données Kerberos) à un principal Kerberos. Par exemple, l'utilisateur `jdb` peut avoir un principal pour son utilisation administrative, appelé `jdb/admin`. De cette façon, l'utilisateur `jdb` obtient uniquement les tickets de `jdb/admin` lorsqu'il a réellement besoin d'utiliser ces privilèges.

*privileges*

Spécifie les opérations qui peuvent être effectuées ou non par le principal. Ce champ est constitué d'une chaîne de caractères de la liste suivante de caractères ou de leur équivalent majuscule. Si le caractère est majuscule (ou non spécifié), alors l'opération n'est pas autorisée. Si le caractère est minuscule, l'opération est autorisée.

- |   |                                                                     |
|---|---------------------------------------------------------------------|
| a | Autorise ou interdit l'ajout de principaux ou de stratégies.        |
| d | Autorise ou interdit la suppression de principaux ou de stratégies. |

|        |                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------|
| m      | Autorise ou interdit la modification de principaux ou de stratégies.                            |
| c      | Autorise ou interdit la modification des mots de passe des principaux.                          |
| i      | Autorise ou interdit la consultation de la base de données Kerberos.                            |
| l      | Autorise ou interdit les liste de principaux ou de stratégies dans la base de données Kerberos. |
| x ou * | Autorise tous les privilèges (admcil).                                                          |

*principal-target* Lorsqu'un principal est indiqué dans ce champ, les *privilèges* s'appliquent uniquement au *principal* lorsque le *principal* fonctionne sur la *principal-target* (cible du principal). N'importe quelle partie du nom du principal peut inclure le caractère générique "\*", ce qui est utile pour un groupe de principaux.

**Exemple 23–8**    Modification des privilèges d'administration de Kerberos

L'entrée suivante dans le fichier `kadm5.ac` accorde à tout principal dans le domaine `EXAMPLE.COM` avec l'instance `admin` tous les privilèges de la base de données Kerberos :

```
*/admin@EXAMPLE.COM *
```

L'entrée suivante dans le fichier `kadm5.ac` donne au principal `jdb@example.com` les privilèges d'ajouter, de répertorier et de consulter tous les principaux qui ont l'instance `root`.

```
jdb@EXAMPLE.COM ali */root@EXAMPLE.COM
```

# Administration des stratégies Kerberos

Cette section fournit les instructions détaillées permettant d'administrer les stratégies à l'aide de l'outil SEAM. Elle fournit également des exemples d'équivalents de lignes de commande, le cas échéant.

## Administration des stratégies Kerberos (liste des tâches)

| Tâche                                    | Description                                                                                                                                | Voir                                                                                         |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Affichage de la liste des stratégies.    | Affichez la liste des stratégies en cliquant sur l'onglet Politiques (Stratégies).                                                         | <a href="#">“Procédure d'affichage de la liste des stratégies Kerberos” à la page 495</a>    |
| Affichage des attributs d'une stratégie. | Affichez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier). | <a href="#">“Procédure d'affichage des attributs d'une stratégie Kerberos” à la page 497</a> |

| Tâche                         | Description                                                                                                                                                                                                                                                                                                                                | Voir                                                                               |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Création d'une stratégie.     | Créez une stratégie en cliquant sur le bouton Create New (Créer) dans le panneau Policy List (Liste de stratégies).                                                                                                                                                                                                                        | <a href="#">“Procédure de création d'une stratégie Kerberos” à la page 499</a>     |
| Duplication d'une stratégie.  | Dupliquez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Duplicate (Dupliquer).                                                                                                                                                                                            | <a href="#">“Procédure de duplication d'une stratégie Kerberos” à la page 501</a>  |
| Modification d'une stratégie. | Modifiez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Modify (Modifier).<br><br>Notez que vous ne pouvez pas modifier le nom d'une stratégie. Pour renommer une stratégie, vous devez la dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancienne. | <a href="#">“Procédure de modification d'une stratégie Kerberos” à la page 501</a> |
| Suppression d'une stratégie.  | Supprimez les attributs d'une stratégie en la sélectionnant dans la liste correspondante, puis en cliquant sur le bouton Delete (Supprimer).                                                                                                                                                                                               | <a href="#">“Procédure de suppression d'une stratégie Kerberos” à la page 502</a>  |

## ▼ Procédure d'affichage de la liste des stratégies Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

## 2 Cliquez sur l'onglet Policies (Stratégies).

La liste des stratégies s'affiche.



## 3 Affichez une stratégie spécifique ou une sous-liste de stratégies.

Saisissez une chaîne de filtrage dans le champ correspondant, puis appuyez sur la touche Entrée. Si le filtre fonctionne, la liste de stratégies qui lui correspond s'affiche.

La chaîne du filtre doit être composée d'un ou plusieurs caractères. Notez bien que le mécanisme de filtrage respecte la casse et qu'il vous faut utiliser les majuscules et minuscules appropriées. Par exemple, si vous entrez la chaîne ge, le mécanisme de filtrage affiche uniquement les stratégies contenant la chaîne ge (george ou edge par exemple).



Si vous souhaitez afficher l'intégralité de la liste de stratégies, cliquez sur Clear Filter (Supprimer le filtre).

### Exemple 23–9 Affichage de la liste de stratégies Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `list_policies` de `kadmin` est utilisée pour obtenir la liste de toutes les stratégies correspondant à `*user*`. Les caractères génériques peuvent être utilisés avec la commande `list_policies`.

```
kadmin: list_policies *user*
testuser
enguser
kadmin: quit
```

## ▼ Procédure d'affichage des attributs d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Policies (Stratégies).

### 3 Sélectionnez la stratégie dans la liste que vous souhaitez afficher, puis cliquez sur Modify (Modifier).

Le panneau Policy Details (Détails de la stratégie) s'affiche.

### 4 Lorsque vous avez fini de consulter ces informations, cliquez sur Cancel (Annuler).

### Exemple 23–10 Affichage des attributs d'une stratégie Kerberos

L'exemple suivant montre le panneau Policy Details (Détails de la stratégie) lorsque vous visualisez la stratégie `test`.



### Exemple 23-11 Affichage des attributs d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `get_policy` de `kadmin` est utilisée pour afficher les attributs de la stratégie `enguser`.

```
kadmin: get_policy enguser
Policy: enguser
Maximum password life: 2592000
Minimum password life: 0
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 0
kadmin: quit
```

Le nombre de références est le nombre de principaux qui utilisent cette stratégie.

## ▼ Procédure de création d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

**1 Si nécessaire, démarrez l'outil SEAM.**

Pour plus d'informations, reportez-vous à la section “Procédure de démarrage de l'outil SEAM” à la page 479.

```
$ /usr/sbin/gkadmin
```

**2 Cliquez sur l'onglet Politiques (Stratégies).**

**3 Cliquez sur New (Nouveau).**

Le panneau Policy Details (Détails de la stratégie) s'affiche.

**4 Spécifiez un nom pour la stratégie dans le champ correspondant.**

Le nom de stratégie est obligatoire.

**5 Spécifiez les valeurs des attributs de la stratégie.**

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au [Tableau 23-5](#) pour toutes les descriptions des attributs de stratégies.

**6 Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).**

### Exemple 23-12 Création d'une stratégie Kerberos

Dans l'exemple suivant, une stratégie appelée `build11` est créée. Les classes de mot de passe minimales sont définies sur 3.



### Exemple 23–13 Création d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `add_policy` de `kadmin` est utilisée pour créer la stratégie `build11`. Cette stratégie requiert au moins trois classes de caractères dans le mot de passe.

```
$ kadmin
kadmin: add_policy -minclasses 3 build11
kadmin: quit
```

## ▼ Procédure de duplication d'une stratégie Kerberos

Cette procédure explique comment utiliser tout ou partie des attributs d'une stratégie existante pour créer une nouvelle stratégie. Il n'existe pas d'équivalent de ligne de commande pour cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Politiques (Stratégies).

### 3 Sélectionnez la stratégie dans la liste que vous souhaitez dupliquer, puis cliquez sur Duplicate (Dupliquer).

Le panneau Policy Details (Détails de la stratégie) s'affiche. Tous les attributs de la stratégie sélectionnée sont dupliqués, sauf le champ de nom, qui est vide.

### 4 Spécifiez un nom pour la stratégie dupliquée dans le champ correspondant.

Le nom de stratégie est obligatoire. Pour effectuer une copie exacte de la stratégie que vous avez sélectionnée, cliquez sur Save et passez à l'[Étape 6](#).

### 5 Spécifiez des valeurs différentes pour les attributs de la stratégie.

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au [Tableau 23–5](#) pour toutes les descriptions des attributs de stratégies.

### 6 Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).

## ▼ Procédure de modification d'une stratégie Kerberos

Un exemple d'équivalent de ligne de commande suit cette procédure.

### 1 Si nécessaire, démarrez l'outil SEAM.

Pour plus d'informations, reportez-vous à la section [“Procédure de démarrage de l'outil SEAM” à la page 479](#).

```
$ /usr/sbin/gkadmin
```

### 2 Cliquez sur l'onglet Politiques (Stratégies).

- 3 **Sélectionnez la stratégie dans la liste que vous souhaitez modifier, puis cliquez sur Modify (Modifier).**

Le panneau Policy Details (Détails de la stratégie) s'affiche.

- 4 **Modifiez les attributs de la stratégie.**

Choisissez l'aide contextuelle dans le menu d'aide pour obtenir plus d'informations sur les divers attributs dans cette fenêtre. Ou reportez-vous au [Tableau 23–5](#) pour toutes les descriptions des attributs de stratégies.

---

**Remarque** – Vous ne pouvez pas modifier le nom d'une stratégie. Pour renommer une stratégie, vous devez la dupliquer, lui donner un nouveau nom, l'enregistrer, puis supprimer l'ancienne.

---

- 5 **Cliquez sur Save (Enregistrer) pour enregistrer la stratégie ou cliquez sur Done (Terminé).**

#### **Exemple 23–14**    Modification d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `modify_policy` de `kadmin` est utilisée pour modifier la longueur minimale d'un mot de passe de cinq caractères pour la stratégie `build11`.

```
$ kadmin
kadmin: modify_policy -minlength 5 build11
kadmin: quit
```

## ▼ **Procédure de suppression d'une stratégie Kerberos**

Un exemple d'équivalent de ligne de commande suit cette procédure.

---

**Remarque** – Avant de supprimer une stratégie, vous devez annuler la stratégie à partir de tous les principaux qui l'utilisent actuellement. Pour ce faire, vous devez modifier les attributs de stratégie des principaux. La stratégie ne peut pas être supprimée si un principal l'utilise.

---

- 1 **Si nécessaire, démarrez l'outil SEAM.**

Pour plus d'informations, reportez-vous à la section "[Procédure de démarrage de l'outil SEAM](#)" à la page 479.

```
$ /usr/sbin/gkadmin
```

- 2 **Cliquez sur l'onglet Politiques (Stratégies).**

- 3 **Sélectionnez la stratégie dans la liste que vous voulez supprimer, puis cliquez sur Delete.**

Après avoir confirmé la suppression, la stratégie est supprimée.

### Exemple 23–15 Suppression d'une stratégie Kerberos (ligne de commande)

Dans l'exemple suivant, la commande `delete_policy` de `kadmin` est utilisée pour supprimer la stratégie `build11`.

```
kadmin: delete_policy build11
Are you sure you want to delete the policy "build11"? (yes/no): yes
kadmin: quit
```

Avant de supprimer une stratégie, vous devez annuler la stratégie à partir de tous les principaux qui l'utilisent actuellement. Pour ce faire, vous devez utiliser la commande `modify_principal -policy` de `kadmin` sur les principaux affectés. La commande `delete_policy` échoue si la stratégie est en cours d'utilisation par un principal.

## Référence de l'outil SEAM

Cette section fournit les descriptions de chaque panneau de l'outil SEAM. En outre, des d'informations sur l'utilisation de privilèges limités avec l'outil SEAM sont fournies.

### Descriptions des panneaux de l'outil SEAM

Cette section fournit des descriptions pour chaque attribut de principal et de stratégie que vous pouvez spécifier ou afficher dans outil SEAM. Les attributs sont organisés par le panneau dans lequel ils sont affichés.

TABLEAU 23–2 Attributs pour le panneau Principal Basics (Informations de base du principal) de l'outil SEAM

| Attribut                                                   | Description                                                                                                                                                                                                                                              |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principal Name (Nom du principal)                          | Nom du principal (qui est la partie <i>primary/instance</i> d'un nom complet de principal). Un principal est une identité unique à laquelle le KDC peut affecter les tickets.<br><br>Si vous modifiez un principal, vous ne pouvez pas modifier son nom. |
| Password (Mot de passe)                                    | Mot de passe du principal. Vous pouvez utiliser le bouton Generate Random Password (Générer un mot de passe aléatoire) pour créer un mot de passe aléatoire pour le principal.                                                                           |
| Policy (Stratégie)                                         | Menu des stratégies disponibles pour le principal.                                                                                                                                                                                                       |
| Account Expires (Expiration du compte)                     | Date et heure d'expiration du compte principal. Lorsque le compte expire, le principal ne peut plus obtenir un ticket d'octroi de tickets (TGT) et peut être incapable de se connecter.                                                                  |
| Last Principal Change (Dernière modification de principal) | Date à laquelle les informations du principal ont été modifiées pour la dernière fois. (Lecture seule)                                                                                                                                                   |
| Last Changed By (Dernière modification par)                | Nom du principal qui a modifié en dernier le compte de ce principal. (Lecture seule)                                                                                                                                                                     |
| Comments (Commentaires)                                    | Commentaires liés au principal (par exemple, "compte temporaire").                                                                                                                                                                                       |

TABLEAU 23-3 Attributs pour le panneau Principal Details (Détails du principal) de l'outil SEAM

| Attribut                                                         | Description                                                                                                                     |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Last Success (Dernier succès)                                    | Date et heure de la dernière connexion réussie du principal. (Lecture seule)                                                    |
| Last Failure (Dernier échec)                                     | Date et heure du dernier échec de connexion du principal. (Lecture seule)                                                       |
| Failure Count (Nombre d'échecs)                                  | Nombre de fois où une erreur de connexion s'est produite pour le principal. (Lecture seule)                                     |
| Last Password Change (Dernière modification du mot de passe)     | Date et heure auxquelles le mot de passe du principal a été modifié pour la dernière fois. (Lecture seule)                      |
| Password Expires (Date d'expiration du mot de passe)             | Date et heure auxquelles le mot de passe actuel du principal expire.                                                            |
| Key Version (Version de la clé)                                  | Numéro de version de la clé pour le principal. Cet attribut n'est généralement modifié que quand le mot de passe est compromis. |
| Maximum Lifetime (seconds) (Durée de vie maximale (en secondes)) | Durée maximale pour laquelle un ticket peut être accordé au principal (sans renouvellement).                                    |
| Maximum Renewal (seconds) (Renouvellement maximal (en secondes)) | Durée maximale pendant laquelle un ticket peut être renouvelé pour le principal.                                                |

TABLEAU 23-4 Attributs du panneau Principal Flags (Indicateurs de principal) de l'outil SEAM

| Attribut (boutons radio)                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable Account (Désactiver un compte)                           | Lorsqu'elle est sélectionnée, cette option empêche le principal de se connecter. Cet attribut fournit un moyen facile de figer temporairement un compte principal.                                                                                                                                                                                                                                                                                                                                 |
| Require Password Change (Exiger la modification du mot de passe) | Lorsque cette option est sélectionnée, l'option fait expirer le mot de passe en cours du principal, ce qui oblige l'utilisateur à utiliser la commande <code>kpasswd</code> pour créer un nouveau mot de passe. Cet attribut est utile si une violation de la sécurité se produit et que vous devez vous assurer que les anciens mots de passe sont remplacés.                                                                                                                                     |
| Allow Postdated Tickets (Autoriser les tickets postdatés)        | Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets postdatés.<br>Par exemple, vous pouvez avoir besoin d'utiliser des tickets postdatés pour les tâches de <code>cron</code> qui doivent s'exécuter après les heures de bureau, mais vous ne pouvez pas obtenir de tickets en avance en raison de courtes durées de vie de tickets.                                                                                                                              |
| Allow Forwardable Tickets (Autoriser les tickets transmissibles) | Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets transmissibles.<br>Les tickets transmissibles sont des tickets qui sont transmis à l'hôte distant pour fournir une session à connexion unique. Par exemple, si vous utilisez des tickets transmissibles et que vous vous authentifiez via <code>ftp</code> ou <code>rsh</code> , d'autres services, tels que les services NFS, sont disponibles sans que vous ne soyez invité à saisir un autre mot de passe. |



TABLEAU 23-4 Attributs du panneau Principal Flags (Indicateurs de principal) de l'outil SEAM (Suite)

| Attribut (boutons radio)                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow Renewable Tickets<br>(Autoriser les tickets renouvelables)                | Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets renouvelables.<br><br>Un principal peut étendre automatiquement la date d'expiration ou le temps qu'un ticket peut être renouvelable (plutôt que d'avoir à obtenir un nouveau ticket une fois que le premier ticket arrive à expiration). Actuellement, le service NFS est le service de ticket qui peut renouveler les tickets.                                                                                                                   |
| Allow Proxiable Tickets<br>(Autoriser les tickets utilisables avec proxy)       | Lorsqu'elle est sélectionnée, cette option permet au principal d'obtenir des tickets utilisables avec proxy.<br><br>Un ticket utilisable avec proxy est un ticket qui peut être utilisé par un service pour le compte d'un client afin d'effectuer une opération pour ce dernier. Avec un ticket utilisable avec proxy, un service peut prendre l'identité d'un client et obtenir un ticket pour un autre service. Toutefois, le service ne peut pas obtenir de ticket d'octroi de tickets (TGT).                                       |
| Allow Service Tickets (Autoriser les tickets de service)                        | Lorsqu'elle est sélectionnée, cette option permet aux tickets de service d'être émis pour le principal.<br><br>Vous ne devez pas autoriser les tickets de service à être émis pour les principaux <code>kadmin/hostname</code> et <code>changepw/hostname</code> . Cette pratique permet de s'assurer que seuls ces principaux peuvent mettre à jour la base de données KDC.                                                                                                                                                            |
| Allow TGT-Based Authentication<br>(Autoriser l'authentification par TGT)        | Lorsque cette option est sélectionnée, le principal de service est autorisé à fournir des services à un autre principal. Plus précisément, cet attribut autorise le KDC à émettre un ticket de service pour le service principal.<br><br>Cet attribut est uniquement valable pour les principaux de service. Lorsque ce bouton n'est pas coché, les tickets de service ne peuvent pas être émis pour le principal de service.                                                                                                           |
| Allow Duplicate Authentication<br>(Autoriser la duplication d'authentification) | Lorsqu'elle est sélectionnée, cette option autorise le principal d'utilisateur à obtenir des tickets de service pour d'autres principaux d'utilisateur.<br><br>Cet attribut est uniquement valide pour les principaux d'utilisateur. Si cette option n'est pas sélectionnée, le principal d'utilisateur peut toujours obtenir des tickets de service pour les principaux de service, mais pas pour d'autres principaux d'utilisateur.                                                                                                   |
| Required Preauthentication<br>(Pré-authentification requise)                    | Lorsque cette option est sélectionnée, le KDC n'envoie pas le ticket d'octroi de tickets (TGT) demandé au principal jusqu'à ce que le KDC puisse authentifier (par le biais d'un logiciel) que le principal est bien celui qui demande le ticket. Cette pré-authentification est généralement effectuée par le biais d'un mot de passe supplémentaire, par exemple, à partir d'une carte DES.<br><br>Si elle n'est pas sélectionnée, le KDC n'a pas besoin de pré-authentifier le principal avant que le KDC lui envoie un TGT demandé. |
| Required Hardware Authentication (Authentification matérielle requise)          | Lorsque cette option est sélectionnée, le KDC n'envoie pas le ticket d'octroi de tickets (TGT) demandé au principal jusqu'à ce que le KDC puisse authentifier (par le biais d'un matériel) que le principal est bien celui qui demande le ticket. La pré-authentification matérielle peut se produire, par exemple, sur un lecteur d'anneau Java.<br><br>Si elle n'est pas sélectionnée, le KDC n'a pas besoin de pré-authentifier le principal avant que le KDC lui envoie un TGT demandé.                                             |

TABLEAU 23-5 Attributs pour le panneau Policy Basics de l'outil SEAM

| Attribut                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Name (Nom de la stratégie)                                                         | Nom de la stratégie. Une stratégie est un ensemble de règles qui régissent le mot de passe et les tickets d'un principal.<br><br>Si vous modifiez une stratégie, vous ne pouvez pas modifier son nom.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Minimum Password Length (Longueur minimale de mot de passe)                               | Longueur minimale du mot de passe du principal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Minimum Password Classes (Nombre minimal de classes de mot de passe)                      | Nombre minimal de types de caractères différents qui sont requis dans le mot de passe du principal.<br><br>Par exemple, une valeur de classes minimales de 2 signifie que le mot de passe doit comporter au moins deux types de caractères différents, tels que des lettres et des chiffres (hi2mom). Une valeur de 3 signifie que le mot de passe doit comporter au moins trois types de caractères différents, comme des lettres, des chiffres et des signes de ponctuation (hi2mom!). Et ainsi de suite...<br><br>Une valeur de 1 définit signifie l'absence de restriction sur le nombre de types de caractères de mot de passe. |
| Saved Password History (Historique de mots de passe enregistrés)                          | Nombre de mots de passe précédents qui ont été utilisés par le principal et liste des mots de passe précédents ne pouvant plus être utilisés.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Minimum Password Lifetime (seconds) (Durée de vie minimale du mot de passe (en secondes)) | Période minimale pendant laquelle le mot de passe doit être utilisé avant de pouvoir être changé.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Maximum Password Lifetime (seconds) (Durée de vie maximale du mot de passe (en secondes)) | Période maximale pendant laquelle le mot de passe peut être utilisé avant de devoir être changé.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Principals Using This Policy (Principaux utilisant cette stratégie)                       | Nombre de principaux auquel cette stratégie s'applique actuellement. (Lecture seule)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Utilisation de l'outil SEAM avec privilèges d'administration Kerberos limités

Toutes les capacités de SEAM Tool sont disponibles si votre principal admin dispose de tous les privilèges d'administration de la base de données Kerberos. Cependant, il se peut que vous ayez des privilèges limités, tels qu'être seulement autorisé à consulter la liste des principaux ou à modifier le mot de passe d'un principal. Avec des privilèges d'administration Kerberos limités, vous pouvez toujours utiliser l'outil SEAM. Cependant, diverses parties de l'outil SEAM

changent en fonction des privilèges d'administration Kerberos dont vous ne disposez pas. Le [Tableau 23–6](#) montre comment l'outil SEAM change en fonction de vos privilèges d'administration Kerberos.

Le changement le plus visible de l'outil SEAM se produit lorsque vous ne disposez pas du privilège de liste. Sans le privilège de liste, les panneaux de listes n'affichent pas la liste des principaux et les stratégies à manipuler. Au lieu de cela, vous devez utiliser le champ de nom dans les panneaux de listes pour spécifier un principal ou une stratégie que vous voulez manipuler.

Si vous vous connectez à l'outil SEAM et que vous ne disposez pas de privilèges suffisants pour effectuer des tâches avec lui, le message suivant s'affiche et vous êtes renvoyé à la fenêtre de connexion d'administration SEAM :

Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal.

Pour modifier les privilèges d'un principal afin qu'il puisse administrer la base de données Kerberos, reportez-vous à la section [“Procédure de modification des privilèges d'administration Kerberos” à la page 493](#).

**TABLEAU 23–6** Utilisation de l'outil SEAM avec des privilèges d'administration Kerberos limités

| Privilège non autorisé       | Changements de l'outil SEAM                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a (ajouter)                  | Les boutons Create New (Créer) et Duplicate (Dupliquer) ne sont pas disponibles dans les panneaux Principal List (Liste de principaux) et Policy List (Liste de stratégies). Sans le privilège d'ajout, vous ne pouvez pas créer de principaux ou de stratégies, ni les dupliquer.                                                                                                                                                                |
| d (supprimer)                | Le bouton Delete (Supprimer) n'est pas disponible dans les panneaux Principal List et Policy List. Sans le privilège de suppression, vous ne pouvez pas supprimer de principaux ou de stratégies.                                                                                                                                                                                                                                                 |
| m (modifier)                 | Le bouton Modify (Modifier) n'est pas disponible dans les panneaux Principal List et Policy List. Sans le privilège de modification, vous ne pouvez pas modifier de principaux ou de stratégies.<br><br>En outre, avec le bouton Modify non disponible, vous ne pouvez pas modifier le mot de passe d'un principal, même si vous avez le privilège de modification de mot de passe.                                                               |
| c (modifier un mot de passe) | Le champ Password (Mot de passe) du panneau Principal Basics (Informations de base du principal) est en lecture seule et ne peut pas être modifié. Sans le privilège de changement de mot de passe, vous ne pouvez pas modifier le mot de passe d'un principal.<br><br>Notez que même si vous avez le privilège changement de mot de passe, vous devez également avoir le privilège de modification pour modifier le mot de passe d'un principal. |

**TABLEAU 23-6** Utilisation de l'outil SEAM avec des privilèges d'administration Kerberos limités (Suite)

| Privilège non autorisé              | Changements de l'outil SEAM                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| i (consultation de base de données) | Les boutons Modify et Duplicate ne sont pas disponibles dans les panneaux Principal List et Policy List. Sans le privilège de consultation, vous ne pouvez pas modifier ou dupliquer de principaux ou de stratégies.<br><br>En outre, avec le bouton Modify non disponible, vous ne pouvez pas modifier le mot de passe d'un principal, même si vous avez le privilège de modification de mot de passe. |
| l (liste)                           | La liste des principaux et des stratégies dans les panneaux de liste est indisponible. Au lieu de cela, vous devez utiliser le champ de nom dans les panneaux de listes pour spécifier un principal ou une stratégie que vous voulez manipuler.                                                                                                                                                         |

## Administration des fichiers keytab

Tous les hôtes qui fournissent un service doivent disposer d'un fichier local, appelé un *keytab* (abréviation de “key table” (table des clés). Le fichier keytab contient le principal pour le service approprié, appelé *clé de service*. Une clé de service est utilisée par un service pour s'authentifier auprès du KDC et est uniquement connue de Kerberos et du service lui-même. Par exemple, si vous avez un serveur NFS utilisant Kerberos, le serveur doit avoir un fichier keytab qui contient son principal de service `nfs`.

Pour ajouter une clé de service à un fichier keytab, vous ajoutez le principal de service approprié à un fichier keytab de l'hôte à l'aide de la commande `ktadd` de `kadmin`. Comme vous êtes en train d'ajouter un principal de service à un fichier keytab, le principal doit exister dans la base de données Kerberos afin que `kadmin` puisse vérifier son existence. Sur les serveurs d'applications qui fournissent des services utilisant Kerberos, le fichier keytab est situé à `/etc/krb5/krb5.keytab`, par défaut.

Un fichier keytab est comparable à un mot de passe d'utilisateur. Tout comme il est important pour les utilisateurs de protéger leurs mots de passe, il est tout aussi important pour les serveurs d'applications de protéger leurs fichiers keytab. Vous devez toujours stocker les fichiers keytab sur un disque local et les rendre lisibles uniquement par l'utilisateur `root`. En outre, vous ne devez jamais envoyer un fichier keytab par le biais d'un réseau non sécurisé.

Il existe également une instance spéciale dans laquelle ajouter un principal `root` au fichier keytab d'un hôte. Si vous souhaitez qu'un utilisateur sur le client Kerberos monte des systèmes de fichiers NFS utilisant Kerberos, qui nécessitent un accès équivalent au `root`, vous devez ajouter le principal `root` du client à son fichier keytab. Dans le cas contraire, les utilisateurs doivent utiliser la commande `kinit` en tant que `root` pour obtenir des informations d'identification pour le principal `root` du client lorsqu'ils souhaitent monter un système de fichiers NFS utilisant Kerberos avec accès `root`, même lorsqu'ils utilisent l'agent de montage automatique.

Une autre commande que vous pouvez utiliser pour administrer les fichiers keytab est la commande `ktutil`. Cette commande interactive vous permet de gérer le fichier keytab d'un hôte local sans disposer de privilèges d'administration Kerberos, car `ktutil` n'interagit pas avec la base de données Kerberos comme le fait `kadmin`. Par conséquent, après l'ajout d'un principal à un fichier keytab, vous pouvez utiliser `ktutil` pour visualiser la liste de clés dans le fichier keytab ou pour désactiver temporairement l'authentification d'un service.

**Remarque** – Lorsque vous modifiez un principal dans un fichier keytab à l'aide de la commande `ktadd` dans `kadmin`, une nouvelle clé est générée et ajoutée au fichier keytab.

## Administration des fichiers keytab (liste des tâches)

| Tâche                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                | Voir                                                                                                                 |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Ajout d'un principal de service à un fichier keytab                         | Utilisez la commande <code>ktadd</code> de <code>kadmin</code> pour ajouter un principal de service dans un fichier keytab.                                                                                                                                                                                                                                                                                                                                | <a href="#">“Procédure d'ajout d'un principal de service Kerberos à un fichier keytab” à la page 509</a>             |
| Suppression d'un principal de service d'un fichier keytab                   | Utilisez la commande <code>ktremove</code> de <code>kadmin</code> pour supprimer un principal de service d'un fichier keytab.                                                                                                                                                                                                                                                                                                                              | <a href="#">“Procédure de suppression d'un principal de service d'un fichier keytab” à la page 511</a>               |
| Affichage de la liste de clés (liste des principaux) dans un fichier keytab | Utilisez la commande <code>ktutil</code> pour afficher la liste de clés dans un fichier keytab.                                                                                                                                                                                                                                                                                                                                                            | <a href="#">“Procédure d'affichage de la liste de clés (principaux) dans un fichier keytab” à la page 512</a>        |
| Désactivation temporaire de l'authentification d'un service sur un hôte     | <p>Cette procédure est un moyen rapide de désactiver temporairement l'authentification d'un service sur un hôte sans disposer des privilèges <code>kadmin</code>.</p> <p>Avant d'utiliser <code>ktutil</code> pour supprimer le principal de service du fichier keytab du serveur, copiez le fichier keytab d'origine vers un emplacement temporaire. Au moment de réactiver le service, copiez le fichier keytab d'origine à son emplacement correct.</p> | <a href="#">“Procédure de désactivation temporaire de l'authentification d'un service sur un hôte” à la page 512</a> |

### ▼ Procédure d'ajout d'un principal de service Kerberos à un fichier keytab

- 1 Assurez-vous que le principal existe déjà dans la base de données Kerberos.  
Pour plus d'informations, reportez-vous à la section [“Procédure d'affichage de la liste des principaux Kerberos” à la page 482](#).

- 2 Connectez-vous en tant que superutilisateur à l'hôte qui a besoin qu'un principal soit ajouté à son fichier keytab.

- 3 Démarrez la commande `kadmin`.

```
# /usr/sbin/kadmin
```

- 4 Ajoutez un principal à un fichier keytab en utilisant la commande `ktadd`.

```
kadmin: ktadd [-e enctype] [-k keytab] [-q] [principal | -glob principal-exp]
```

`-e enctype` Remplace la liste des types de chiffrement définie dans le fichier `krb5.conf`.

`-k keytab` Spécifie le fichier keytab. Par défaut, `/etc/krb5/krb5.keytab` est utilisé.

`-q` Affiche des informations moins détaillées.

`principal` Spécifie le principal à ajouter au fichier keytab. Vous pouvez ajouter les principaux de service suivants : `host`, `root`, `nfs` et `ftp`.

`-glob principal-exp` Spécifie les expressions de principal. Tous les principaux qui correspondent à `principal-exp` sont ajoutés au fichier keytab. Les règles qui régissent l'expression de principal sont les mêmes que pour la commande `list_principals` de `kadmin`.

- 5 Quittez la commande `kadmin`.

```
kadmin: quit
```

### Exemple 23-16 Ajout d'un principal de service dans un fichier keytab

Dans l'exemple suivant, le principal d'`host` de `denver` est ajouté au fichier keytab de `denver`, de manière à ce que le KDC puisse authentifier les services de réseau de `denver`.

```
denver # /usr/sbin/kadmin
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS
mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc mode
with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## ▼ Procédure de suppression d'un principal de service d'un fichier keytab

- 1 Connectez-vous en tant que superutilisateur sur l'hôte avec un principal de service qui doit être supprimé de son fichier keytab.

- 2 Démarrez la commande `kadmin`.

```
# /usr/sbin/kadmin
```

- 3 (Facultatif) Pour afficher la liste actuelle des principaux (clés) dans le fichier keytab, utilisez la commande `ktutil`.

Pour obtenir des instructions détaillées, reportez-vous à la section “[Procédure d'affichage de la liste de clés \(principaux\) dans un fichier keytab](#)” à la page 512.

- 4 Supprimez une identité du fichier keytab à l'aide de la commande `ktremove`.

```
kadmin: ktremove [-k keytab] [-q] principal [kvno | all | old ]
```

`-k keytab` Spécifie le fichier keytab. Par défaut, `/etc/krb5/krb5.keytab` est utilisé.

`-q` Affiche des informations moins détaillées.

`principal` Spécifie le principal à supprimer du fichier keytab.

`kvno` Supprime toutes les entrées pour le principal spécifié dont le numéro de version de clé correspond à `kvno`.

`all` Supprime toutes les entrées pour le principal spécifié.

`old` Supprime toutes les entrées pour le principal spécifié, à l'exception des principaux avec les numéros de version de clé les plus élevés.

- 5 Quittez la commande `kadmin`.

```
kadmin: quit
```

### Exemple 23–17 Suppression d'un principal de service d'un fichier keytab.

Dans l'exemple suivant, le principal d'host de denver est supprimé du fichier keytab de denver.

```
denver # /usr/sbin/kadmin
kadmin: ktremove host/denver.example.com@EXAMPLE.COM
kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3
        removed from keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## ▼ Procédure d'affichage de la liste de clés (principaux) dans un fichier keytab

- 1 Connectez-vous en tant que superutilisateur sur l'hôte avec le fichier keytab.

---

**Remarque** – Bien qu'il soit possible de créer des fichiers keytab détenus par d'autres utilisateurs, l'utilisation de l'emplacement par défaut pour le fichier keytab requiert la propriété root.

---

- 2 Démarrez la commande `ktutil`.

```
# /usr/bin/ktutil
```

- 3 Lisez le fichier keytab dans le tampon de la liste de clés à l'aide de la commande `read_kt`.

```
ktutil: read_kt keytab
```

- 4 Affichez le tampon de la liste de clés en utilisant la commande `list`.

```
ktutil: list
```

Le tampon de la liste de clés actuel s'affiche.

- 5 Quittez la commande `ktutil`.

```
ktutil: quit
```

### Exemple 23–18 Affichage de la liste de clés (principaux) dans un fichier keytab

L'exemple suivant affiche la liste de clés dans le fichier `/etc/krb5/krb5.keytab` sur l'hôte `denver` hôte.

```
denver # /usr/bin/ktutil
ktutil: read_kt /etc/krb5/krb5.keytab
ktutil: list
slot KVNO Principal
-----
1      5 host/denver@EXAMPLE.COM
ktutil: quit
```

## ▼ Procédure de désactivation temporaire de l'authentification d'un service sur un hôte

Parfois, il peut s'avérer nécessaire de désactiver temporairement le mécanisme d'authentification d'un service, tel que `rlogin` ou `ftp`, sur un serveur d'applications réseau. Par exemple, si vous le souhaitez, vous pouvez empêcher les utilisateurs de se connecter à un système pendant que vous êtes en train d'effectuer des procédures de maintenance. La



commande `ktutil` permet d'accomplir cette tâche en supprimant le principal de service à partir du fichier keytab du serveur, sans nécessiter de privilèges `kadmin`. Pour réactiver l'authentification, il vous suffit de copier le fichier keytab d'origine que vous avez enregistré jusqu'à son emplacement d'origine.

---

**Remarque** – Par défaut, la plupart des services sont configurés de façon à exiger l'authentification. Si un service n'est pas configuré pour demander l'authentification, le service fonctionne toujours, même si vous désactivez l'authentification pour le service.

---

**1 Connectez-vous en tant que superutilisateur sur l'hôte avec le fichier keytab.**

---

**Remarque** – Bien qu'il soit possible de créer des fichiers keytab détenus par d'autres utilisateurs, l'utilisation de l'emplacement par défaut pour le fichier keytab requiert la propriété `root`.

---

**2 Enregistrez le fichier keytab actuel dans un fichier temporaire.**

**3 Démarrez la commande `ktutil`.**

```
# /usr/bin/ktutil
```

**4 Lisez le fichier keytab dans le tampon de la liste de clés à l'aide de la commande `read_kt`.**

```
ktutil: read_kt keytab
```

**5 Affichez le tampon de la liste de clés en utilisant la commande `list`.**

```
ktutil: list
```

Le tampon de la liste de clés actuel s'affiche. Notez le numéro d'emplacement du service que vous voulez désactiver.

**6 Pour désactiver temporairement un service d'hôte, supprimez le principal de service du tampon de la liste de clés à l'aide de la commande `delete_entry`.**

```
ktutil: delete_entry slot-number
```

Où *slot-number* indique le numéro d'emplacement du principal de service à supprimer, ce qui est affiché par la commande `list`.

**7 Ecrivez le tampon de la liste de clés sur un nouveau fichier keytab à l'aide de la commande `write_kt`.**

```
ktutil: write_kt new-keytab
```

**8 Quittez la commande `ktutil`.**

```
ktutil: quit
```

**9 Déplacez le nouveau fichier keytab.**

```
# mv new-keytab keytab
```

**10 Lorsque vous souhaitez réactiver le service, copiez le fichier keytab temporaire (d'origine) vers son emplacement d'origine.****Exemple 23–19 Désactivation temporaire d'un service sur un hôte**

Dans l'exemple suivant, le service host sur l'hôte denver est temporairement désactivé. Pour réactiver le service d'hôte sur denver, vous devez copier le fichier `krb5.keytab.temp` vers le fichier `/etc/krb5/krb5.keytab`.

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp
denver # /usr/bin/ktutil
      ktutil:read_kt /etc/krb5/krb5.keytab
      ktutil:list
slot KVNO Principal
-----
1      8 root/denver@EXAMPLE.COM
2      5 host/denver@EXAMPLE.COM
      ktutil:delete_entry 2
      ktutil:list
slot KVNO Principal
-----
1      8 root/denver@EXAMPLE.COM
      ktutil:write_kt /etc/krb5/new.krb5.keytab
      ktutil:quit
denver # cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab
```

## Utilisation des applications Kerberos (tâches)

---

Ce chapitre est destiné à tout utilisateur d'un système sur lequel le service Kerberos est configuré. Ce chapitre explique comment utiliser les commandes utilisant Kerberos et les services qui sont fournis. Vous devez être déjà familiarisé avec ces commandes (dans leurs versions n'incluant pas l'utilisation de Kerberos) avant de lire les descriptions ci-après.

Etant donné que ce chapitre est destiné à l'utilisateur standard, il inclut des informations sur les tickets : obtention, affichage et destruction. Ce chapitre inclut également des informations sur la sélection ou la modification d'un mot de passe Kerberos.

Les informations contenues dans ce chapitre sont répertoriées ci-après :

- “Gestion des tickets Kerberos” à la page 515
- “Gestion des mots de passe Kerberos” à la page 519
- “Commandes utilisateur Kerberos” à la page 524

Pour une présentation du produit Kerberos Oracle Solaris, reportez-vous au [Chapitre 19](#), “Introduction au service Kerberos”.

### Gestion des tickets Kerberos

Cette section explique comment obtenir, afficher et détruire les tickets. Pour une présentation des tickets, reportez-vous à la section “[Fonctionnement du service Kerberos](#)” à la page 350.

### Avez-vous besoin de vous soucier des tickets ?

Avec l'une des versions SEAM ou les versions Oracle Solaris installées, Kerberos est intégré dans la commande `login`, et vous obtenez des tickets automatiquement lorsque vous vous connectez. Les commandes utilisant Kerberos `rsh`, `rcp`, `telnet` et `rlogin` sont généralement configurées pour fournir des copies de vos tickets aux autres machines, de sorte que vous n'avez pas à demander explicitement des billets pour obtenir l'accès à ces machines. Votre configuration

peut ne pas inclure ce transfert automatique, mais il s'agit du comportement par défaut. Reportez-vous aux sections “[Présentation des commandes utilisant Kerberos](#)” à la page 524 et “[Transfert des tickets Kerberos](#)” à la page 527 pour plus d’informations sur le transfert de tickets.

Pour plus d’informations sur les durées de vie des tickets, reportez-vous à la section “[Durée de vie des tickets](#)” à la page 538.

## Création d'un ticket Kerberos

Normalement, si le PAM est configuré correctement, un ticket est créé automatiquement lorsque vous vous connectez, et vous n'avez pas besoin d'effectuer une action spécifique pour obtenir un ticket. Cependant, vous devrez peut-être créer un ticket si votre ticket arrive à expiration. En outre, vous devrez peut-être utiliser un autre principal en plus de votre principal par défaut, par exemple, si vous utilisez `rlogin -l` pour vous connecter à un ordinateur sous l'identité d'un autre utilisateur.

Pour créer un ticket, utilisez la commande `kinit`.

```
% /usr/bin/kinit
```

La commande `kinit` vous invite à saisir votre mot de passe. Pour la syntaxe complète de la commande `kinit`, reportez-vous à la page de manuel [kinit\(1\)](#).

### EXEMPLE 24-1 Création d'un ticket Kerberos

Cet exemple illustre un utilisateur, `jennifer`, créant un ticket sur son propre système.

```
% kinit
Password for jennifer@ENG.EXAMPLE.COM: <Type password>
```

Ici, l'utilisateur `david` crée un ticket qui est valide pendant trois heures avec l'option `-l`.

```
% kinit -l 3h david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

L'exemple affiche l'utilisateur `david` créant un ticket transmissible (avec l'option `-f`) pour lui-même. Avec ce ticket transmissible, il peut, par exemple, se connecter à un autre système, puis se connecter via Internet ou un réseau local (`telnet`) à un système tiers.

```
% kinit -f david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

Pour plus d’informations sur la façon dont le transfert de tickets fonctionne, reportez-vous aux sections “[Transfert des tickets Kerberos](#)” à la page 527 et “[Types de tickets](#)” à la page 536.

## Affichage des tickets Kerberos

Tous les tickets ne sont pas similaires. Un seul ticket peut, par exemple, être *transmissible*. Un autre ticket peut être *postdaté*. Un troisième ticket peut être à la fois transmissible et postdaté. Vous pouvez voir les billets que vous avez, ainsi que leurs attributs, en utilisant la commande `klist` avec l'option `-f` :

```
% /usr/bin/klist -f
```

Les symboles suivants indiquent les attributs qui sont associés à chaque ticket, tel qu'affiché par `klist` :

|   |                                    |
|---|------------------------------------|
| A | Préauthentifié (Preauthenticated)  |
| D | Postdatable                        |
| d | Postdaté (Postdated)               |
| F | Transmissible (Forwardable)        |
| f | Transmis (Forwarded)               |
| I | Initial                            |
| i | Non valide (Invalid)               |
| P | Utilisable avec proxy (Proxiabale) |
| p | Proxy                              |
| R | Renouvelable (Renewable)           |

La section “[Types de tickets](#)” à la page 536 décrit les différents attributs qu'un ticket peut avoir.

### EXEMPLE 24-2 Affichage des tickets Kerberos

Cet exemple montre que l'utilisateur jennifer a un ticket *initial*, qui est *transmissible* (F) et *postdaté* (d), mais il n'a pas encore été validé (i).

```
% /usr/bin/klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: jennifer@EXAMPLE.COM

Valid starting          Expires              Service principal
09 Mar 04 15:09:51      09 Mar 04 21:09:51  nfs/EXAMPLE.COM@EXAMPLE.COM
                    renew until 10 Mar 04 15:12:51, Flags: Fdi
```

L'exemple suivant montre que l'utilisateur david a deux tickets qui ont été *transmis* (f) à son hôte à partir d'un autre hôte. Les tickets sont également *transmissibles* (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
```

**EXEMPLE 24-2** Affichage des tickets Kerberos (Suite)

Default principal: david@EXAMPLE.COM

| Valid starting                            | Expires            | Service principal            |
|-------------------------------------------|--------------------|------------------------------|
| 07 Mar 04 06:09:51                        | 09 Mar 04 23:33:51 | host/EXAMPLE.COM@EXAMPLE.COM |
| renew until 10 Mar 04 17:09:51, Flags: fF |                    |                              |

| Valid starting                            | Expires            | Service principal           |
|-------------------------------------------|--------------------|-----------------------------|
| 08 Mar 04 08:09:51                        | 09 Mar 04 12:54:51 | nfs/EXAMPLE.COM@EXAMPLE.COM |
| renew until 10 Mar 04 15:22:51, Flags: fF |                    |                             |

L'exemple suivant montre comment afficher les types de chiffrement de la clé de session et du ticket en utilisant l'option `-e`. L'option `-a` est utilisée pour mapper l'adresse de l'hôte à un nom d'hôte si le service de noms peut faire la conversion.

```
% klist -fea
```

Ticket cache: /tmp/krb5cc\_74287

Default principal: david@EXAMPLE.COM

| Valid starting                                                        | Expires            | Service principal              |
|-----------------------------------------------------------------------|--------------------|--------------------------------|
| 07 Mar 04 06:09:51                                                    | 09 Mar 04 23:33:51 | krbtgt/EXAMPLE.COM@EXAMPLE.COM |
| renew until 10 Mar 04 17:09:51, Flags: FRIA                           |                    |                                |
| Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32 |                    |                                |
| Addresses: client.example.com                                         |                    |                                |

## Destruction des tickets Kerberos

Si vous souhaitez détruire tous les tickets Kerberos acquis au cours de votre session en cours, utilisez la commande `kdestroy`. La commande détruit votre cache des informations d'identification, ce qui détruit toutes vos informations d'identification et tous les tickets. Bien que ce ne soit pas généralement nécessaire, l'exécution de `kdestroy` réduit le risque de compromettre le cache des informations d'identification pendant que vous n'êtes pas connecté.

Pour détruire vos tickets, utilisez la commande `kdestroy`.

```
% /usr/bin/kdestroy
```

La commande `kdestroy` détruit vos tickets *all*. Vous ne pouvez pas utiliser cette commande pour détruire sélectivement un ticket donné.

Si vous allez vous éloigner de votre système et êtes inquiet qu'un intrus puisse utiliser vos autorisations, vous devez utiliser `kdestroy` ou un économiseur d'écran qui verrouille l'écran.

# Gestion des mots de passe Kerberos

Avec le service Kerberos configuré, vous avez maintenant deux mots de passe : votre mot de passe Solaris normal et un mot de passe Kerberos. Vous pouvez faire en sorte que les deux mots de passe soient le même, ou ils peuvent être différents.

## Conseils sur le choix d'un mot de passe

Votre mot de passe peut inclure presque n'importe quel caractère que vous pouvez taper. Les principales exceptions sont les touches Ctrl et Entrée. Un bon mot de passe est un mot de passe facile à retenir, mais qu'aucune autre personne ne peut deviner facilement. Voici quelques exemples de mauvais mots de passe :

- Les mots qui peuvent être trouvés dans un dictionnaire.
- N'importe quel nom commun ou populaire.
- Le nom d'une personne ou d'un personnage célèbre.
- Votre nom ou nom d'utilisateur sous la forme de votre choix (par exemple : votre nom écrit à l'envers, répété deux fois et ainsi de suite).
- Nom du conjoint, d'un enfant ou d'un animal de compagnie.
- Votre date de naissance ou la date de naissance d'un parent.
- Votre numéro de sécurité sociale, numéro de permis de conduire, numéro de passeport ou autre numéro d'identification.
- Tout exemple de mot de passe apparaissant dans ce manuel ou n'importe quel autre manuel.

Un bon mot de passe est un mot de passe d'au moins huit caractères. En outre, un mot de passe doit inclure une combinaison de caractères, tels que des lettres majuscules et minuscules, des chiffres et des signes de ponctuation. Exemples de mots de passe qui seraient convenables s'ils ne figuraient pas dans ce manuel :

- Acronymes, tels que "I2LMHinSF" (dont on se souvient sous la forme "I too left my heart in San Francisco" (J'ai moi aussi eu le coeur brisé à San Francisco))
- Mots dénués de sens faciles à prononcer, tels que "WumpaBun" ou "WangDangdoodle!"
- Expressions délibérément mal orthographiées, telles que "6o'cluck" ou "RrriotGrrrlsRrrule!"



**Attention** – N'utilisez pas ces exemples. Les mots de passe qui figurent dans des manuels sont les premiers mots de passe qu'un intrus va essayer.

## Modification de votre mot de passe

Si le PAM est correctement configuré, vous pouvez modifier votre mot de passe Kerberos de deux manières :

- Avec la commande `passwd` UNIX habituelle. Avec le service Kerberos configuré, la commande `passwd` vous invite également automatiquement à entrer un nouveau mot de passe Kerberos.

L'avantage d'utiliser `passwd` au lieu de `kpasswd` est que vous pouvez définir les deux mots de passe Kerberos et UNIX en même temps. Cependant, en règle générale, *il n'est pas nécessaire* de modifier les deux mots de passe avec `passwd`. Souvent, vous pouvez uniquement modifier le mot de passe UNIX et laisser le mot de passe Kerberos inchangé, ou vice-versa.

---

**Remarque** – Le comportement de `passwd` dépend de la façon dont le module PAM est configuré. Vous pouvez être amené à modifier les deux mots de passe dans certaines configurations. Pour certains sites, le mot de passe UNIX doit être modifié, alors que d'autres sites nécessitent la modification du mot de passe Kerberos.

---

- Avec la commande `kpasswd`. `kpasswd` est très similaire à `passwd`. Une différence est que `kpasswd` ne change que les mots de passe Kerberos. Vous devez utiliser `passwd` si vous souhaitez modifier votre mot de passe UNIX.

Une autre différence est que `kpasswd` peut modifier un mot de passe pour un principal Kerberos qui n'est pas un utilisateur UNIX valide. Par exemple, `david/admin` est un principal Kerberos, mais n'est pas un utilisateur UNIX réel. Par conséquent, vous devez utiliser `kpasswd` au lieu de `passwd`.

Une fois que vous avez modifié votre mot de passe, un certain temps s'écoule avant que le changement ne se propage sur l'ensemble d'un système (en particulier sur un réseau de grande taille). En fonction de la configuration de votre système, ce délai peut prendre de quelques minutes à une heure ou plus. Si vous avez besoin d'obtenir de nouveaux tickets Kerberos peu de temps après avoir modifié votre mot de passe, essayez d'abord le nouveau mot de passe. Si le nouveau mot de passe ne fonctionne pas, essayez de nouveau à l'aide de l'ancien mot de passe.

Le protocole Kerberos V5 permet aux administrateurs système de définir des critères relatifs aux mots de passe autorisés pour chaque utilisateur. Ces critères sont définis par la *stratégie* définie pour chaque utilisateur (ou par une stratégie par défaut). Reportez-vous à la section [“Administration des stratégies Kerberos” à la page 494](#) pour plus d'informations sur les politiques.

Par exemple, supposons que la stratégie de l'utilisateur `jennifer` (appelons-la `jenpol`) demande que les mots de passe contiennent au moins huit lettres et incluent un mélange de deux types de caractères. `kpasswd` rejettera donc une tentative d'utiliser "sloth" comme mot de passe.



```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:      <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'sloth'>
New password (again): <Jennifer re-types 'sloth'>
kpasswd: New password is too short.
Please choose a password which is at least 4 characters long.
```

Ici, jennifer utilise "slothrop49" comme mot de passe. "Slothrop49" répond aux critères, car il contient plus de huit lettres et contient deux types différents de caractères (chiffres et lettres minuscules).

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:      <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'slothrop49'>
New password (again): <Jennifer re-types 'slothrop49'>
Kerberos password changed.
```

#### EXEMPLE 24-3 Modification de votre mot de passe

Dans l'exemple suivant, l'utilisateur david modifie ses deux mots de passe UNIX et Kerberos avec passwd.

```
% passwd
passwd: Changing password for david
Enter login password:      <Type the current UNIX password>
New password:              <Type the new UNIX password>
Re-enter password:         <Confirm the new UNIX password>
Old KRB5 password:         <Type the current Kerberos password>
New KRB5 password:         <Type the new Kerberos password>
Re-enter new KRB5 password: <Confirm the new Kerberos password>
```

Notez que passwd demande à la fois le mot de passe UNIX et le mot de passe Kerberos. Ce comportement est établi par la configuration par défaut. Dans ce cas, l'utilisateur david doit utiliser kpasswd pour définir son mot de passe Kerberos sur une autre valeur, comme indiqué ci-après.

**EXEMPLE 24-3** Modification de votre mot de passe (Suite)

Cet exemple illustre l'utilisateur david changeant seulement son mot de passe Kerberos avec `kpasswd`.

```
% kpasswd
kpasswd: Changing password for david@ENG.EXAMPLE.COM.
Old password:          <Type the current Kerberos password>
New password:          <Type the new Kerberos password>
New password (again):  <Confirm the new Kerberos password>
Kerberos password changed.
```

Dans cet exemple, l'utilisateur david modifie le mot de passe pour le principal Kerberos david/admin (qui n'est pas un utilisateur UNIX valide). Il doit utiliser `kpasswd`.

```
% kpasswd david/admin
kpasswd: Changing password for david/admin.
Old password:          <Type the current Kerberos password>
New password:          <Type the new Kerberos password>
New password (again):  <Type the new Kerberos password>
Kerberos password changed.
```

## Octroi de l'accès à votre compte

Si vous avez besoin d'autoriser quelqu'un à se connecter à votre compte (sous votre identité), vous pouvez le faire via Kerberos, sans révéler votre mot de passe, en insérant un fichier `.k5login` dans votre répertoire personnel. Un fichier `.k5login` est une liste d'un ou plusieurs principaux Kerberos correspondant à chaque personne à laquelle vous souhaitez accorder l'accès. Chaque principal doit figurer sur une ligne distincte.

Supposons que l'utilisateur david conserve un fichier `.k5login` dans son répertoire personnel qui se présente comme suit :

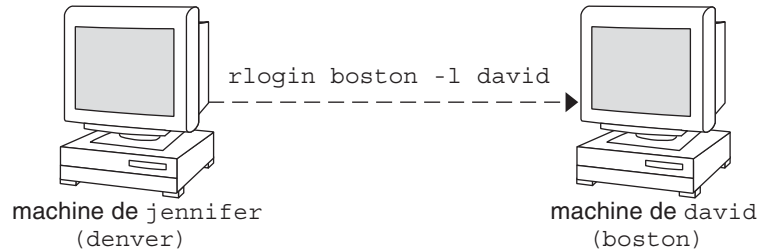
```
jennifer@ENG.EXAMPLE.COM
joe@EXAMPLE.ORG
```

Ce fichier permet aux utilisateurs jennifer et joe d'endosser l'identité de david, à condition qu'ils aient déjà des tickets Kerberos dans leurs domaines respectifs. Par exemple, jennifer peut se connecter à distance à la machine de david(boston), en tant que david, sans avoir à donner son mot de passe.

FIGURE 24-1 Utilisation du fichier .k5login pour accorder l'accès à votre compte

jennifer peut se connecter  
avec le compte de david  
sur la machine de celui-ci  
sans mot de passe.

david possède un fichier  
.k5login qui contient  
jennifer@ENG.ACME.COM



Dans le cas de figure où le répertoire personnel de david est monté sur NFS, à l'aide de protocoles Kerberos V5, à partir d'une autre (troisième) machine, jennifer doit avoir un ticket transmissible pour accéder à son répertoire personnel. Reportez-vous à la section [“Création d'un ticket Kerberos” à la page 516](#) pour obtenir un exemple d'utilisation d'un ticket transmissible.

Si vous devez vous connecter à d'autres ordinateurs sur un réseau, vous devrez inclure vos propres principaux Kerberos dans les fichiers .k5login sur ces machines.

L'utilisation d'un fichier .k5login est plus sûre que de donner votre mot de passe à un autre utilisateur, pour les raisons suivantes :

- Vous pouvez annuler l'accès à n'importe quel moment en supprimant le principal de votre fichier .k5login.
- Les principaux d'utilisateurs nommés dans le fichier .k5login dans votre répertoire personnel disposent d'un accès complet à votre compte sur cette machine (ou des ensembles de machines, si le fichier .k5login est partagé, par exemple, sur NFS). Toutefois, les services utilisant Kerberos autoriseront l'accès en fonction de l'identité de cet utilisateur, pas de la vôtre. Par conséquent, jennifer peut se connecter à la machine de joe et y effectuer des tâches. Toutefois, si elle utilise un programme utilisant Kerberos, tel que ftp ou rlogin, elle le fait sous sa propre identité.
- Kerberos conserve un journal des utilisateurs qui obtiennent des tickets. C'est pourquoi un administrateur système peut savoir, si nécessaire, qui est capable d'utiliser votre identité d'utilisateur à un moment donné.

Une méthode commune d'utiliser le fichier .k5login est de le placer dans le répertoire personnel de root, octroyant ainsi l'accès root pour cette machine aux principaux Kerberos répertoriés. Cette configuration permet aux administrateurs système de devenir root

localement, ou de se connecter à distance en tant que root, sans avoir à communiquer le mot de passe root, et sans qu'il soit nécessaire pour quiconque de taper le mot de passe root sur le réseau.

**EXEMPLE 24-4** Utilisation du fichier .k5login pour accorder l'accès à votre compte

Supposons que Jennifer décide de se connecter à l'ordinateur `boston.example.com` en tant que root. Parce qu'elle a une entrée pour son nom de principal dans le fichier `.k5login` dans le répertoire personnel de root sur `boston.example.com`, elle n'a à nouveau pas besoin de taper son mot de passe.

```
% rlogin boston.example.com -l root -x
This rlogin session is using DES encryption for all data transmissions.
Last login: Thu Jun 20 16:20:50 from daffodil
SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998
boston[root]%
```

## Commandes utilisateur Kerberos

Le produit Kerberos V5 est un système à *connexion unique*, ce qui signifie que vous n'avez à saisir votre mot de passe qu'une seule fois. Les programmes de Kerberos V5 effectuent l'authentification (et éventuellement le chiffrement) pour vous, car Kerberos a été intégré dans une suite de programmes réseau existants et connus. Les applications de Kerberos V5 sont des versions de programmes réseau UNIX existants auxquels des fonctions Kerberos ont été ajoutées.

Par exemple, lorsque vous utilisez un programme utilisant Kerberos pour vous connecter à un hôte distant, le programme, le KDC et l'hôte distant effectuent un ensemble de négociations rapides. Lorsque ces négociations sont terminées, le programme a prouvé votre identité en votre nom à l'hôte distant, et l'hôte distant vous a accordé l'accès.

Notez que les commandes utilisant Kerberos tentent de s'authentifier auprès de Kerberos en premier lieu. Si l'authentification Kerberos échoue, une erreur se produit ou l'authentification UNIX est tentée, en fonction des options qui ont été utilisées avec la commande. Reportez-vous à la section *Kerberos Security* dans chaque page de manuel des commandes Kerberos pour obtenir des informations plus détaillées.

## Présentation des commandes utilisant Kerberos

Les services réseau utilisant Kerberos sont des programmes qui se connectent à une autre machine quelque part sur Internet. Ces programmes sont les suivants :

- ftp
- rcp

- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Ces programmes ont des fonctionnalités qui utilisent de façon transparente vos tickets Kerberos pour négocier l'authentification et le chiffrement optionnel avec l'hôte distant. Dans la plupart des cas, vous remarquerez uniquement que vous n'avez plus à saisir votre mot de passe pour les utiliser, car Kerberos fournira une preuve de votre identité pour vous.

Les programmes réseau Kerberos V5 comprennent des options qui vous permettent de réaliser les opérations suivantes :

- Transférer vos billets à un autre hôte (si vous avez préalablement obtenu des tickets transmissibles).
- Chiffrer les données transférées entre vous et l'hôte distant.

---

**Remarque** – Cette section part du principe que vous êtes déjà familiarisé avec les versions non Kerberos de ces programmes, et met en évidence les fonctionnalités Kerberos ajoutées par le package Kerberos V5. Pour obtenir des descriptions détaillées des commandes décrites ici, reportez-vous à leurs pages de manuel respectives.

---

Les options Kerberos suivantes ont été ajoutées à `ftp`, `rcp`, `rlogin`, `rsh` et `telnet` :

- a           Tente la connexion automatique à l'aide de vos tickets existants. Utilise le nom d'utilisateur tel que renvoyé par `getlogin()`, sauf si le nom est différent de l'ID utilisateur en cours. Reportez-vous à la page de manuel `telnet(1)` pour plus de détails.
- f           Transfère un ticket *non transmissible* à un hôte distant. Cette option est mutuellement exclusive avec l'option `-F`. Elles ne peuvent pas être utilisées ensemble dans la même commande.

Vous voudrez transmettre un ticket si vous avez des raisons de croire que vous aurez besoin de vous authentifier auprès d'autres services basés sur Kerberos sur un troisième hôte. Par exemple, vous pouvez être amené à vous connecter à distance à un autre ordinateur, puis à vous connecter à distance à partir de celui-ci à une troisième machine.

Vous devez absolument utiliser un ticket transmissible si votre répertoire personnel sur l'hôte distant est monté sur NFS à l'aide du mécanisme Kerberos V5. Dans le cas contraire, vous ne pourrez pas accéder à votre répertoire personnel. En d'autres termes, supposons que vous vous connectiez d'abord au système 1. A partir du système 1, vous vous connectez

à distance sur votre machine, système 2, qui permet de monter votre répertoire personnel du système 3. Sauf si vous avez utilisé l'option - f ou -F avec rlogin, vous ne pourrez pas accéder à votre répertoire personnel car votre ticket ne peut pas être transmis au système 3.

Par défaut, kinit obtient des tickets d'octroi de tickets transmissibles (TGT, ticket-granting ticket). Cependant, votre configuration peut varier à cet égard.

Pour plus d'informations sur le transfert de tickets, reportez-vous à la section [“Transfert des tickets Kerberos” à la page 527](#).

-F Transfère une copie *retransmissible* de votre TGT à un système distant. Elle est similaire à - f, mais elle permet d'accéder à une autre machine (par exemple, une quatrième ou une cinquième). L'option -F peut donc être considérée comme étant un surensemble de l'option - f. L'option -F est mutuellement exclusive avec l'option - f. Elles ne peuvent pas être utilisées ensemble dans la même commande.

Pour plus d'informations sur le transfert de tickets, reportez-vous à la section [“Transfert des tickets Kerberos” à la page 527](#).

-k *realm* Demande des tickets pour l'hôte distant dans le domaine (*realm*) spécifié, au lieu de déterminer le domaine lui-même à l'aide du fichier krb5.conf.

-K Utilise vos billets pour l'authentification auprès de l'hôte distant, mais n'effectue pas la connexion automatiquement.

-m *mechanism* Spécifie le mécanisme de sécurité GSS-API à utiliser, comme indiqué dans le fichier /etc/gss/mech. La valeur par défaut est kerberos\_v5.

-x Chiffre cette session.

-X *auth-type* Désactive le type d'authentification *auth-type*.

Le tableau suivant présente les commandes offrant des options spécifiques. Un "X" indique que la commande a une option de ce type.

TABLEAU 24-1 Options Kerberos pour les commandes réseau

|    | ftp | rcp | rlogin | rsh | telnet |
|----|-----|-----|--------|-----|--------|
| -a |     |     |        |     | X      |
| -f | X   |     | X      | X   | X      |
| -F |     |     | X      | X   | X      |
| -k |     | X   | X      | X   | X      |

TABLEAU 24-1 Options Kerberos pour les commandes réseau (Suite)

|    | ftp | rcp | rlogin | rsh | telnet |
|----|-----|-----|--------|-----|--------|
| -K |     |     |        |     | X      |
| -m | X   |     |        |     |        |
| -x | X   | X   | X      | X   | X      |
| -X |     |     |        |     | X      |

En outre, `ftp` permet la définition du niveau de protection d'une session à son invité :

|                              |                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clear</code> (Annuler) | Définit le niveau de protection sur "clear" (aucune protection). Ce niveau de protection est la valeur par défaut.                                                                                                                                      |
| <code>private</code> (Privé) | Définit le niveau de protection sur "private". La confidentialité et l'intégrité des transmissions de données sont protégées par chiffrement. Toutefois, le service de confidentialité peut ne pas être disponible pour tous les utilisateurs Kerberos. |
| <code>safe</code> (Sécurisé) | Définit le niveau de protection sur "safe". L'intégrité des transmissions de données est protégée par contrôle cryptographique.                                                                                                                         |

Vous pouvez également définir le niveau de protection à l'invite `ftp` en tapant `protect` suivi par l'un des niveaux de protection indiqués ci-dessus (`clear`, `private` ou `safe`).

## Transfert des tickets Kerberos

Comme décrit dans la section "[Présentation des commandes utilisant Kerberos](#)" à la page 524, certaines commandes vous permettent de transférer les tickets à l'aide de l'option `-f` ou `-F`. Le transfert des billets vous permet de "chaîner" vos transactions réseau. Vous pouvez, par exemple, vous connecter à distance sur un seul ordinateur, puis vous connecter à distance à partir de celui-ci à une autre machine. L'option `-f` vous permet de transférer un ticket, tandis que l'option `-F` vous permet de retransférer un ticket transmis.

Dans la figure suivante, l'utilisateur `david` obtient un ticket d'octroi de tickets (TGT) non transmissible avec `kinit`. Le ticket est non transmissible car il n'a pas spécifié l'option `-f`. Dans le scénario 1, il est en mesure de se connecter à distance à la machine B, mais il ne peut aller plus loin. Dans le scénario 2, la commande `rlogin -f` échoue car il tente de transférer un ticket qui est non transmissible.

FIGURE 24-2 Utilisation des tickets non transmissibles

1. (Sur A) : `kinit david@ACME.ORG`



2. (Sur A) : `kinit david@ACME.ORG`



En réalité, les fichiers de configuration Kerberos sont définis de sorte que `kinit` obtient des tickets transmissibles par défaut. Cependant, votre configuration peut être différente. Pour les besoins de notre explication, supposons que `kinit` *n'obtienne pas* de TGT transmissibles sauf si elle est appelée avec `kinit -f`. Notez d'ailleurs que `kinit` n'a pas d'option `-F`. Les TGT sont soit transmissibles ou non.

Dans la figure suivante, l'utilisateur `david` obtient des TGT transmissibles avec `kinit -f`. Dans le scénario 3, il est en mesure d'atteindre la machine C, car il utilise un ticket transmissible avec la commande `rlogin`. Dans le scénario 4, la deuxième commande `rlogin` échoue parce que le ticket n'est pas retransférable. En utilisant l'option `-F` à la place, comme dans le scénario 5, la deuxième `rlogin` réussit et le ticket peut être retransféré à l'ordinateur D.

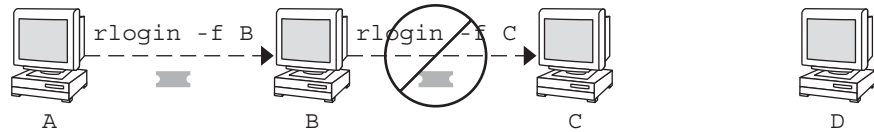


FIGURE 24-3 Utilisation de tickets transmissibles

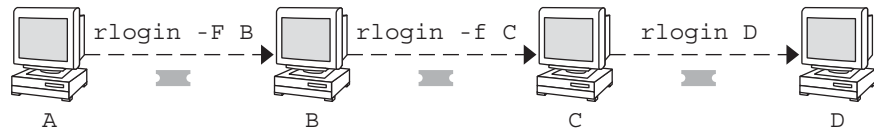
3. (Sur A) : `kinit -f david@ACME.ORG`



4. (Sur A) : `kinit -f david@ACME.ORG`



5. (Sur A) : `kinit -f david@ACME.ORG`



## Utilisation de commandes utilisant Kerberos (exemples)

Les exemples suivants montrent comment les options des commandes utilisant Kerberos fonctionnent.

**EXEMPLE 24-5** Utilisation des options `-a`, `-f` et `-x` avec `telnet`

Dans cet exemple, l'utilisateur david s'est déjà connecté et souhaite se connecter via Internet ou un réseau local (`telnet`) à la machine `denver.example.com`. Il utilise l'option `-f` pour transférer ses tickets existants, l'option `-x` pour chiffrer la session et l'option `-a` pour effectuer la connexion automatique. Dans la mesure où il n'a pas l'intention d'utiliser les services d'un troisième hôte, il peut utiliser `-f` au lieu de `-F`.

```
% telnet -a -f -x denver.example.com
Trying 128.0.0.5...
Connected to denver.example.com. Escape character is '^'.
[ Kerberos V5 accepts you as "david@eng.example.com" ]
[ Kerberos V5 accepted forwarded credentials ]
SunOS 5.9: Tue May 21 00:31:42 EDT 2004 Welcome to SunOS
%
```

Vous remarquerez que l'ordinateur de david a utilisé Kerberos pour l'authentifier auprès de `denver.example.com` et l'a connecté automatiquement sous son identité. Il a eu une session chiffrée, une copie de ses tickets déjà en attente, et il n'a jamais eu à entrer son mot de passe. S'il

**EXEMPLE 24-5** Utilisation des options -a, -f et -x avec telnet (Suite)

avait utilisé une version non Kerberos de telnet, il aurait été invité à saisir son mot de passe, lequel aurait été envoyé sur le réseau, non chiffré. Si un intrus avait analysé le trafic réseau à ce moment-là, il aurait connu le mot de passe de david.

Si vous transférez vos tickets Kerberos, telnet (ainsi que les autres commandes abordées ici) les détruit lorsqu'elle s'arrête.

**EXEMPLE 24-6** Utilisation de rlogin avec l'option -F

Ici, l'utilisateur jennifer veut se connecter à sa propre machine, boston.example.com. Elle transmet ses tickets existants avec l'option -F, et chiffre la session à l'aide de l'option -x. Elle choisit -F plutôt que -f car une fois qu'elle s'est connectée à boston, elle peut vouloir effectuer d'autres transactions réseau nécessitant le retransfert des tickets. En outre, dans la mesure où elle transfère ses tickets existants, elle n'a pas à saisir son mot de passe.

```
% rlogin boston.example.com -F -x
This rlogin session is using encryption for all transmissions.
Last login Mon May 19 15:19:49 from daffodil
SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003
%
```

**EXEMPLE 24-7** Définition du niveau de protection dans ftp

Supposons que joe veuille utiliser ftp pour obtenir son courrier à partir du répertoire ~joe/MAIL de la machine denver.example.com, en chiffrant la session. L'échange se présente comme suit :

```
% ftp -f denver.example.com
Connected to denver.example.com
220 denver.example.org FTP server (Version 6.0) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded Name (daffodil.example.org:joe)
232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe
230 User joe logged in.
Remote system type is UNIX.
Using BINARY mode to transfer files.
ftp> protect private
200 Protection level set to Private
ftp> cd ~joe/MAIL
250 CWD command successful.
ftp> get RMAIL
227 Entering Passive Mode (128,0,0,5,16,49)
150 Opening BINARY mode data connection for RMAIL (158336 bytes).
226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)
ftp> quit
%
```

Pour chiffrer la session, joe définit le niveau de protection sur private.

## Service Kerberos (référence)

---

Ce chapitre présente un grand nombre de fichiers, de commandes et de démons faisant partie du produit Kerberos. En outre, ce chapitre fournit des informations détaillées sur le fonctionnement de l'authentification Kerberos.

La liste suivante répertorie les informations de référence fournies dans ce chapitre :

- “Fichiers Kerberos” à la page 531
- “Commandes Kerberos” à la page 533
- “Démons Kerberos” à la page 534
- “Terminologie Kerberos” à la page 534
- “Fonctionnement du système d'authentification Kerberos” à la page 540
- “Obtention de l'accès à un service à l'aide de Kerberos” à la page 541
- “Utilisation des types de chiffrement Kerberos” à la page 544
- “Utilisation de la table `gsscred`” à la page 546
- “Différences notables entre Oracle Solaris Kerberos et MIT Kerberos” à la page 547

## Fichiers Kerberos

Cette section présente certains des fichiers utilisés par le service Kerberos.

TABLEAU 25-1 Fichiers Kerberos

| Nom du fichier                   | Description                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <code>~/ .gkadmin</code>         | Valeurs par défaut pour la création de principaux dans l'outil SEAM.                                                           |
| <code>~/ .k5login</code>         | Liste de principaux permettant l'accès à un compte Kerberos.                                                                   |
| <code>/etc/krb5/kadm5.acl</code> | Fichier ACL de Kerberos incluant les noms de principaux des administrateurs KDC et leurs privilèges d'administration Kerberos. |

TABLEAU 25-1 Fichiers Kerberos (Suite)

| Nom du fichier                  | Description                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| /etc/krb5/kadm5.keytab          | Obsolète : ce fichier a été supprimé de la version Oracle Solaris 11.                                                                                 |
| /etc/krb5/kdc.conf              | Fichier de configuration du KDC.                                                                                                                      |
| /etc/krb5/kpropd.acl            | Fichier de configuration de propagation de la base de données Kerberos.                                                                               |
| /etc/krb5/krb5.conf             | Fichier de configuration du domaine Kerberos.                                                                                                         |
| /etc/krb5/krb5.keytab           | Fichier keytab pour les serveurs d'application réseau.                                                                                                |
| /etc/krb5/warn.conf             | Fichier de configuration de renouvellement automatique et d'avertissement d'expiration des tickets Kerberos.                                          |
| /etc/pam.conf                   | PAM, fichier de configuration                                                                                                                         |
| /tmp/krb5cc_uid                 | par défaut, où <i>uid</i> est l'UID décimal de l'utilisateur.                                                                                         |
| /tmp/ovsec_adm.xxxxxxx          | Cache d'informations d'identification pour la durée de vie des opérations de modification de mot de passe, où <i>xxxxxx</i> est une chaîne aléatoire. |
| /var/krb5/.k5.REALM             | Fichier stash KDC contenant une copie de la clé principale de KDC                                                                                     |
| /var/krb5/kadmin.log            | Fichier journal de kadmin                                                                                                                             |
| /var/krb5/kdc.log               | Fichier journal du KDC                                                                                                                                |
| /var/krb5/principal             | Base de données de principaux Kerberos                                                                                                                |
| /var/krb5/principal.kadm5       | Base de données d'administration Kerberos contenant des informations de stratégie                                                                     |
| /var/krb5/principal.kadm5.lock  | Fichier de verrouillage de la base de données d'administration Kerberos                                                                               |
| /var/krb5/principal.ok          | Fichier d'initialisation de la base de données de principaux Kerberos, créé lors de l'initialisation réussie de la base de données Kerberos           |
| /var/krb5/principal.ulong       | Fichier journal de mise à jour Kerberos contenant des mises à jour pour la propagation incrémentielle                                                 |
| /var/krb5/slave_datatrans       | Fichier de sauvegarde du KDC utilisé par le script <i>kprop_script</i> pour la propagation                                                            |
| /var/krb5/slave_datatrans_slave | Fichier de vidage temporaire créé lors des mises à jour complètes sur le <i>slave</i> spécifié                                                        |

# Commandes Kerberos

Cette section présente quelques commandes incluses dans le produit Kerberos.

TABLEAU 25-2 Commandes Kerberos

| Commande                 | Description                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /usr/bin/ftp             | Programme FTP                                                                                                                                                                                                                                    |
| /usr/bin/kdestroy        | Détruit les tickets Kerberos                                                                                                                                                                                                                     |
| /usr/bin/kinit           | Obtient et met en cache les tickets d'octroi de tickets Kerberos                                                                                                                                                                                 |
| /usr/bin/klist           | Affiche les tickets Kerberos actuels                                                                                                                                                                                                             |
| /usr/bin/kpasswd         | Modifie un mot de passe Kerberos                                                                                                                                                                                                                 |
| /usr/bin/ktutil          | Gère les fichiers keytab Kerberos                                                                                                                                                                                                                |
| /usr/bin/kvno            | Répertorie les numéros de version clé pour les principaux Kerberos                                                                                                                                                                               |
| /usr/bin/rcp             | Programme de copie de fichiers à distance                                                                                                                                                                                                        |
| /usr/bin/rlogin          | Programme de connexion à distance                                                                                                                                                                                                                |
| /usr/bin/rsh             | Programme de shell à distance                                                                                                                                                                                                                    |
| /usr/bin/telnet          | Programme telnet utilisant Kerberos                                                                                                                                                                                                              |
| /usr/lib/krb5/kprop      | Programme de propagation de base de données Kerberos                                                                                                                                                                                             |
| /usr/sbin/gkadmin        | Programme d'interface graphique d'administration de base de données Kerberos utilisé pour gérer les principaux et les stratégies                                                                                                                 |
| /usr/sbin/gsscred        | Gère les entrées de tableau gsscred                                                                                                                                                                                                              |
| /usr/sbin/kadmin         | Programme d'interface graphique d'administration de base de données Kerberos à distance (utilisé avec l'authentification Kerberos), utilisé pour gérer les principaux, les stratégies et les fichiers keytab                                     |
| /usr/sbin/kadmin.local   | Programme d'interface graphique d'administration de base de données Kerberos local (utilisé sans l'authentification Kerberos et devant être exécuté sur le KDC maître), utilisé pour gérer les principaux, les stratégies et les fichiers keytab |
| /usr/sbin/kcclient       | Script d'installation du client Kerberos utilisé avec ou sans profil d'installation                                                                                                                                                              |
| /usr/sbin/kdb5_ldap_util | Crée des conteneurs LDAP pour les bases de données Kerberos                                                                                                                                                                                      |
| /usr/sbin/kdb5_util      | Crée des bases de données Kerberos et des fichiers stash                                                                                                                                                                                         |

| TABLEAU 25-2 Commandes Kerberos (Suite) |                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------|
| Commande                                | Description                                                                         |
| /usr/sbin/kgcmgr                        | Configure les KDC maître et esclaves Kerberos                                       |
| /usr/sbin/kproplog                      | Présente un récapitulatif des entrées de mise à jour dans le journal de mise à jour |

## Démons Kerberos

La table suivante répertorie les démons utilisés par les produits Kerberos.

| TABLEAU 25-3 Démons Kerberos |                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------|
| Démon                        | Description                                                                              |
| /usr/sbin/in.ftpd            | Démon de FTP                                                                             |
| /usr/lib/krb5/kadmind        | Démon d'administration de base de données Kerberos                                       |
| /usr/lib/krb5/kpropd         | Démon de propagation de base de données Kerberos                                         |
| /usr/lib/krb5/krb5kdc        | Démon de traitement des tickets Kerberos                                                 |
| /usr/lib/krb5/ktkt_warnd     | Démon de renouvellement automatique et d'avertissement d'expiration des tickets Kerberos |
| /usr/sbin/in.rlogind         | Démon de connexion à distance                                                            |
| /usr/sbin/in.rshd            | Démon de shell à distance                                                                |
| /usr/sbin/in.telnetd         | Démon telnet                                                                             |

## Terminologie Kerberos

La section suivante présente les termes Kerberos et leurs définitions. Ces termes sont utilisés dans la documentation Kerberos. Une bonne compréhension de ces termes est essentielle pour appréhender les concepts Kerberos.

### Terminologie spécifique à Kerberos

Vous devez comprendre les termes de cette section pour pouvoir administrer les KDC.

Le *Centre de distribution des clés (Key Distribution Center)* ou *KDC* est le composant de Kerberos responsable de l'émission d'informations d'identification. Ces informations d'identification sont créées à l'aide des informations stockées dans la base de données KDC. Chaque domaine a besoin d'au moins deux KDC, un maître et au moins un esclave. Tous les

KDC génèrent des informations d'identification, mais seul le KDC maître gère toutes les modifications apportées à la base de données KDC.

Un *fichier stash* contient la clé principale du KDC. Cette clé est utilisée lorsqu'un serveur est redémarré pour authentifier automatiquement le KDC avant qu'il ne démarre les commandes `kadmind` et `krb5kdc`. Etant donné que ce fichier inclut la clé principale, ce fichier et toutes ses sauvegardes doivent être sécurisés. Le fichier est créé avec des autorisations en lecture seule pour `root`. Pour garder le fichier sécurisé, vous ne devez pas modifier les autorisations. Si le fichier est compromis, la clé peut être utilisée pour accéder à la base de données KDC ou la modifier.

## Terminologie spécifique à l'authentification

Vous devez connaître les termes de cette section pour comprendre le processus d'authentification. Les programmeurs et les administrateurs système doivent être familiarisés avec ces termes.

Un *client* est un logiciel qui s'exécute sur le poste de travail d'un utilisateur. Le logiciel Kerberos qui s'exécute sur le client effectue de nombreuses demandes au cours de ce processus. Par conséquent, il est important de différencier les actions de ce logiciel de celles de l'utilisateur.

Les termes *server* et *service* sont souvent interchangeables. Pour clarifier, le terme *server* est utilisé pour définir le système physique sur lequel le logiciel Kerberos est en cours d'exécution. Le terme *service* correspond à une fonction particulière prise en charge sur un serveur (par exemple, `ftp` ou `nfs`). Dans la plupart des cas, la documentation mentionne les serveurs dans le cadre d'un service, mais cette définition obscurcit la signification des termes. Par conséquent, le terme *server* fait référence au système physique. Le terme *service* désigne le logiciel.

Le produit Kerberos utilise deux types de clés. Un type de clé est dérivé du mot de passe. Chaque principal d'utilisateur reçoit une clé dérivée du mot de passe qui n'est connue que du KDC et de l'utilisateur. L'autre type de clé utilisé par le produit Kerberos est une clé aléatoire qui n'est pas associée à un mot de passe et donc n'est pas adapté à l'utilisation par les principaux d'utilisateur. Les clés aléatoires sont généralement utilisées pour les principaux de service qui ont des entrées dans un fichier `keytab` et les clés de session générées par le KDC. Les principaux de service peuvent utiliser des clés aléatoires étant donné que le service peut accéder à la clé dans le fichier `keytab` qui lui permet de fonctionner de manière non interactive. Les clés de session sont générées par le KDC (et partagées entre le client et le service) pour assurer la sécurité des transactions entre un client et un service.

Un *ticket* est un paquet d'informations servant à transmettre en toute sécurité l'identité d'un utilisateur à un serveur ou un service. Un ticket n'est valable que pour un client et un service particulier sur un serveur spécifique. Un ticket contient les informations suivantes :

- Nom du principal du service
- Nom du principal de l'utilisateur

- Adresse IP de l'hôte de l'utilisateur
- Horodatage
- Valeur définissant la durée de vie du ticket.
- Copie de la clé de session

Toutes ces données sont chiffrées dans la clé de service du serveur. Notez que le KDC émet le ticket incorporé dans des informations d'identification décrites ci-dessous. Une fois le ticket émis, il peut être réutilisé jusqu'à son expiration.

Les *informations d'identification* sont un paquet d'informations comprenant un ticket et la clé de session correspondante. Les informations d'identification sont chiffrées avec la clé du principal effectuant la demande. En règle générale, le KDC génère des informations d'identification en réponse à une demande de ticket d'un client.

Un *authentificateur* correspond à des informations utilisées par le serveur pour authentifier le principal de l'utilisateur du client. Un authentificateur inclut le nom du principal de l'utilisateur, un horodatage et d'autres données. 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 partagée par le client et le serveur. En général, le client crée l'authentificateur et l'envoie à l'aide du ticket du serveur ou du service pour s'authentifier auprès du serveur ou du service.

## Types de tickets

Les tickets ont des propriétés qui régissent la façon dont ils peuvent être utilisés. Ces propriétés sont assignées au ticket lors de sa création et peuvent être modifiées ultérieurement. Par exemple, un ticket peut passer de *transmissible* à *transmis*. Vous pouvez visualiser les propriétés de ticket à l'aide de la commande `klist`. Voir “[Affichage des tickets Kerberos](#)” à la page 517.

Les tickets peuvent être décrits par un ou plusieurs des termes suivants :

Transmissible/transmis (Forwardable/forwarded)

Un ticket transmissible peut être envoyé à partir d'un hôte vers un autre hôte, supprimant la nécessité d'un client de se réauthentifier. Par exemple, si l'utilisateur `david` obtient un ticket transmissible sur la machine de l'utilisateur `jennifer`, il peut se connecter à sa propre machine sans devoir demander un nouveau ticket (et donc s'authentifier à nouveau). Pour consulter un exemple d'utilisation d'un ticket transmissible, reportez-vous à l'[Exemple 24-1](#).

Initial

Un ticket initial est un ticket émis directement, et non sur la base d'un ticket d'octroi de tickets. Certains services, tels que les applications modifiant les mots de passe, peuvent nécessiter des tickets marqués comme étant initiaux afin d'assurer que le client peut démontrer qu'il connaît sa clé secrète. Un ticket initial indique que le client s'est récemment authentifié et ne dépend pas d'un ticket d'octroi de tickets qui peut exister depuis un certain temps.



### Non valide (Invalid)

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

### Postdatable/postdaté (Postdatable/postdated)

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

### Utilisable avec proxy/proxy (Proxiable/proxy)

Parfois, il est nécessaire à un principal de permettre à un service d'effectuer une opération en son nom. Le nom du principal du proxy doit être spécifié lorsque le ticket est créé. La version Oracle Solaris ne prend pas en charge les tickets utilisables avec proxy ou les tickets proxy.

Un ticket utilisable avec proxy est similaire à un ticket transmissible, à ceci près qu'il n'est valide que pour un seul service, tandis qu'un ticket transmissible accorde l'utilisation complète de l'identité du client au service. Un ticket transmissible peut par conséquent être considéré comme une sorte de super-proxy.

### Renouvelable (Renewable)

Comme les tickets avec de très longues durées de vie impliquent un risque de sécurité, les tickets peuvent être désignés comme renouvelables. Un ticket renouvelable possède deux moments d'expiration : l'heure à laquelle l'instance courante du ticket expire et la durée de vie maximale de tout ticket (une semaine). Si un client souhaite continuer à utiliser un ticket, il peut le renouveler avant sa première expiration. Par exemple, un ticket peut être valide pendant une heure, et tous les tickets ont une durée de vie maximale de dix heures. Si le client détenant le ticket souhaite le conserver plus d'une heure, il doit le renouveler dans l'heure. Lorsqu'un ticket atteint sa durée de vie maximale (dix heures), celui-ci expire automatiquement et ne peut pas être renouvelé.

Pour plus d'informations sur la façon de visualiser les attributs de tickets, reportez-vous à la section [“Affichage des tickets Kerberos” à la page 517](#).

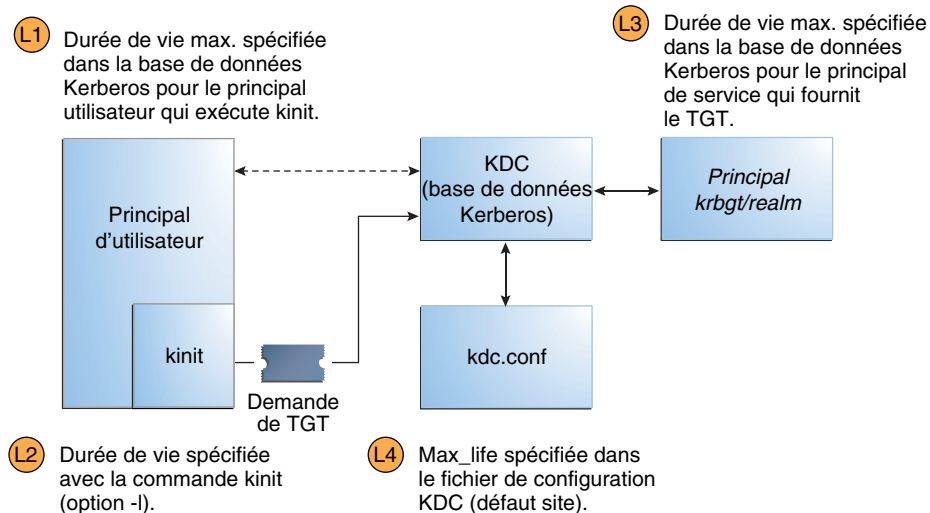
## Durée de vie des tickets

Chaque fois qu'un principal obtient un ticket, y compris un ticket d'octroi de tickets (TGT), la durée de vie du ticket est définie comme la plus petite des valeurs de durée de vie suivantes :

- Valeur de durée de vie spécifiée par l'option `-l` de la commande `kinit`, si `kinit` est utilisée pour obtenir le ticket. Par défaut, `kinit` utilise la valeur de durée de vie maximale.
- Valeur de durée de vie maximale (`max_life`) spécifiée dans le fichier `kdc.conf`.
- Valeur de durée de vie maximale spécifiée dans la base de données Kerberos pour le principal de service fournissant le ticket. Dans le cas de `kinit`, le principal de service est `krbtgt/realm`.
- Valeur de durée de vie maximale spécifiée dans la base de données Kerberos pour le principal d'utilisateur demandant le ticket.

La [Figure 25-1](#) montre comment la durée de vie d'un TGT est déterminée et d'où les quatre valeurs de durée de vie proviennent. Même si cette figure montre comment la durée de vie d'un TGT est déterminée, la même chose se produit globalement pour chaque obtention de ticket par un principal. La seule différence est que `kinit` n'offre pas une valeur de durée de vie et que le principal de service fournissant le ticket fournit une valeur de durée de vie maximale (au lieu du principal `krbtgt/realm`).

FIGURE 25-1 Détermination de la durée de vie d'un TGT



Durée de vie des tickets = valeur minimum de L1, L2, L3 et L4

La durée de vie d'un ticket renouvelable est également déterminée à partir de la plus basse de quatre valeurs, mais des valeurs de durée de vie renouvelables sont utilisées à la place, comme suit :

- Valeur de durée de vie renouvelable spécifiée par l'option `-r` de `kinit`, si `kinit` est utilisée pour obtenir ou renouveler le ticket.
- Valeur de durée de vie renouvelable maximale (`max_renewable_life`) spécifiée dans le fichier `kdc.conf`.
- Valeur de durée de vie renouvelable maximale spécifiée dans la base de données Kerberos pour le principal de service fournissant le ticket. Dans le cas de `kinit`, le principal de service est `krbtgt/realm`.
- Valeur de durée de vie renouvelable maximale spécifiée dans la base de données Kerberos pour le principal d'utilisateur demandant le ticket.

## Noms de principaux Kerberos

Chaque ticket est identifié par un nom de principal. Le nom de principal peut identifier un utilisateur ou un service. Voici des exemples de noms de principaux.

TABLEAU 25-4 Exemples de noms de principaux Kerberos

| Principal Name (Nom du principal)                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>changepw/kdc1.example.com@EXAMPLE.COM</code> | Principal pour le serveur KDC maître qui permet l'accès au KDC lorsque vous modifiez les mots de passe.                                                                                                                                                                                                                                                                                                                                |
| <code>clntconfig/admin@EXAMPLE.COM</code>          | Principal utilisé par l'utilitaire d'installation <code>kclient</code> .                                                                                                                                                                                                                                                                                                                                                               |
| <code>ftp/boston.example.com@EXAMPLE.COM</code>    | Principal utilisé par le service <code>ftp</code> . Ce principal peut être utilisé à la place d'un principal <code>host</code> .                                                                                                                                                                                                                                                                                                       |
| <code>host/boston.example.com@EXAMPLE.COM</code>   | Principal utilisé par des applications utilisant Kerberos ( <code>klist</code> et <code>kprop</code> , par exemple) et des services (tels que <code>ftp</code> et <code>telnet</code> ). Ce principal est appelé <code>host</code> ou principal de service. Le principal est utilisé pour authentifier les montages NFS. Ce principal est également utilisé par un client pour vérifier que le TGT émis au client provient du bon KDC. |
| <code>K/M@EXAMPLE.COM</code>                       | Nom de principal de la clé principale. Un nom de principal de clé principale est associé à chaque KDC maître.                                                                                                                                                                                                                                                                                                                          |
| <code>kadmin/history@EXAMPLE.COM</code>            | Principal incluant une clé utilisée pour conserver l'historique des mots de passe d'autres principaux. Chaque KDC maître possède l'un de ces principaux.                                                                                                                                                                                                                                                                               |
| <code>kadmin/kdc1.example.com@EXAMPLE.COM</code>   | Principal pour le serveur KDC maître qui permet l'accès au KDC à l'aide de la commande <code>kadmin</code> .                                                                                                                                                                                                                                                                                                                           |

TABLEAU 25-4 Exemples de noms de principaux Kerberos (Suite)

| Principal Name (Nom du principal)        | Description                                                                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| kadmin/changepw.example.com@EXAMPLE.COM  | Principal utilisé pour accepter les demandes de modification de mot de passe émises par les clients qui n'exécutent pas une version d'Oracle Solaris. |
| krbtgt/EXAMPLE.COM@EXAMPLE.COM           | Ce principal est utilisé lors de la génération d'un ticket d'octroi de tickets.                                                                       |
| krbtgt/EAST.EXAMPLE.COM@WEST.EXAMPLE.COM | Ce principal est un exemple de ticket d'octroi de tickets inter-domaine.                                                                              |
| nfs/boston.example.com@EXAMPLE.COM       | Principal utilisé par le service NFS. Ce principal peut être utilisé à la place d'un principal host.                                                  |
| root/boston.example.com@EXAMPLE.COM      | Principal associé au compte root sur un client. Ce principal est appelé principal root et fournit un accès root aux systèmes de fichiers montés NFS.  |
| username@EXAMPLE.COM                     | Principal d'un utilisateur.                                                                                                                           |
| username/admin@EXAMPLE.COM               | Principal admin pouvant être utilisé pour l'administration de la base de données KDC.                                                                 |

## Fonctionnement du système d'authentification Kerberos

Des applications vous permettent de vous connecter à un système distant si vous pouvez fournir un ticket apportant la preuve de votre identité et un clé de session correspondante. La clé de session contient des informations spécifiques à l'utilisateur et au service en cours d'accès. Un ticket et une clé de session sont créés par le KDC pour tous les utilisateurs lors de leur première connexion. Le ticket et la clé de session correspondante constituent des informations d'identification. Lors de l'utilisation de plusieurs services réseau, un utilisateur peut obtenir de nombreuses informations d'identification. L'utilisateur doit disposer d'informations d'identification pour chaque service s'exécutant sur un serveur particulier. Par exemple, l'accès au service ftp sur un serveur nommé boston nécessite des informations d'identification. L'accès au service ftp sur un autre serveur nécessite ses propres informations d'identification.

Le processus de création et de stockage des informations d'identification est transparent. Les informations d'identification sont créées par le KDC, qui les envoie aux demandeurs. Une fois reçues, les informations d'identification sont stockées dans un cache d'informations d'identification.

## Interaction du service Kerberos avec le DNS et le service nsswitch.conf

Le service Kerberos est compilé pour utiliser le DNS pour la résolution des noms d'hôte. Le service nsswitch n'est pas du tout consulté lorsque la résolution de nom d'hôte est terminée.

## Obtention de l'accès à un service à l'aide de Kerberos

Pour accéder à un service spécifique sur un serveur spécifique, l'utilisateur doit obtenir deux types d'informations d'identification. Le premier est pour le ticket d'octroi de tickets (aussi appelé TGT). Une fois que le service d'octroi de ticket a déchiffré ces informations d'identification, le service crée d'autres informations d'identification pour le serveur auquel l'utilisateur demande l'accès. Ces informations d'identification peuvent ensuite être utilisées pour demander l'accès à ce service sur le serveur. Une fois que le serveur a déchiffré ces informations d'identification, l'utilisateur obtient l'accès. Les sections suivantes décrivent le processus de manière plus détaillée.

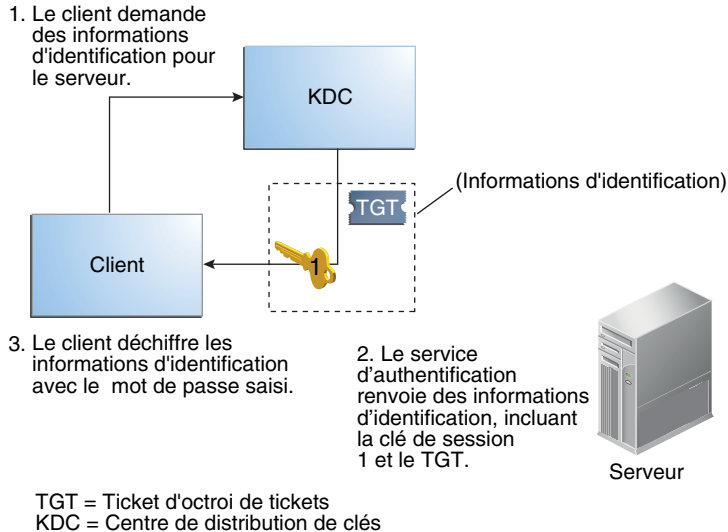
### Obtention d'informations d'identification pour le service d'octroi de tickets

1. Pour démarrer le processus d'authentification, le client envoie une demande au serveur d'authentification pour un principal d'utilisateur spécifique. Cette demande est envoyée sans chiffrement. Aucune information sécurisée n'est incluse dans la demande, de sorte qu'il n'est pas nécessaire d'utiliser de chiffrement.
2. Lorsque la demande est reçue par le service d'authentification, le nom de principal de l'utilisateur est recherché dans la base de données KDC. Si un principal correspond à l'entrée dans la base de données, le service d'authentification obtient la clé privée pour ce principal. Le service d'authentification génère ensuite une clé de session utilisable par le client et le service d'octroi de tickets (appelez-la Session key 1) et un ticket pour le service d'octroi de tickets (Ticket 1). Ce ticket est également qualifié de *ticket d'octroi de tickets* (TGT). La clé de session et le ticket sont chiffrés à l'aide de la clé privée de l'utilisateur, et les informations sont renvoyées au client.
3. Le client utilise ces informations pour déchiffrer Session Key 1 et Ticket 1 à l'aide de la clé privée pour le principal de l'utilisateur. Comme la clé privée doit uniquement être connue de l'utilisateur et de la base de données KDC, les informations du paquet doivent être sécurisées. Le client stocke les informations dans le cache d'informations d'identification.

Au cours de ce processus, l'utilisateur est invité à saisir un mot de passe normalement. Si le mot de passe spécifié par l'utilisateur est le même que celui utilisé pour créer la clé privée stockée dans la base de données KDC, alors le client peut déchiffrer les informations envoyées par le

service d'authentification. Maintenant, le client dispose d'informations d'identification à utiliser avec le service d'octroi de tickets. Le client est prêt à demander des informations d'identification pour un serveur.

FIGURE 25-2 Obtention d'informations d'identification pour le service d'octroi de tickets



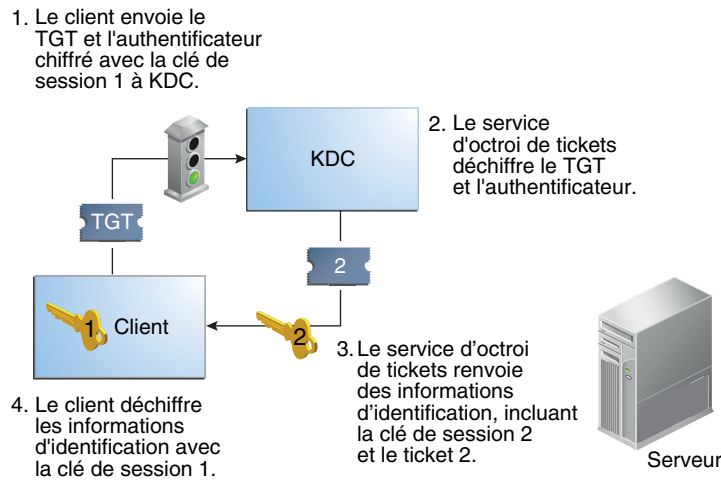
## Obtention d'informations d'identification pour un serveur

1. Pour demander l'accès à un serveur spécifique, un client doit d'abord avoir obtenu des informations d'identification pour ce serveur à partir du service d'authentification. Reportez-vous à la section [“Obtention d'informations d'identification pour le service d'octroi de tickets” à la page 541](#). Le client envoie ensuite une demande au service d'octroi de ticket, qui inclut le nom du principal de service, Ticket 1, et un authentificateur chiffré avec Session Key 1. Ticket 1 a été initialement chiffré par le service d'authentification à l'aide de la clé du service d'octroi de tickets.
2. Comme la clé de service du service d'octroi de tickets est connue du service d'octroi de tickets, Ticket 1 peut être déchiffré. Les informations de Ticket 1 comprennent Session Key 1, de sorte que le service d'octroi de tickets peut déchiffrer l'authentificateur. A ce stade, le principal de l'utilisateur est authentifié avec le service d'octroi de tickets.
3. Une fois l'authentification réussie, le service d'octroi de tickets génère une clé de session pour le principal de l'utilisateur et le serveur (Session Key 2), et un ticket pour le serveur (Ticket 2). Session Key 2 et Ticket 2 sont ensuite chiffrés à l'aide de Session Key 1. Etant

donné que Session Key 1 est uniquement connue du client et du service d'octroi de tickets, cette information est sécurisée et peut être envoyée sans problème sur le réseau.

4. Lorsque le client reçoit ce paquet d'informations, il déchiffre les informations en utilisant Session Key 1, qui était stockée dans le cache des informations d'identification. Le client dispose d'informations d'identification à utiliser avec le serveur. Maintenant, le client est prêt à demander l'accès à un service particulier sur ce serveur.

FIGURE 25-3 Obtention d'informations d'identification pour un serveur

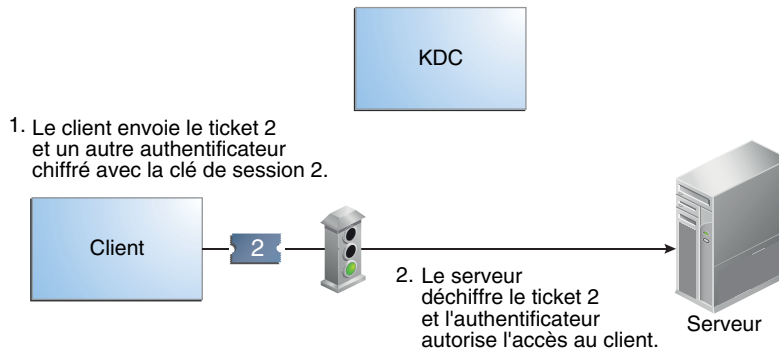


TGT = Ticket d'octroi de tickets  
KDC = Centre de distribution de clés

## Obtention de l'accès à un service donné

1. Pour demander l'accès à un service spécifique, le client doit d'abord avoir obtenu des informations d'identification pour le service d'octroi de tickets à partir du serveur d'authentification, et des informations d'identification de serveur à partir du service d'octroi de tickets. Reportez-vous aux sections [“Obtention d'informations d'identification pour le service d'octroi de tickets” à la page 541](#) et [“Obtention d'informations d'identification pour un serveur” à la page 542](#). Le client peut alors envoyer une demande au serveur en incluant Ticket 2 et un autre authentificateur. L'authentificateur est chiffré à l'aide de Session key 2.
2. Ticket 2 a été chiffré par le service d'octroi de tickets avec la clé de service pour le service. Etant donné que la clé de service est appelée par le principal de service, le service peut déchiffrer Ticket 2 et obtenir Session Key 2. Session Key 2 peut alors être utilisée pour déchiffrer l'authentificateur. Si l'authentificateur est correctement déchiffré, le client obtient l'accès au service.

FIGURE 25-4 Obtention de l'accès à un service donné



## Utilisation des types de chiffrement Kerberos

Les types de chiffrement identifient les algorithmes cryptographiques et le mode à utiliser lors d'opérations cryptographiques. Les types de chiffrement aes, des3-cbc-sha1 et rc4-hmac permettent de créer des clés à utiliser pour des opérations cryptographiques renforcées. Ces opérations renforcées améliorent la sécurité globale du service Kerberos.

---

**Remarque** – Dans les versions antérieures à la version Solaris 10 8/07, le type de chiffrement aes256-cts-hmac-sha1-96 peut être utilisé avec le service Kerberos si les packages Strong Cryptographic non fournis en standard sont installés.

---

Lorsqu'un client demande un ticket au KDC, le KDC doit utiliser des clés dont le type de chiffrement est compatible à la fois avec le client et le serveur. Bien que le protocole Kerberos permette au client de demander à ce que le KDC utilise certains types de chiffrement pour la partie de réponse du ticket du client, le protocole n'autorise pas le serveur à spécifier des types de chiffrement au KDC.

---

**Remarque** – Si le KDC maître installé n'exécute pas la version Solaris 10, les KDC esclaves doivent être mis à niveau vers la version Solaris 10 avant de mettre à niveau le KDC maître. Un KDC maître Solaris 10 utilise les nouveaux types de chiffrement, ce qu'un esclave plus ancien n'est pas en mesure de faire.

---

Le tableau suivant répertorie certains des problèmes à prendre en compte avant de modifier les types de chiffrement.

- Le KDC suppose que le premier type de clé/chiffrement associé à l'entrée du principal du serveur dans la base de données du principal est pris en charge par le serveur.



- Sur le KDC, vous devez vous assurer que les clés générées pour le principal sont compatibles avec les systèmes sur lesquels le principal sera authentifié. Par défaut, la commande `kadmin` crée des clés pour tous les types de chiffrement pris en charge. Si les systèmes sur lesquels le principal est utilisé ne prennent pas en charge cette configuration par défaut des types de chiffrement, vous devez restreindre les types de chiffrement lors de la création d'un principal. Vous pouvez limiter les types de chiffrement par l'intermédiaire de l'indicateur `-e` dans `kadmin addprinc` ou en définissant le paramètre `supported_encetypes` dans le fichier `kdc.conf` sur ce sous-ensemble. Le paramètre `supported_encetypes` doit être utilisé lorsque la plupart des systèmes d'un domaine Kerberos prennent en charge un sous-ensemble de l'ensemble par défaut des types de chiffrement. Le paramètre `supported_encetypes` spécifie l'ensemble par défaut des types de chiffrement utilisés par `kadmin addprinc` lorsqu'il crée un principal pour un domaine particulier. En règle générale, il est préférable de contrôler les types de chiffrement utilisés par Kerberos à l'aide de l'une de ces deux méthodes.
- Au moment de déterminer les types de chiffrement pris en charge par un système, pensez à la fois à la version de Kerberos exécutée sur le système et aux algorithmes cryptographiques pris en charge par l'application du serveur pour lequel un principal de serveur est en cours de création. Par exemple, lorsque vous créez un principal de service `nfs/hostname`, il est conseillé de limiter les types de chiffrement aux types pris en charge par le serveur NFS de l'hôte. Notez que dans la version Solaris 10, tous les types de chiffrement Kerberos pris en charge le sont également par le serveur NFS.
- Le paramètre `master_key_encetype` dans le fichier `kdc.conf` peut être utilisé pour contrôler le type de chiffrement de la clé principale qui chiffre les entrées dans la base de données du principal. N'utilisez pas ce paramètre si la base de données du principal KDC a déjà été créée. Le paramètre `master_key_encetype` peut être utilisé au moment de la création de la base de données afin de faire passer le type de chiffrement de la clé principale par défaut de `des-cbc-crc` à un type de chiffrement supérieur. Assurez-vous que tous les KDC esclaves prennent en charge le type de chiffrement choisi et qu'ils ont la même entrée `master_key_encetype` dans leur `kdc.conf` lorsque vous configurez les KDC esclaves. Assurez-vous également que le paramètre `master_key_encetype` est défini sur l'un des types de chiffrement dans `supported_encetypes`, si `supported_encetypes` est défini dans `kdc.conf`. Si l'une ou l'autre de ces situations n'est pas gérée correctement, le KDC maître peut ne pas être en mesure de travailler avec les KDC esclaves.
- Sur le client, vous pouvez contrôler les types de chiffrement demandés par le client lors de l'obtention de tickets du KDC par le biais de quelques paramètres dans `krb5.conf`. Le paramètre `default_tkt_encetypes` spécifie les types de chiffrement que le client est disposé à utiliser lorsqu'il demande un ticket d'octroi de tickets (TGT) au KDC. Le TGT est utilisé par le client pour acquérir d'autres tickets de serveur d'une manière plus efficace. L'effet du paramètre `default_tkt_encetypes` est de donner au client un contrôle sur les types de chiffrement utilisés pour protéger les communications entre le client et le KDC, lorsque le client demande un ticket de serveur via TGT (aussi appelé demande TGS). Notez que les types de chiffrement spécifiés dans `default_tkt_encetypes` doivent correspondre à au moins l'un des types de chiffrement de clé du principal dans la base de données du principal stockée sur le KDC. Dans le cas contraire, la demande TGS échoue. Dans la plupart des cas,

il est préférable de ne pas définir `default_tkt_etypes` car ce paramètre peut être une source de problèmes d'interopérabilité. Par défaut, le code client demande tous les types de chiffrement pris en charge et le KDC choisit les types de chiffrement en fonction des clés que le KDC trouve dans la base de données du principal.

- Le paramètre `default_tgs_etypes` restreint les types de chiffrement demandés par le client dans ses demandes TGS, qui sont utilisés pour l'acquisition de tickets de serveur. Ce paramètre restreint également les types de chiffrement utilisés par le KDC lors de la création de la clé de session partagée par le client et le serveur. Par exemple, si un client souhaite utiliser uniquement le chiffrement 3DES pour un NFS sécurisé, vous devez définir `default_tgs_etypes = des3-cbc-sha1`. Assurez-vous que les principaux du client et du serveur ont une clé `des-3-cbc-sha1` dans la base de données du principal. Comme avec `default_tkt_etype`, il est sans doute préférable dans la plupart des cas de ne pas définir ce paramètre, car il peut provoquer des problèmes d'interopérabilité si les informations d'identification ne sont pas configurées correctement sur le KDC et le serveur.
- Sur le serveur, vous pouvez contrôler les types de chiffrement acceptés par le serveur avec le paramètre `permitted_etypes` de `kdc.conf`. De plus, vous pouvez spécifier les types de chiffrement utilisés lors de la création d'entrées `keytab`. Encore une fois, il est généralement préférable de ne pas utiliser l'une de ces méthodes pour contrôler les types de chiffrement et de laisser le KDC déterminer les types de chiffrement à utiliser, car le KDC ne communique pas avec l'application de serveur pour déterminer la clé ou le type de chiffrement à utiliser.

## Utilisation de la table gsscred

La table `gsscred` est utilisée par un serveur NFS lorsque le serveur tente d'identifier un utilisateur Kerberos, si les mappages par défaut ne sont pas suffisants. Le service NFS utilise des ID UNIX pour identifier les utilisateurs. Ces ID ne font pas partie d'un principal ou d'informations d'identification d'utilisateur. La table `gsscred` assure le mappage supplémentaires d'informations d'identification GSS aux UID UNIX (à partir du fichier de mots de passe). La table doit être créée et administrée une fois que la base de données KDC est remplie. Pour plus d'informations, reportez-vous à la section [“Mappage d'informations d'identification GSS sur des informations d'identification UNIX”](#) à la page 368.

Lorsqu'une demande de client arrive, le service NFS tente de faire correspondre le nom des informations d'identification avec un ID UNIX. Si le mappage échoue, la table `gsscred` est vérifiée.

## Différences notables entre Oracle Solaris Kerberos et MIT Kerberos

La version Solaris 10 du service Kerberos est basée sur la version 1.2.1 de MIT Kerberos. Le tableau suivant répertorie les améliorations incluses dans la version Solaris 10 et pas dans la version MIT 1.2.1 :

- Prise en charge par Kerberos des applications distantes Oracle Solaris
- Propagation incrémentielle pour la base de données KDC
- Script de configuration client
- Messages d'erreur localisés
- Prise en charge des enregistrements d'audit BSM
- Utilisation à thread sécurisé de Kerberos par le biais de GSS-API
- Utilisation de la structure de chiffrement pour la cryptographie

Cette version comprend également certaines corrections de bogues post-MIT 1.2.1. En particulier, les corrections de bogues btree 1.2.5 et l'ajout de la prise en charge du 1.3 TCP ont été ajoutés.



## PARTIE VII

# Audit dans Oracle Solaris

Cette section fournit des informations sur la configuration, la gestion et l'utilisation du sous-système d'audit.

- [Chapitre 26, “Audit \(présentation\)”](#)
- [Chapitre 27, “Planification de l'audit”](#)
- [Chapitre 28, “Gestion de l'audit \(tâches\)”](#)
- [Chapitre 29, “Audit \(référence\)”](#)



## Audit (présentation)

---

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

- “Description de l'audit” à la page 551
- “Terminologie et concepts de l'audit” à la page 552
- “Rapports entre l'audit et la sécurité” à la page 561
- “Fonctionnement de l'audit” à la page 562
- “Configuration de l'audit” à la page 563
- “Audit sur un système à zones Oracle Solaris” à la page 564
- “A propos du service d'audit dans cette version” à la page 565

Pour obtenir des suggestions de planification, reportez-vous au [Chapitre 27, “Planification de l'audit”](#). Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au [Chapitre 28, “Gestion de l'audit \(tâches\)”](#). Pour obtenir des informations de référence, reportez-vous au [Chapitre 29, “Audit \(référence\)”](#).

## Description de l'audit

L'audit consiste à collecter des données sur l'utilisation des ressources système. Les données d'audit fournissent un enregistrement des événements système ayant trait à la sécurité. Ces données peuvent ensuite être utilisées pour déterminer la responsabilité quant aux actions survenant sur un hôte. Un audit réussi commence par deux fonctions de sécurité : identification et authentification. A chaque connexion, une fois qu'un utilisateur fournit un nom d'utilisateur et que l'authentification PAM réussit, un *ID utilisateur d'audit* 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 effectue les opérations suivantes :

- Surveillance des événements liés à la sécurité survenant sur l'hôte
- Enregistrement des événements dans une piste d'audit à l'échelle du réseau
- Détection des utilisations inappropriées et des activités non autorisées
- Examen des modèles d'accès et des historiques d'accès des individus et des objets
- Identification des tentatives de contournement des mécanismes de protection
- Détection de l'utilisation étendue d'un privilège survenant lorsqu'un utilisateur change d'identité

## 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              | <p>Groupe d'événements d'audit. Les classes d'audit permettent de sélectionner un groupe d'événements à auditer.</p> <p>Pour plus d'informations, reportez-vous à la section “<a href="#">Classes d'audit et présélection</a>” à la page 555 et aux pages de manuel <a href="#">audit_flags(5)</a>, <a href="#">audit_class(4)</a> et <a href="#">audit_event(4)</a>.</p> |
| système de fichiers d'audit | <p>Référentiel de fichiers d'audit au format binaire.</p> <p>Pour plus d'informations, reportez-vous à la section “<a href="#">Journaux d'audit</a>” à la page 558 et à la page de manuel <a href="#">audit.log(4)</a>.</p>                                                                                                                                               |
| événement d'audit           | <p>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.</p> <p>Pour plus d'informations, reportez-vous à la section “<a href="#">Événements d'audit</a>” à la page 554 et à la page de manuel <a href="#">audit_event(4)</a>.</p>                              |
| indicateur d'audit          | <p>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 (^)</p>                                                                                                         |



précédant les symboles plus ou moins 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 648.

#### 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 plug-in d'audit](#)” à la page 557 et aux pages de manuel de 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. Ces options permettent notamment d'indiquer si certains types de données d'audit doivent être enregistrés ou pas. Elles permettent aussi de préciser si les actions auditables doivent être suspendues ou pas lorsque la file d'attente d'audit est saturée.

Pour plus d'informations, reportez-vous à la section “[Assimilation des concepts de stratégie d'audit](#)” à la page 573 et à la page de manuel [auditconfig\(1M\)](#).

#### enregistrement d'audit

Données d'audit recueillies 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 557 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 654 et à la page de manuel [audit.log\(4\)](#).

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| piste d'audit | <p>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 <code>audit_binfile</code>.</p> <p>Pour plus d'informations, reportez-vous à la section “<a href="#">Piste d'audit</a>” à la page 652.</p>                                                                                                                                                                                                                                      |
| postsélection | <p>Sélection des événements d'audit à examiner dans la piste d'audit. Le plug-in actif par défaut <code>audit_binfile</code> crée la piste d'audit. Un outil de postsélection, la commande <code>auditreduce</code>, sélectionne les enregistrements dans la piste d'audit.</p> <p>Pour plus d'informations, reportez-vous aux pages de manuel <a href="#">auditreduce(1M)</a> and <a href="#">praudit(1M)</a>.</p>                                                                                                                               |
| présélection  | <p>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.</p> <p>Pour plus d'informations, reportez-vous à la section “<a href="#">Classes d'audit et présélection</a>” à la page 555 et aux pages de manuel <a href="#">audit_flags(5)</a> et <a href="#">auditconfig(1M)</a>.</p>       |
| objet public  | <p>Fichier appartenant à l'utilisateur <code>root</code> et lisible par tout le monde. Par exemple, les fichiers des répertoires <code>/etc</code> et <code>/usr/bin</code> 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 <code>file_read(fr)</code> 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 <code>public</code>.</p> |

## Événements d'audit

Actions système pouvant être auditées. 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 :

|                    |        |                              |
|--------------------|--------|------------------------------|
| 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 :

- **Événements 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.
- **Événements non attribuables** : événements se produisant au niveau d'interruption du noyau ou avant l'authentification d'un utilisateur. La classe d'audit ne 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.
- **Événements synchrones** : événements associés à un processus dans le système. Les événements synchrones constituent la majorité des événements système.
- **Événements asynchrones** : événements associés à aucun processus, de sorte qu'aucun processus ne peut être bloqué puis réactivé ultérieurement. 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 ou plusieurs *classes d'audit*. Les classes d'audit sont des conteneurs pratiques pour les grands nombres d'événements d'audit. Lorsque vous *présélectionnez* une classe 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 651. Pour connaître quels indicateurs d'audit configurés sont utilisés, reportez-vous à la section “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la page 217.

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 :

```
0x00000000000001000:lo:login or logout
0x00000000000100000: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 plus d'informations sur cette procédure, reportez-vous à la section “[Procédure de modification de l'appartenance à une classe d'un événement d'audit](#)” à la page 596. 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* consigne l'occurrence d'un seul événement audité. L'enregistrement inclut des informations telles que l'auteur de l'action, les fichiers affectés, l'action tentée, ainsi que l'endroit et l'heure à laquelle l'action s'est produite. L'exemple suivant montre un enregistrement d'audit `login` :

```
header,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`.

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

## Modules plug-in d'audit

Vous pouvez spécifier les modules enfichables (plug-ins) d'audit qui gèrent les enregistrements placés par votre présélection dans la file d'attente d'audit. 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 configurer un plug-in, reportez-vous à la page de manuel [auditconfig\(1M\)](#) Pour obtenir des exemples de configuration de plug-in, reportez-vous aux tâches décrites dans la section “[Configuration des journaux d'audit \(tâches\)](#)” à la page 597.

Pour plus d'informations sur les plug-ins, reportez-vous 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 manière à recueillir les enregistrements d'audit dans 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, qu'ils utilisent le mode `syslog`, ou qu'ils utilisent n'importe quelle combinaison de ces modes. Le tableau suivant compare les enregistrements d'audit binaires et les enregistrements `syslog`.

**TABLERAU 26-1** Comparaison des enregistrements d'audit binaires, distants et `syslog`

| Fonction                  | Enregistrements binaires et distants                                                             | Enregistrements <code>syslog</code>                |
|---------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Protocole                 | Binaire : écrit dans le système de fichiers<br><br>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 |

TABLEAU 26-1 Comparaison des enregistrements d'audit binaires, distants et syslog (Suite)

| Fonction      | Enregistrements binaires et distants                                                                                                                                                                              | Enregistrements syslog                                                                                              |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Emplacement   | Binaire : stocké dans un zpool sur le système<br><br>Distant : référentiel distant                                                                                                                                | Stockés dans un emplacement spécifié dans le fichier <code>syslog.conf</code>                                       |
| Configuration | Binaire : définir l'attribut <code>p_dir</code> sur le plug-in <code>audit_binfile</code><br><br>Distant : définir l'attribut <code>p_hosts</code> sur le plug-in <code>audit_remote</code> et activer le plug-in | Activer le plug-in <code>audit_syslog</code> et configurer le fichier <code>syslog.conf</code>                      |
| Lecture       | Binaire : en général, en mode batch, sortie navigateur au format XML<br><br>Distant : le référentiel dicte la procédure                                                                                           | En temps réel ou recherché par des scripts que vous avez créés pour <code>syslog</code><br><br>Sortie en texte brut |
| Exhaustivité  | Exhaustivité garantie et affichage dans l'ordre approprié                                                                                                                                                         | Exhaustivité non garantie                                                                                           |
| Horodatage    | Temps universel (UTC)                                                                                                                                                                                             | Heure du système audité                                                                                             |

Des enregistrements binaires offrent la plus grande sécurité et la meilleure couverture. La sortie binaire répond aux exigences de certifications de sécurité, telles que les 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.

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. D'autre part, lorsque les enregistrements d'audit sont stockés à distance, ceux-ci sont susceptibles de faire l'objet

d'attaques réseau, telles que le déni de service et l'usurpation d'adresses source. En outre, UDP peut couper des paquets ou les distribuer dans le désordre. Le nombre limite de caractères pour les entrées `syslog` est de 1024, de sorte que certains enregistrements d'audit peuvent être tronqués dans le journal. Sur un système, tous les enregistrements d'audit ne sont pas collectés. Les enregistrements peuvent ne pas s'afficher dans l'ordre. Dans la mesure où chaque enregistrement d'audit est indiqué avec la date et l'heure du système local, vous ne pouvez pas vous fier à l'horodatage pour créer une piste d'audit pour plusieurs systèmes.

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

- La page de manuel [audit\\_binfile\(5\)](#)
- La page de manuel [audit\\_syslog\(5\)](#)
- La page de manuel [audit.log\(4\)](#)
- “Procédure d'affectation de l'espace d'audit pour la piste d'audit” à la page 601
- “Procédure de configuration des journaux d'audit `syslog`” à la page 605

## Stockage et gestion de la piste d'audit

Lorsque le plug-in `audit_binfile` est actif, un *système de fichiers d'audit* détient 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 “[Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit](#)” à la page 598.

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 racine d'audit par défaut est `/var/audit`. L'option `-M` de la commande `auditreduce` et l'option `-S` peuvent être utilisées pour spécifier les fichiers d'audit à partir d'un ordinateur spécifique et un autre système de fichiers d'audit, respectivement. 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 *Administration d'Oracle Solaris : Services réseau* et à la page de manuel `xntpd(1M)`.

## Gestion d'un référentiel distant

Lorsque le plug-in `audit_remote` est actif, le référentiel distant gère les enregistrements d'audit.

# 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 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 le [Chapitre 27](#), “Planification de l'audit” et le [Chapitre 28](#), “Gestion de l'audit (tâches)”.

L'audit ne peut pas empêcher les pirates d'entrer dans le système de manière non autorisée. Cependant, le service d'audit permet par exemple de générer des rapports indiquant qu'un utilisateur spécifique a effectué certaines actions à une heure et une date données. Le rapport d'audit peut identifier l'utilisateur par le biais du chemin d'entrée et du nom de l'utilisateur. Ces informations peuvent être envoyées immédiatement à votre terminal et signalées dans un fichier pour une analyse ultérieure. Par conséquent, le service d'audit fournit des données permettant de déterminer les éléments suivants :

- La manière dont la sécurité du système a été compromise.
- Les brèches à combler pour assurer le niveau de sécurité souhaité.

## Fonctionnement de l'audit

L'audit génère des enregistrements d'audit lorsque des événements donnés se produisent. Le plus souvent, les événements générant des enregistrements d'audit sont les suivants :

- Démarrage et arrêt du système
- Connexion et déconnexion
- Création ou destruction de processus et création ou destruction de threads
- Ouverture, fermeture, création, destruction, ou modification du nom d'objets
- Utilisation des capacités de privilège ou du contrôle d'accès basé sur les rôles (RBAC)
- Actions d'identification et d'authentification
- Modification d'autorisations par un processus ou un utilisateur
- Actions d'administration, telles que l'installation d'un package
- Applications spécifiques à un site

Les enregistrements d'audit sont générés à partir de trois sources :

- Par une application
- 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 pour les *plug-ins* actifs. Au moins un *plug-in* doit être actif, bien que tous puissent l'être.

Par défaut, un seul *plug-in* est actif. Il s'agit du *plug-in* `audit_binfile`, qui écrit les enregistrements d'audit dans les fichiers d'audit. Ces fichiers sont stockés localement au format binaire. Un *plug-in* `audit_remote` actif envoie ces enregistrements à un référentiel distant. Un *plug-in* `audit_syslog` actif envoie des résumés au format texte à l'utilitaire `syslog`. Pour obtenir un exemple, reportez-vous à la [Figure 26–1](#).

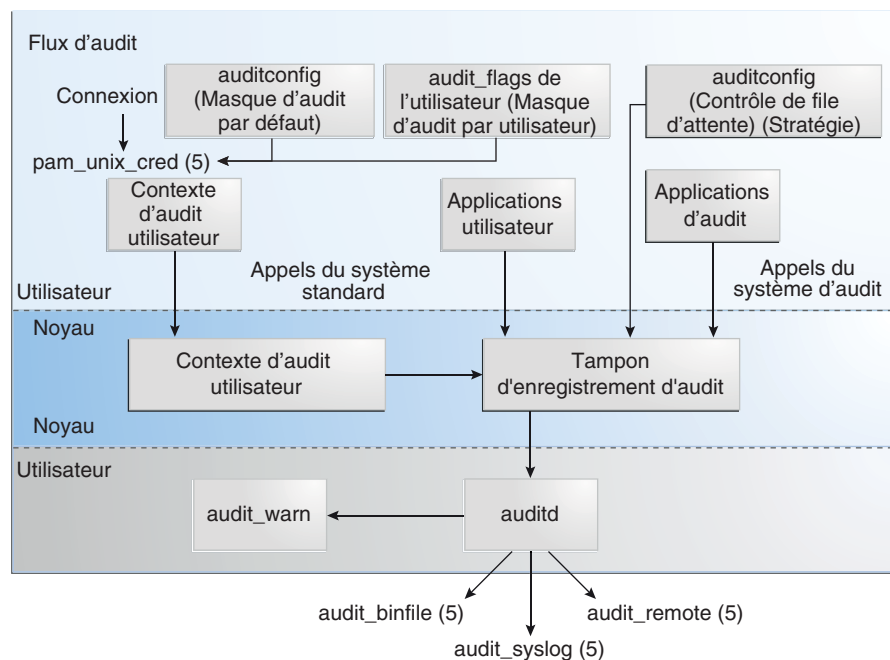
Lorsqu'ils sont stockés en local, les fichiers d'audit peuvent résider dans un ou plusieurs pools ZFS. Les pools ZFS facilitent la gestion du stockage local. Ils peuvent résider sur différents systèmes et sur des réseaux différents mais liés. L'ensemble des fichiers d'audit liés est considéré comme une *piste d'audit*.

Pour plus d'informations, reportez-vous aux sections “[Configuration de l'audit](#)” à la page 563, “[Journaux d'audit](#)” à la page 558 et “[Modules plug-in d'audit](#)” à la page 557.

## 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 26-1 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`. Les outils de post-sélection vous permettent d'examiner des parties intéressantes de la 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 zones Oracle Solaris” à la page 647](#).

## Audit sur un système à zones Oracle Solaris

Une zone non globale représente un environnement virtualisé du système d'exploitation, créé dans une seule instance du SE Oracle Solaris. Le service d'audit contrôle le système dans sa totalité, y compris les activités dans les zones. Un système doté de zones non globales peut exécuter un service d'audit pour contrôler toutes les zones de manière identique. Il peut également 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 personnalisés.

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 personnalisés. Ces différents domaines administratifs fonctionnent généralement comme des serveurs.

- Des administrateurs de zones particulières souhaitent contrôler l'audit dans les zones qu'ils gèrent. En procédant à un audit par zone, les administrateurs de zones peuvent décider d'activer ou de désactiver l'audit de la zone qu'ils gèrent.

Les avantages de l'audit par zone sont la fourniture d'une piste d'audit personnalisée pour chaque zone et la possibilité de désactiver l'audit en fonction de la zone. En revanche, ces avantages peuvent impliquer un temps système d'administration. 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.

## A propos du service d'audit dans cette version

Les fonctions d'audit suivantes ont été introduites :

- L'audit est un service. Reportez-vous à la section [“Service d'audit” à la page 643](#).
- L'audit est activé par défaut.
- Il n'est pas nécessaire de procéder à une réinitialisation lorsque le service d'audit est activé ou désactivé.
- La commande `auditconfig` permet d'afficher et de modifier la stratégie d'audit, les indicateurs non attribuables, les indicateurs attribuables, les plug-ins et les contrôles de file d'attente. Reportez-vous à la page de manuel [auditconfig\(1M\)](#).
- L'audit des objets publics génère moins de bruit dans la piste d'audit.
- L'audit des événements de non noyau n'a aucune incidence sur les performances.
- Par défaut, les événements dans la classe `login/logout` font l'objet d'un audit pour le système et pour le compte `root`.
- Oracle Solaris fournit trois plug-ins : `audit_binfile`, `audit_remote` et `audit_syslog`. Reportez-vous aux pages de manuel correspondantes [audit\\_binfile\(5\)](#), [audit\\_remote\(5\)](#) et [audit\\_syslog\(5\)](#).
- Les zones non globales peuvent être soumises à un audit sans que ce soit le cas de la zone globale. Pour effectuer l'audit des zones non globales, il suffit que la stratégie d'audit `perzone` soit définie dans la zone globale.
- Le nombre de classes d'audit possible passe de 32 à 64. Les huit premiers bits de haut niveau sont réservés aux clients.
- Les profils de droits d'audit ont été reconfigurés. Reportez-vous à la section [“Profils de droits pour l'administration de l'audit” à la page 646](#).
- L'attribut de sécurité `audit_flags` permet de configurer les différences utilisateur par rapport à l'audit du système. Ce mot-clé est un argument des commandes `useradd`, `usermod`, `roleadd` et `rolemod`. La valeur `audit_flags` est stockée dans la base de données `user_attr`. Reportez-vous aux pages de manuel [useradd\(1M\)](#), [usermod\(1M\)](#), [roleadd\(1M\)](#), [rolemod\(1M\)](#) et [user\\_attr\(4\)](#).

Les mots-clés `always_audit` et `never_audit` de la commande `profils` mettent à jour l'attribut de sécurité `audit_flags` dans la base de données `prof_attr`. Pour plus d'informations, reportez-vous à la page de manuel [profiles\(1\)](#) et à la section “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la page 217.

- De nouvelles classes d'audit sont définies. La classe d'audit `ft` contient les événements d'audit de transfert de fichiers. Les commandes `ftp` et `sftp` font partie des événements qui font l'objet d'un audit par cette classe. La classe d'audit `frcp` contient les événements d'audit enregistrés, qu'ils soient ou non présélectionnés par un administrateur. La commande `auditrecord -c classname` décrit les événements d'audit dans ces nouvelles classes.

## Planification de l'audit

---

Ce chapitre décrit les procédures de personnalisation du service d'audit pour votre installation Oracle Solaris. Vous trouverez ci-après une liste des informations relatives à la planification citées dans ce chapitre :

- “Planification de l'audit (tâches)” à la page 567
- “Assimilation des concepts de stratégie d'audit” à la page 573
- “Contrôle des coûts d'audit” à la page 576
- “Gestion efficace de l'audit” à la page 578

Pour une présentation de l'audit, reportez-vous au [Chapitre 26, “Audit \(présentation\)”](#). Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au [Chapitre 28, “Gestion de l'audit \(tâches\)”](#). Pour obtenir des informations de référence, reportez-vous au [Chapitre 29, “Audit \(référence\)”](#).

### Planification de l'audit (tâches)

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.

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

| Tâche                                                             | Voir                                                                           |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Détermination de la stratégie d'audit pour les zones non globales | <a href="#">“Procédure de planification de l'audit par zone” à la page 568</a> |

| Tâche                                                       | Voir                                                                                                    |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Planification de l'espace de stockage pour la piste d'audit | <a href="#">“Procédure de planification du stockage pour les enregistrements d'audit” à la page 569</a> |
| Détermination des personnes et objets à auditer             | <a href="#">“Procédure de planification des personnes et objets à auditer” à la page 570</a>            |

## ▼ Procédure de planification de l'audit par zone

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 à zones Oracle Solaris” à la page 564](#).

- **Procédez de l'une des manières suivantes :**

- **OPTION 1 : configuration d'un service d'audit pour toutes les zones.**

L'audit de toutes les zones de façon identique peut créer une piste d'audit à image unique. Une piste d'audit à image unique 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 pour chaque zone non globale.

- a. **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 la stratégie `per zone` 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.

---

- b. **Activez les enregistrements d'audit, y compris 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 `audit reduce` peut alors



sélectionner les événements d'audit par zone dans la piste d'audit. Pour un exemple, reportez-vous à la page de manuel [audit reduce\(1M\)](#).

Pour planifier une piste d'audit à image unique, reportez-vous à la section “[Procédure de planification des personnes et objets à auditer](#)” à la page 570. Commencez à la première étape. L'administrateur de la zone globale doit également réserver du stockage, comme décrit dans la section “[Procédure de planification du stockage pour les enregistrements d'audit](#)” à la page 569.

#### ■ **OPTION 2 : configuration 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 à partir 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 “[Procédure de configuration de l'audit par zone](#)” à la page 609.
- 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 ahl t.
- 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.

Pour planifier l'audit par zone, reportez-vous à la section “[Procédure de planification des personnes et objets à auditer](#)” à la page 570. Vous pouvez ignorer la première étape. Si le plug-in audit\_binfile est actif, les administrateurs de zone doivent également réserver de l'espace de stockage pour chaque zone, comme décrit à la section “[Procédure de planification du stockage pour les enregistrements d'audit](#)” à la page 569.

## ▼ **Procédure de planification du stockage 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.

**Avant de commencer**

Si vous mettez en oeuvre des zones non globales, effectuez la [“Procédure de planification de l'audit par zone” à la page 568](#) avant d'utiliser cette procédure.

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 576](#) et [“Gestion efficace de l'audit” à la page 578](#).

Les sections [“Procédure d'atténuation du volume des enregistrements d'audit produits” à la page 629](#), [“Procédure de compression des fichiers d'audit sur un système de fichiers dédié” à la page 638](#) et [Exemple 28–28](#) décrivent dans le détail les étapes à suivre.

**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. La section [“Stockage et gestion de la piste d'audit” à la page 560](#) et la page de manuel [audit\\_reduce\(1M\)](#) contiennent des directives pour la configuration. Pour spécifier les systèmes de fichiers d'audit, reportez-vous à la section [“Procédure d'affectation de l'espace d'audit pour la piste d'audit” à la page 601](#).

**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 561](#).

## ▼ Procédure de planification des personnes et objets à auditer

**Avant de commencer**

Si vous mettez en oeuvre des zones non globales, consultez la section [“Procédure de planification de l'audit par zone” à la page 568](#) avant d'utiliser cette procédure.

**1 Déterminez si vous souhaitez une piste d'audit d'image système unique.**

---

**Remarque** – Cette étape 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. Si vos systèmes utilisent différents services de noms, commencez par l'[Étape 2](#). Ensuite, effectuez le reste des étapes de planification pour chaque système.

Pour créer une piste d'audit d'image système unique pour un site, chaque système dans l'installation doit être configuré 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 obtenir 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.

## 2 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 “[Assimilation des concepts de stratégie d'audit](#)” à la page 573.
- Pour connaître l'effet de la stratégie `cnt`, reportez-vous à la section “[Stratégies d'audit des événements asynchrones et synchrones](#)” à la page 650.
- Pour définir la stratégie d'audit, reportez-vous à la section “[Procédure de modification de la stratégie d'audit](#)” à la page 590.

## 3 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 “[Procédure de modification de l'appartenance à une classe d'un événement d'audit](#)” à la page 596 présente un exemple.

## 4 Déterminez les classes d'audit à présélectionner.

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

Les classes d'audit que vous présélectionnez avec les options `-setflags` et `-setnaflags` de 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, consultez le fichier `/etc/security/audit_class`.

## 5 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, utilisez l'attribut de sécurité `audit_flags` de la commande `useradd`, `usermod`, `roleadd` ou `rolemod`. Vous pouvez également utiliser la commande `profiles` pour ajouter cet attribut à un profil de droits dans la base de données `prof_attr`. Le masque de présélection utilisateur est modifié pour les utilisateurs qui utilisent un profil de droits avec des indicateurs d'audit explicites.

Pour obtenir cette procédure, reportez-vous à la section “[Procédure de configuration des caractéristiques d'audit d'un utilisateur](#)” à la page 586. Pour connaître les valeurs d'indicateur d'audit en vigueur, reportez-vous à la section “[Ordre de recherche pour les attributs de sécurité affectés](#)” à la page 217.

## 6 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 “[Procédure de configuration de l'alias de messagerie `audit\_warn`](#)” à la page 594.

## 7 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 “[Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit](#)” à la page 598.
- 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 fichiers. Pour obtenir cette procédure, reportez-vous à la section “[Procédure d'envoi des fichiers d'audit à un référentiel distant](#)” à la page 604.
- 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 “[Procédure de configuration des journaux d'audit `syslog`](#)” à la page 605.

Pour obtenir une comparaison des formats binaire et `syslog`, reportez-vous à la section “[Journaux d'audit](#)” à la page 558.

## 8 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 définir un pourcentage d'espace libre minimal, reportez-vous à l'[Exemple 28–17](#).

## 9 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.

Pour une description de ces options de stratégie, reportez-vous à la section “[Stratégies d'audit des événements asynchrones et synchrones](#)” à la page 650. Pour configurer ces options de stratégie, reportez-vous à l'[Exemple 28–6](#).

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.

---

**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.

---

# Assimilation des concepts de 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 plusieurs options de stratégie d'audit.

TABLEAU 27–1 Effets des options de stratégie d'audit

| Nom de la stratégie | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Pourquoi modifier l'option de stratégie                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ahl t               | <p>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.</p> <p>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.</p> | <p>L'option désactivée est judicieuse lorsque la disponibilité du système est plus importante que la sécurité.</p> <p>L'option activée est opportune dans un environnement où la sécurité est primordiale. Pour obtenir de plus amples renseignements, reportez-vous à la section <a href="#">“Stratégies d'audit des événements asynchrones et synchrones”</a> à la page 650.</p>                                                                                                               |
| arge                | <p>Lorsqu'elle est désactivée, cette stratégie omet les variables d'environnement d'un programme exécuté dans l'enregistrement d'audit excecve.</p> <p>Lorsqu'elle est activée, cette stratégie ajoute les variables d'environnement d'un programme exécuté à l'enregistrement d'audit excecve. Les enregistrements d'audit qui en résultent contiennent beaucoup plus de détails que lorsque cette stratégie est désactivée.</p>                                                                                                                                                                        | <p>L'option désactivée collecte beaucoup moins d'informations que l'option activée. Pour obtenir une comparaison, reportez-vous à la section <a href="#">“Procédure d'audit de toutes les commandes par les utilisateurs”</a> à la page 631.</p> <p>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.</p> |
| argv                | <p>Lorsqu'elle est désactivée, cette stratégie omet les arguments d'un programme exécuté dans l'enregistrement d'audit excecve.</p> <p>Lorsqu'elle est activée, cette stratégie ajoute les arguments d'un programme exécuté pour l'enregistrement d'audit excecve. Les enregistrements d'audit qui en résultent contiennent beaucoup plus de détails que lorsque cette stratégie est désactivée.</p>                                                                                                                                                                                                     | <p>L'option désactivée collecte beaucoup moins d'informations que l'option activée. Pour obtenir une comparaison, reportez-vous à la section <a href="#">“Procédure d'audit de toutes les commandes par les utilisateurs”</a> à la page 631.</p> <p>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.</p>              |

TABLEAU 27-1 Effets des options de stratégie d'audit (Suite)

| Nom de la stratégie | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Pourquoi modifier l'option de stratégie                                                                                                                                                                                                                                                                                                                                            |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cnt                 | <p>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.</p> <p>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.</p>                                                                                                         | <p>L'option désactivée est opportune dans un environnement où la sécurité est primordiale.</p> <p>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 "<a href="#">Stratégies d'audit des événements asynchrones et synchrones</a>" à la page 650.</p> |
| group               | <p>Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de liste de groupes aux enregistrements d'audit.</p> <p>Lorsqu'elle est activée, cette stratégie ajoute une liste de groupes à chaque enregistrement d'audit en tant que jeton spécial.</p>                                                                                                                                                                                                                                                                                                                                       | <p>L'option désactivée répond généralement aux exigences de sécurité du site.</p> <p>L'option activée est utile lorsque vous avez besoin d'auditer les groupes supplémentaires auquel subject appartient.</p>                                                                                                                                                                      |
| path                | <p>Lorsqu'elle est désactivée, cette stratégie consigne dans un enregistrement d'audit au maximum un chemin utilisé au cours d'un appel système.</p> <p>Lorsqu'elle est activée, cette stratégie enregistre chaque chemin d'accès utilisé en association avec un événement d'audit pour chaque enregistrement d'audit.</p>                                                                                                                                                                                                                                                                    | <p>L'option désactivée place au maximum un chemin d'accès dans un enregistrement d'audit.</p> <p>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.</p>                                                                                                                      |
| perzone             | <p>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.</p> <p>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.</p> | <p>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.</p> <p>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.</p>         |
| public              | <p>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.</p> <p>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.</p>                                                                                                                         | <p>L'option désactivée répond généralement aux exigences de sécurité du site.</p> <p>L'option activée est rarement utilisée.</p>                                                                                                                                                                                                                                                   |

TABLEAU 27-1 Effets des options de stratégie d'audit (Suite)

| Nom de la stratégie | Description                                                                                                                                                                                                                                                                                         | Pourquoi modifier l'option de stratégie                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| seq                 | <p>Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de numéro de séquence à chaque enregistrement d'audit.</p> <p>Lorsqu'elle est activée, cette stratégie ajoute un numéro de séquence à chaque enregistrement d'audit. Le jeton <code>sequence</code> contient le numéro de séquence.</p> | <p>L'option désactivée est suffisante lorsque l'audit s'exécute correctement.</p> <p>L'option activée est utile lorsque la stratégie <code>cnt</code> est activée. La stratégie <code>seq</code> vous permet de déterminer si des données ont été supprimées. Vous pouvez également utiliser la commande <code>auditstat</code> pour visualiser les enregistrements rejetés.</p>        |
| trailer             | <p>Lorsqu'elle est désactivée, cette stratégie n'ajoute pas de jeton <code>trailer</code> aux enregistrements d'audit.</p> <p>Lorsqu'elle est activée, cette stratégie ajoute un jeton <code>trailer</code> à chaque enregistrement d'audit.</p>                                                    | <p>L'option désactivée crée un enregistrement d'audit de plus petite taille.</p> <p>L'option activée marque clairement la fin de chaque enregistrement d'audit avec un jeton <code>trailer</code>. Le jeton <code>trailer</code> est souvent utilisé avec le jeton <code>sequence</code>. Le jeton <code>trailer</code> contribue à la restauration des pistes d'audit endommagées.</p> |
| zonename            | <p>Lorsqu'elle est désactivée, cette stratégie n'inclut pas de jeton <code>zonename</code> dans les enregistrements d'audit.</p> <p>Lorsqu'elle est activée, cette stratégie comprend un jeton <code>zonename</code> dans chaque enregistrement d'audit.</p>                                        | <p>L'option désactivée est utile lorsque vous n'avez pas besoin d'effectuer le suivi du comportement d'audit par zone.</p> <p>L'option activée est utile lorsque vous souhaitez isoler et comparer le comportement d'audit des différentes zones par post-sélection des enregistrements en fonction de la zone.</p>                                                                     |

## 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, à moins que les événements du noyau ne soient présélectionnés, le noyau n'a aucun impact mesurable sur les performances du système au-delà de l'impact du service d'audit.

## 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 des 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 577](#) et [“Gestion efficace de l'audit” à la page 578](#) 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
- Niveau 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.

Basez votre philosophie sur des mesures raisonnables. De telles mesures incluent le niveau de traçabilité requis par votre site et les types d'utilisateurs que vous administrez.

## Gestion efficace de l'audit

Les techniques suivantes peuvent vous aider à atteindre les objectifs de sécurité de votre organisation tout en améliorant l'efficacité de l'audit.

- 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.
- Surveillez 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 surveiller certaines activités dans la piste d'audit. Vous pouvez écrire un script pour déclencher une augmentation automatique de l'audit de certains utilisateurs ou systèmes en réponse à la détection d'événements inhabituels.

Par exemple, vous pouvez écrire un script effectuant les opérations suivantes :

1. Surveillance de la création des fichiers d'audit sur 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.



## Gestion de l'audit (tâches)

Ce chapitre fournit les procédures pour vous aider à configurer et gérer l'audit sur un système Oracle Solaris. Ce chapitre comprend également des instructions pour l'administration de la piste d'audit et le dépannage du service d'audit. Vous trouverez ci-après une liste des informations citées dans ce chapitre.

- “Gestion de l'audit (liste des tâches)” à la page 581
- “Configuration du service d'audit (tâches)” à la page 582
- “Configuration des journaux d'audit (tâches)” à la page 597
- “Configuration du service d'audit dans les zones (tâches)” à la page 607
- “Activation et désactivation du service d'audit (tâches)” à la page 611
- “Gestion des enregistrements d'audit sur les systèmes locaux (tâches)” à la page 615
- “Dépannage du service d'audit (tâches)” à la page 626

Pour obtenir une présentation générale du service d'audit, reportez-vous au [Chapitre 26, “Audit \(présentation\)”](#). Pour obtenir des suggestions de planification, reportez-vous au [Chapitre 27, “Planification de l'audit”](#). Pour obtenir des informations de référence, reportez-vous au [Chapitre 29, “Audit \(référence\)”](#).

### Gestion de l'audit (liste des tâches)

La liste des tâches suivante présente les principales tâches nécessaires à la gestion de l'audit. A l'exception de la section concernant le dépannage, les tâches sont décrites dans l'ordre.

| Tâche                       | Description                                                                                                | Voir                                                              |
|-----------------------------|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1. Planification de l'audit | Vous devez prendre un certain nombre de décisions avant de procéder à la configuration du service d'audit. | <a href="#">“Planification de l'audit (tâches)” à la page 567</a> |

| Tâche                                   | Description                                                                                                                                                                                                                           | Voir                                                                                                           |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 2. Configuration de l'audit             | Vous définissez les événements d'audit qui seront enregistrés pour les utilisateurs et les systèmes. Le cas échéant, vous modifiez la stratégie d'audit, les mappages classe-événement d'audit et les contrôles de la file d'attente. | <a href="#">“Configuration du service d'audit (liste des tâches)” à la page 582</a>                            |
|                                         | Vous configurez les plug-ins, qui déterminent l'emplacement de stockage des enregistrements d'audit et leur format.                                                                                                                   | <a href="#">“Configuration des journaux d'audit (tâches)” à la page 597</a>                                    |
| 3. Activation de l'audit                | Vous démarrez le service d'audit.<br>Vous arrêtez le service d'audit.                                                                                                                                                                 | <a href="#">“Activation et désactivation du service d'audit (tâches)” à la page 611</a>                        |
|                                         | Sur un hôte doté de zones non globales, un service d'audit s'exécute par zone. Vous pouvez également utiliser le service d'audit de la zone globale.                                                                                  | <a href="#">“Configuration du service d'audit dans les zones (tâches)” à la page 607</a>                       |
| 4. Gestion des enregistrements d'audit. | Vous recueillez et analysez les données d'audit de la piste d'audit.                                                                                                                                                                  | <a href="#">“Gestion des enregistrements d'audit sur les systèmes locaux (liste des tâches)” à la page 615</a> |
| Dépannage de l'audit.                   | Vous résolvez les problèmes liés au service d'audit.                                                                                                                                                                                  | <a href="#">“Dépannage du service d'audit (tâches)” à la page 626</a>                                          |

## Configuration du service d'audit (tâches)

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 zones Oracle Solaris” à la page 647](#). Pour la planification, reportez-vous à la section [“Procédure de planification de l'audit par zone” à la page 568](#). Pour plus d'informations sur les procédures, reportez-vous à la section [“Configuration du service d'audit dans les zones \(tâches\)” à la page 607](#).

## Configuration du service d'audit (liste des tâches)

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

| Tâche                                                                                   | Description                                                                                                                                                                                | Voir                                                                                                            |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Affichage des valeurs par défaut de l'audit.                                            | Avant la configuration de l'audit, affiche la stratégie par défaut, les contrôles de file d'attente, les indicateurs et l'utilisation des plug-ins.                                        | <a href="#">“Procédure d'affichage des paramètres par défaut du service d'audit” à la page 583</a>              |
| 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.                               | <a href="#">“Procédure de présélection des classes d'audit” à la page 585</a>                                   |
| Sélection des événements qui font l'objet d'un audit pour des utilisateurs spécifiques. | Définit des exceptions utilisateur aux classes d'audit à l'échelle du système.                                                                                                             | <a href="#">“Procédure de configuration des caractéristiques d'audit d'un utilisateur” à la page 586</a>        |
| Spécification de la stratégie d'audit.                                                  | Définit d'autres données d'audit dont votre site a besoin.                                                                                                                                 | <a href="#">“Procédure de modification de la stratégie d'audit” à la page 590</a>                               |
| 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. | <a href="#">“Procédure de modification des contrôles de file d'attente d'audit” à la page 592</a>               |
| 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.                                                                 | <a href="#">“Procédure de configuration de l'alias de messagerie audit_warn” à la page 594</a>                  |
| Configuration des journaux d'audit.                                                     | Configure l'emplacement des enregistrements d'audit pour chaque plug-in.                                                                                                                   | <a href="#">“Configuration des journaux d'audit (tâches)” à la page 597</a>                                     |
| Ajout des classes d'audit.                                                              | Réduit le nombre d'enregistrements d'audit en créant une nouvelle classe d'audit pour contenir les événements critiques.                                                                   | <a href="#">“Procédure d'ajout d'une classe d'audit” à la page 595</a>                                          |
| Modification des mappages événements-classes.                                           | Réduit le nombre d'enregistrements d'audit en modifiant les mappages événements-classes.                                                                                                   | <a href="#">“Procédure de modification de l'appartenance à une classe d'un événement d'audit” à la page 596</a> |

## ▼ Procédure d'affichage des paramètres par défaut du service d'audit

Les commandes de cette procédure affichent la configuration d'audit en cours. Le résultat de cette procédure est pris d'un système non configuré.

### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) ou Audit Control (contrôle d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175.](#)

**2 Affichez les classes présélectionnées pour les événements attribuables.**

```
# 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*).

**3 Affichez les classes présélectionnées pour les événements non attribuables.**

```
# auditconfig -getnaflags
```

```
active non-attributable audit flags = lo(0x1000,0x1000)
```

```
configured non-attributable audit flags = lo(0x1000,0x1000)
```

---

**Remarque** – 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`.

---

**4 Affichez la stratégie d'audit.**

```
$ 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.

**5 Affichez les informations sur les plug-ins d'audit.**

```
$ auditconfig -getplugin
```

```
Plugin: audit_binfile (active)
```

```
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.

**6 Affichez les 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.



**7 Affichez les classes d'audit présélectionnées pour les utilisateurs existants.**

Recherchez les utilisateurs, puis affichez la valeur d'attribut `audit_flags` de chaque utilisateur.

```
# 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)
...
# userattr audit_flags adoe
# userattr audit_flags jdoe
```

Par défaut, les utilisateurs sont soumis à un audit pour les paramètres à l'échelle du système uniquement.

La commande `userattr` est décrite à la page de manuel [userattr\(1\)](#). Le mot-clé `audit_flags` est décrit à la page de manuel [user\\_attr\(4\)](#).

**▼ Procédure de 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**

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

**2 Déterminez les classes présélectionnées actuelles.**

```
# auditconfig -getflags
...

# auditconfig -getnaflags
...
```

Pour obtenir une explication de la sortie, reportez-vous à la section “[Procédure d'affichage des paramètres par défaut du service d'audit](#)” à la page 583.

**3 Présélectionnez les classes attribuables.**

```
# auditconfig -setflags lo,ps,fw
user default audit flags = ps,lo,fw(0x101002,0x101002)
```

Cette commande effectue des audits des événements dans les classes de connexion/déconnexion, de démarrage/d'arrêt de processus et d'écriture de fichier, portant sur la réussite et l'échec.

---

**Remarque** – La commande `auditconfig -setflags` n'*ajoute* pas de classes aux paramètres par défaut du système. Cette commande *remplace* les paramètres par défaut du système, de sorte que vous devez spécifier toutes les classes que vous souhaitez présélectionner.

---

#### 4 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* les valeurs par défaut du système, de sorte que vous devez spécifier toutes les classes que vous souhaitez présélectionner.

---

## ▼ Procédure de configuration des caractéristiques d'audit d'un utilisateur

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.

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 651.

### Avant de commencer

Vous devez être dans le rôle `root`.

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

##### ■ 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*.

|                     |                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>always-audit</i> | 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, exécutez 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 les attributs de sécurité affectés](#)” à la page 217.

### Exemple 28–1 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, j doe. La classe pf est créée dans l'[Exemple 28–10](#).

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

La commande `userattr` affiche l'ajout.

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

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

```
# auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = ss,pf,lo(0x0100000000000000,0x0100000008011000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

### Exemple 28–2 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 28–3 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 28–10](#).

```
# 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 28-4 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 28-5 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
```

## ▼ Procédure de modification de la stratégie d'audit

La stratégie d'audit détermine les caractéristiques des enregistrements d'audit pour le système local. Il peut être utile de modifier la stratégie d'audit 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

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Affichez la stratégie d'audit actuelle.

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

Pour obtenir une explication de la sortie, reportez-vous à la section [“Procédure d'affichage des paramètres par défaut du service d'audit”](#) à la page 583.

#### 3 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 `perzone` et `ahlt` ne peuvent être définies que dans la zone globale. Pour que les compromis utilisent une option de stratégie particulière, reportez-vous à la section “[Assimilation des concepts de stratégie d'audit](#)” à la page 573.

---

#### 4 Activez ou désactivez les options de stratégie d'audit sélectionnées.

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

**-t**           Facultatif. 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 un 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 28–6 Définition de l'option de stratégie d'audit `ahlt`

Dans cet exemple, la stratégie `cnt` est désactivée et la stratégie `ahlt` est activée. Avec cette configuration, l'utilisation du système est interrompue lorsque les files d'attente d'audit sont complètes et qu'un événement asynchrone se produit. Lorsqu'un événement synchrone se produit, le processus qui a créé le thread se bloque. Cette configuration est appropriée lorsque la sécurité est plus importante que la disponibilité. Pour plus d'informations, reportez-vous à la section “[Stratégies d'audit des événements asynchrones et synchrones](#)” à la page 650.

```
# 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 les paramètres de la stratégie actuelle.

#### Exemple 28–7 Définition d'une stratégie d'audit temporaire

Dans cet exemple, le service d'audit est activé et la stratégie d'audit `ahlt` est configurée. L'administrateur ajoute la stratégie d'audit `trail` à la stratégie active (`+trail`), mais ne

configure pas le service d'audit pour une utilisation permanente de la stratégie d'audit `trail` (`-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 [“Procédure de modification des contrôles de file d'attente d'audit”](#) à la page 592.

### Exemple 28–8 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.

```
$ 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
```

## ▼ Procédure de 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

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.



**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

**2 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 “[Procédure d'affichage des paramètres par défaut du service d'audit](#)” à la page 583.

**3 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
```

Par exemple, définissez la valeur *interval* sur 10 sans définir d'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 `-setqctrl 0 0 0 interval`, comme dans `# auditconfig -setqdelay 10`.

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

**Exemple 28–9 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 modifie 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
```

## ▼ Procédure de 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 être dans le rôle `root`.

#### ● Configurez l'alias de messagerie `audit_warn`.

Procédez de l'une des manières suivantes :

- **OPTION 1** : remplacez l'alias de messagerie `audit_warn` par un autre compte de messagerie dans le script `audit_warn`.

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
```



**Attention** – Lorsque vous effectuez une mise à niveau vers une nouvelle version du SE Oracle Solaris, vous devez fusionner manuellement votre fichier `audit_warn` personnalisé avec le fichier `audit_warn.new`. Ce nouveau fichier peut contenir des modifications importantes. Pour obtenir une description de l'action du fichier `preserve=renamenew` sur la mise à niveau, reportez-vous à la page de manuel `pkg(5)`.

- **OPTION 2** : redirigez l'e-mail `audit_warn` vers un autre compte de messagerie.

Dans ce cas, vous devez ajouter l'alias de messagerie `audit_warn` au fichier d'alias de messagerie approprié. Vous pouvez ajouter l'alias au fichier local `/etc/mail/aliases` ou à la base de données `mail_aliases` de l'espace de noms. L'entrée `/etc/mail/aliases` doit ressembler à ce qui suit si les comptes électroniques `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 `aliases`.

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

## ▼ Procédure d'ajout d'une classe d'audit

Lorsque vous créez votre propre classe d'audit, vous pouvez y placer uniquement les événements que vous souhaitez auditer pour votre site.

Lorsque vous ajoutez la classe sur un seul système, copiez la modification sur tous les systèmes audités. Il est préférable de créer les classes d'audit avant d'activer le service d'audit.



**Attention** – Lorsque vous effectuez une mise à niveau vers une nouvelle version du SE Oracle Solaris, vous devez fusionner manuellement votre fichier `audit_class` personnalisé avec le fichier `audit_class.new`. Ce nouveau fichier peut contenir des modifications importantes. Pour obtenir une description de l'action du fichier `preserve=renamenew` sur la mise à niveau, reportez-vous à la page de manuel `pkg(5)`.

### Avant de commencer

L'entrée doit être unique. Vous devez choisir des bits libres. Les bits disponibles à l'usage du client sont décrits dans le fichier `/etc/security/audit_class`.

Vous devez être dans le rôle `root`.

#### 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 :

```
0x64bitnumber: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 28–10 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 28–11](#) remplit la nouvelle classe d'audit.

**Erreurs  
fréquentes**

Si vous avez personnalisé le fichier `audit_class`, assurez-vous que les exceptions utilisateur éventuelles au masque de présélection d'audit du système sont cohérentes avec les nouvelles classes d'audit. Des erreurs se produisent lorsqu'une valeur `audit_flags` n'est pas un sous-ensemble du fichier `audit_class`.

## ▼ Procédure de 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 utilisateurs ne se connectent.



**Attention** – Lorsque vous effectuez une mise à niveau vers une nouvelle version du SE Oracle Solaris, vous devez fusionner manuellement votre fichier `audit_event` personnalisé avec le fichier `audit_event.new`. Ce nouveau fichier peut contenir des modifications importantes. Pour obtenir une description de l'action du fichier `preserve=renamenew` sur la mise à niveau, reportez-vous à la page de manuel `pkg(5)`.

**Avant de  
commencer**

Vous devez être dans le rôle `root`.

**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.

|                    |                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| <i>description</i> | En règle générale, l'appel système ou l'exécutable qui déclenche la création d'un enregistrement d'audit. |
| <i>class-list</i>  | Liste de classes d'audit séparées par des virgules.                                                       |

### Exemple 28–11 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 28–10](#). Par défaut, l'événement d'audit AUE\_PFEXEC est mappé à quatre classes, ps, ex, ua et as. En créant la nouvelle classe, l'administrateur peut auditer les événements AUE\_PFEXEC sans auditer les événements dans les quatre autres classes.

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

## Configuration des journaux d'audit (tâches)

Deux plug-ins d'audit, `audit_binfile` et `audit_syslog`, envoient des journaux d'audit à des emplacements que vous pouvez configurer. Les tâches suivantes vous aident à configurer ces journaux.

### Configuration des journaux d'audit (liste des tâches)

La liste des tâches suivante indique les procédures de configuration des journaux d'audit pour les différents plug-ins. Toutes les tâches sont facultatives.

| Tâche                                                                          | Description                                                                                                     | Voir                                                                                                        |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Ajout d'espace de stockage local pour le plug-in <code>audit_binfile</code> .  | Crée de l'espace disque local pour les fichiers d'audit et les protège à l'aide d'autorisations de fichiers.    | <a href="#">“Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit” à la page 598</a> |
| Assignation d'espace de stockage pour le plug-in <code>audit_binfile</code> .  | Identifie les répertoires pour les enregistrements d'audit binaires.                                            | <a href="#">“Procédure d'affectation de l'espace d'audit pour la piste d'audit” à la page 601</a>           |
| Configuration d'espace de stockage pour le plug-in <code>audit_remote</code> . | Vous permet d'envoyer des enregistrements d'audit à un référentiel distant par le biais d'un mécanisme protégé. | <a href="#">“Procédure d'envoi des fichiers d'audit à un référentiel distant” à la page 604</a>             |

| Tâche                                                            | Description                                                              | Voir                                                                                   |
|------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Configuration d'espace de stockage pour le plug-in audit_syslog. | Vous permet de diffuser les événements d'audit au format texte à syslog. | <a href="#">“Procédure de configuration des journaux d'audit syslog” à la page 605</a> |

## ▼ Procédure de 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** Les profils de droits ZFS System Management (gestion de système ZFS) et ZFS Storage Management (gestion de stockage ZFS) doivent vous être attribués. Le dernier profil vous permet de créer des pools de stockage.

- 1
- Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).
- 2
- Déterminez la quantité d'espace disque requis.**  
Attribuez au moins 200 Mo d'espace disque par hôte. Toutefois, le type d'audit dont vous avez besoin dicte l'espace disque requis. Par conséquent, elles peuvent être beaucoup plus élevées que cette figure.

---

**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 l'endossement de rôle, la connexion ou la déconnexion.

---

- 3
- Créez un pool de stockage ZFS mis en miroir.**  
La commande `zpool create` crée un pool de stockage, 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 \*Administration d'Oracle Solaris : Systèmes de fichiers ZFS\*](#).  

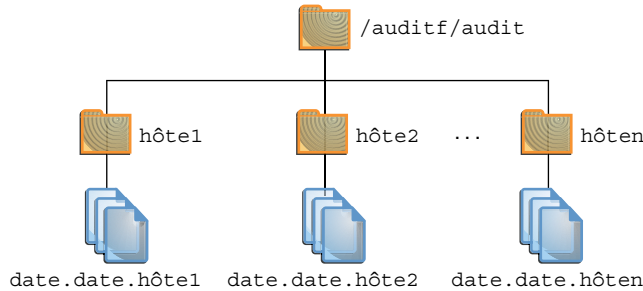
```
# zpool create audit-pool mirror disk1 disk2
```

  
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
```

#### 4 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 voir un exemple, reportez-vous à l'[Exemple 28–12](#).

Le chiffrement doit se gérer. 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 *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

```
# 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
```

#### 5 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
```

#### 6 (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 9](#). 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
```

**7 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
```

**8 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 *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

**9 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
```

**10 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. Reportez-vous à l'[Exemple 28–14](#).

**Exemple 28–12 Création d'un système de fichiers chiffré pour les fichiers d'audit**

Pour respecter les exigences du site en matière de sécurité, l'administrateur crée le système de fichiers d'audit avec le chiffrement activé. Ensuite, il définit le point de montage.

```
# zfs create -o encryption=on auditp/auditf
Enter passphrase for auditp/auditf': /** Type 8-character minimum passphrase**/
Enter again: /** Confirm passphrase **/
```



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

Lorsqu'il crée d'autres systèmes de fichiers sous le système de fichiers `auditf`, ces systèmes de fichiers descendants sont également chiffrés.

### Exemple 28-13 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
```

## ▼ Procédure d'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

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Déterminez les attributs du plug-in `audit_binfile`.

Consultez 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 in bytes that
an audit file can become before it is automatically closed
and a new audit file opened. ...
```

#### 3 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 active 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 “[Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit](#)” à la page 598.

#### 4 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 28–14 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 active p_fsize=4M
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
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 28–15 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`.

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

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

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

```
# audit -s
```

### Exemple 28–16 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 (active)
  Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
  Queue size: 200
# auditconfig -setplugin audit_binfile active "" ""
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
  Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
```

Les derniers guillemets vides ("" ) définissent 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 28–17 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 active 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 [“Procédure de configuration de l'alias de messagerie `audit\_warn`”](#) à la page 594.

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

```
# auditconfig -setplugin audit_binfile active 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
```

## ▼ Procédure d'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.

### Avant de commencer

Vous devez disposer d'un récepteur des fichiers d'audit au niveau du référentiel distant. Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

#### 2 Déterminez les attributs du plug-in `audit_remote`.

Consultez 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.

#### 3 Pour spécifier les hôtes distants, utilisez l'attribut `p_hosts`.

```
# auditconfig -setplugin audit_remote active p_hosts=rhost1:16088:kerberos_v5
```

#### 4 Pour spécifier le nombre de relances, utilisez l'attribut `p_retries`.

```
# auditconfig -setplugin audit_remote active p_retries=5
```

#### 5 Pour spécifier la longueur du délai d'attente de connexion, utilisez l'attribut `p_timeout`.

```
# auditconfig -setplugin audit_remote active p_timeout=3
```

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

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

```
# audit -s
```

## ▼ Procédure de 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 affecter le profil de droit Audit Configuration (configuration d'audit). Pour configurer l'utilitaire `syslog`, vous devez disposer du 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. Actualisez les informations de configuration du service `syslog`.**

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

**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 28–18 Spécification des classes d'audit pour la sortie syslog**

Dans l'exemple suivant, l'utilitaire `syslog` collecte un sous-ensemble de classes d'audit présélectionnées. La classe `pf` est créée dans l'[Exemple 28–10](#).

```
# 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'enregistrement d'audit binaire inclut toutes les utilisations d'un appel à la commande `pfexec`. Pour que ces événements soient disponibles pour la postsélection, le plug-in `audit_binfile` ou `audit_remote` doit être actif. L'utilitaire `syslog` collecte les appels réussis à la commande `pfexec`.

**Exemple 28–19 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
```

# Configuration du service d'audit dans les zones (tâches)

Le service d'audit effectue des audits sur la totalité du système, y compris les événements d'audit dans les zones. Un système doté de zones non globales peut auditer toutes les zones de manière identique, ou configurer l'audit par zone. Pour de plus amples détails, reportez-vous à la section [“Audit sur un système à zones Oracle Solaris” à la page 564](#). Pour la planification, reportez-vous à la section [“Procédure de planification de l'audit par zone” à la page 568](#).

Lorsque vous effectuez un audit des zones non globales identique à celui de la zone globale, le service d'audit s'exécute dans la zone globale. Le service recueille les enregistrements d'audit à partir de la zone globale et de toutes les zones non globales. Les administrateurs de zones non globales peuvent ne pas avoir accès aux enregistrements d'audit.

---

**Remarque** – L'administrateur de la zone globale peut choisir de modifier les masques d'audit des utilisateurs dans les zones non globales.

---

Lorsque vous auditez les zones non globales individuellement, un service d'audit distinct s'exécute dans chaque zone qui fait l'objet d'un audit. Chaque zone collecte ses propres enregistrements d'audit. Les enregistrements sont visibles à la zone non globale et à la zone globale à partir de la racine de zone non globale.

## ▼ Procédure de 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 être dans le rôle root.

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

Effectuez les tâches de la section [“Configuration du service d'audit \(liste des tâches\)” à la page 582](#), à l'exception des points suivants :

- N'activez pas la stratégie d'audit perzone.
- N'activez pas le service d'audit. Vous pouvez activer le service d'audit après avoir configuré les zones non globales pour l'audit.
- 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
add fs
  set special=/etc/security/audit-file
  set dir=/etc/security/audit-file
  set type=lofs
  add options [ro,nodevices,nosetuid]
  commit
end
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 la 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 la 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 la 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 à nouveau le fichier dans les zones non globales.

Les zones non globales sont auditées lorsque le service d'audit est activé dans la zone globale.



**Exemple 28–20** 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
add fs
  set special=/etc/security/audit_class
  set dir=/etc/security/audit_class
  set type=lofs
  add options [ro,nodevices,nosetuid]
  commit
end
add fs
  set special=/etc/security/audit_event
  set dir=/etc/security/audit_event
  set type=lofs
  add options [ro,nodevices,nosetuid]
  commit
end
exit
# zonecfg -z machine1-appserver
add fs
  set special=/etc/security/audit_class
  set dir=/etc/security/audit_class
  set type=lofs
  add options [ro,nodevices,nosetuid]
  commit
end
...
exit
```

Lorsque les zones non globales sont réinitialisées, les fichiers `audit_class` et `audit_event` sont en lecture seule dans les zones.

## ▼ Procédure de 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**

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué pour configurer l'audit. Le profil de droits Audit Control (contrôle d'audit) doit vous avoir été attribué pour activer le service d'audit.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.
- 2 **Dans la zone globale, configurez l'audit.**
  - a. **Effectuez les tâches de la section [“Configuration du service d'audit \(liste des tâches\)”](#) à la page 582.**
  - b. **Ajoutez la stratégie d'audit perzone. Pour la commande, reportez-vous à l'[Exemple 28–8](#).**

---

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

---

- 3 **Dans chaque zone non globale que vous envisagez d'auditer, configurez les fichiers d'audit.**
  - a. **Effectuez les tâches de la section [“Configuration du service d'audit \(liste des tâches\)”](#) à la page 582.**
  - b. **Ne configurez pas les paramètres d'audit système.**  
En particulier, n'ajoutez pas la stratégie perzone ou ahl t à la zone non globale.
- 4 **Activez l'audit dans votre zone.**

```
myzone# audit -s
```

**Exemple 28–21** Désactivation de l'audit dans une zone non globale

Cet exemple fonctionne si la zone globale a défini la stratégie d'audit perzone. L'administrateur de zone de la zone noaudit désactive l'audit pour cette zone.

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

# Activation et désactivation du service d'audit (tâches)

Le service d'audit est activé par défaut et configuré par la commande `auditconfig`. Si la stratégie d'audit `perzone` est définie dans la zone globale, les administrateurs de zone peuvent activer, actualiser et désactiver le service dans leurs zones non globales.

## ▼ Procédure d'actualisation du service d'audit

Cette procédure met à jour le service d'audit lorsque vous avez modifié la configuration d'un plug-in d'audit après l'activation du service d'audit.

### Avant de commencer

Le profil de droits Audit Control (contrôle d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Actualisez le service d'audit.

```
# audit -s
```

---

**Remarque** – Lors de l'actualisation du service d'audit, tous les paramètres de configuration temporaires sont perdus. La stratégie d'audit et les contrôles de file d'attente permettent de définir des paramètres temporaires. Pour plus d'informations, reportez-vous à la page de manuel [auditconfig\(1M\)](#).

---

#### 3 Mettez à jour les masques de présélection des utilisateurs qui sont audités.

Les enregistrements d'audit sont générés en fonction du masque de présélection d'audit associé à chaque processus. L'actualisation du service d'audit *ne modifie pas* les masques de processus existants. Pour réinitialiser explicitement le masque de présélection pour un processus existant, reportez-vous à la section “[Procédure de mise à jour du masque de présélection des utilisateurs connectés](#)” à la page 635.

### Exemple 28–22 Actualisation d'un service d'audit activé

Dans cet exemple, l'administrateur reconfigure l'audit, vérifie les modifications, puis actualise le service 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 (active)
  Attributes: p_dir=/audit/sys1.1,/var/audit;
             p_minfree=2;p_fsize=4G;
Queue size: 200
# auditconfig -setplugin audit_binfile active "" ""
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
  Attributes: p_dir=/audit/sys1.1,/var/audit
             p_minfree=2;p_fsize=4G;
```

Les derniers guillemets vides ("" ) définissent la taille de la file d'attente pour le plug-in sur la valeur par défaut.

- 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 50.

```
# auditconfig -setplugin audit_syslog active p_flags=+lo,-ex 50
# auditconfig -getplugin audit_syslog
auditconfig -getplugin audit_syslog
Plugin: audit_syslog (active)
  Attributes: p_flags=+lo,-ex;
Queue size: 50
```

- 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 = ahl,arge,argv,perzone
active audit policies = ahl,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 lowwater 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 (active)
  Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;

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

## ▼ Procédure de désactivation du service d'audit

Cette procédure montre comment désactiver l'audit dans la zone globale et dans une zone non globale lorsque la stratégie d'audit per zone est définie.

- Si la stratégie d'audit per zone n'est pas définie, l'audit est désactivé pour toutes les zones.
- Si la stratégie d'audit per zone est définie dans la zone globale, elle reste en vigueur dans les zones non globales qui ont activé l'audit.

Dans la mesure où la stratégie per zone est définie dans la zone globale, la zone non globale continue à collecter les enregistrements d'audit pour toutes les réinitialisations de la zone globale et des zones non globales.

### Avant de commencer

Le profil de droits Audit Control (contrôle d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Exécutez la commande `audit -t` pour désactiver le service d'audit.

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

- Dans la zone globale, désactivez le service d'audit.

```
# audit -t
```

Si la stratégie d'audit per zone n'est pas définie, cette commande désactive l'audit dans toutes les zones.

- **Dans une zone non globale, désactivez le service d'audit.**

Si la stratégie d'audit perzone est définie, l'administrateur de zone non globale doit désactiver le service dans la zone non globale.

```
zone1 # audit -t
```

## ▼ Procédure d'activation du service d'audit

Cette procédure permet d'activer le service d'audit pour toutes les zones une fois le service désactivé par l'administrateur. Pour démarrer le service d'audit dans une zone non globale, reportez-vous à l'[Exemple 28–23](#).

### Avant de commencer

Pour activer ou désactiver le service d'audit, vous devez disposer du profil de droits Audit Control (contrôle d'audit).

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

- 2 **Utilisez la commande `audit -s` pour activer le service d'audit.**

```
# audit -s
```

Pour plus d'informations, reportez-vous à la page de manuel [audit\(1M\)](#).

- 3 **Vérifiez que l'audit est activé.**

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

### Exemple 28–23 Activation de l'audit dans une zone non globale

Dans cet exemple, l'administrateur de zone active le service d'audit pour zone1 après avoir exécuté les actions suivantes :

- L'administrateur de la zone globale définit la stratégie perzone dans la zone globale.
- L'administrateur de la zone non globale configure le service d'audit et les personnalisations par utilisateur.

Ensuite, l'administrateur de zone active le service d'audit pour la zone.

```
zone1# audit -s
```

# Gestion des enregistrements d'audit sur les systèmes locaux (tâches)

Le plug-in par défaut `audit_binfile` crée une piste d'audit. En gérant la piste d'audit, vous pouvez surveiller les actions des utilisateurs de votre réseau. L'audit peut générer de grandes quantités de données. Les tâches suivantes vous indiquent comment travailler avec toutes ces données.

## Gestion des enregistrements d'audit sur les systèmes locaux (liste des tâches)

La liste des tâches suivante présente les procédures de sélection, d'analyse et de gestion des enregistrements d'audit.

| Tâche                                                   | Description                                                                                                                  | Voir                                                                                                    |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Affichage des formats des enregistrements d'audit.      | Affiche le type d'informations collectées pour un événement d'audit et l'ordre dans lequel les informations sont présentées. | <a href="#">“Procédure d'affichage des définitions d'enregistrement d'audit” à la page 615</a>          |
| Fusion des enregistrements d'audit.                     | Combine des fichiers d'audit provenant de plusieurs machines dans une seule piste d'audit.                                   | <a href="#">“Procédure de fusion des fichiers d'audit de la piste d'audit” à la page 617</a>            |
| Sélection des enregistrements à examiner.               | Sélectionne des événements particuliers à examiner.                                                                          | <a href="#">“Procédure de sélection des événements d'audit de la piste d'audit” à la page 619</a>       |
| Affichage des enregistrements d'audit.                  | Vous permet d'afficher des enregistrements d'audit binaires.                                                                 | <a href="#">“Procédure d'affichage du contenu des fichiers d'audit binaires” à la page 621</a>          |
| 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.  | <a href="#">“Procédure de nettoyage d'un fichier d'audit <code>not_terminated</code>” à la page 623</a> |
| 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.                   | <a href="#">“Procédure de contrôle du dépassement de la piste d'audit” à la page 624</a>                |

### ▼ Procédure d'affichage des définitions d'enregistrement d'audit

La commande `auditrecord` affiche les définitions d'enregistrement d'audit. 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.

- **Placez les définitions de tous les enregistrements d'événements d'audit dans un fichier HTML.**

L'option `-a` répertorie toutes les définitions d'événements d'audit. L'option `-h` place la liste au format HTML.

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

---

**Astuce** – 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.

---

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

### Exemple 28–24 Affichage des formats d'enregistrement d'audit d'un programme

Dans cet exemple, le format de tous les enregistrements d'audit sont générés par le programme `login` est affiché. Les programmes de connexion incluent `rlogin`, `telnet`, `newgrp` et la fonction Secure Shell d'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 28–25 Affichage des formats d'enregistrement d'audit d'une classe d'audit

Dans cet exemple, le format de tous les enregistrements d'audit dans la classe `pf` qui a été créée dans l'[Exemple 28–10](#) s'affiche.

```
% auditrecord -c pf
```

```
pfexec
```



|                    |        |                                                             |
|--------------------|--------|-------------------------------------------------------------|
| system call        | pfexec | See <code>execve(2)</code> with <code>pfexec</code> enabled |
| event ID           | 116    | AUE_PFEEXEC                                                 |
| 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.

## ▼ Procédure de fusion des fichiers d'audit de la piste d'audit

En fusionnant tous les fichiers d'audit de tous les répertoires d'audit, vous pouvez analyser le contenu de la piste d'audit entière. La commande `auditreduce` fusionne tous les enregistrements à partir de ses fichiers d'entrée dans un seul fichier de sortie. Les fichiers d'entrée peuvent ensuite être supprimés. Si aucun chemin n'est spécifié, la commande `auditreduce` utilise le système de fichiers `/var/audit`.

---

**Remarque** – Dans la mesure où les horodatages dans 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

Le profil de droits Audit Review (vérification d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

#### 2 Créez un système de fichiers pour stocker les fichiers d'audit fusionnés.

Ce système de fichiers doit figurer dans un *zpool* différent des systèmes de fichiers que vous avez créés à la section [“Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit”](#) à la page 598 pour stocker les fichiers d'origine.

### 3 Fusionnez les enregistrements d'audit de la piste d'audit.

Remplacez les répertoires par le répertoire de stockage des fichiers d'audit fusionnés. 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.

```
# 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 racine 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\(1M\)](#).

### 4 Déplacez le fichier fusionné vers le système de fichiers dans le zpool différent.

Pour déplacer le fichier vers un autre système, utilisez la commande `sftp`. Pour obtenir des instructions, reportez-vous à la page de manuel [sftp\(1\)](#).

## Exemple 28–26 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 racine 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 vers un fichier fusionné. Le chemin d'accès complet est spécifié comme valeur de l'option `-O`. 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, seuls les fichiers complets sont copiés du système `sys1.1` dans un fichier fusionné.

```
$ cd /var/audit/storage
$ auditreduce -M sys1.1 -O example1summ
$ ls /var/audit/storage/*summ
20100827183214.20100827214217.example1summ
```

### Exemple 28–27 Déplacement de fichiers d'audit dans un fichier résumé

L'option `-D` de la commande `auditreduce` supprime un fichier d'audit lorsque vous la copiez dans un autre emplacement. Dans l'exemple suivant, les fichiers d'audit complets pour le système `sys1.1` sont copiés dans le système de fichiers `audit_summary` pour examen à une date ultérieure.

```
$ cd /var/audit/audit_summary
$ auditreduce -C -O daily_sys1.1 -D sys1.1
$ ls *sys1.1
20100827183214.20100827214217.daily_sys1.1
```

Les fichiers d'audit du système `sys1.1`, qui étaient les entrées du fichier `*daily_sys1.1`, sont supprimés lorsque cette commande se termine.

## ▼ Procédure de sélection des événements d'audit de la piste d'audit

Vous pouvez filtrer les enregistrements d'audit pour les examiner. Pour obtenir la liste complète des options de filtrage, reportez-vous à la page de manuel [auditreduce\(1M\)](#).

#### Avant de commencer

Le profil de droits Audit Review (vérification d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

#### 2 Sélectionnez les types d'enregistrements que vous souhaitez dans la piste d'audit, ou à partir d'un fichier d'audit spécifié.

```
auditreduce -lowercase-option argument [optional-file]
```

*argument*      Argument spécifique qui nécessite une option minuscule. Par exemple, l'option `-c` exige un *argument* d'une classe d'audit, tel que `ua`.

- d Sélectionne tous les événements à une date donnée. Le format de date pour *argument* est *aaaammjj*. D'autres options de date, -b et -a, sélectionnent les événements avant et après une date particulière.
  - u Sélectionne tous les événements attribuables à un utilisateur particulier. L'*argument* est un nom d'utilisateur. Une autre option utilisateur, -e, sélectionne tous les événements attribuables à un ID d'utilisateur effectif.
  - c Sélectionne tous les événements d'une classe d'audit présélectionnée. L'*argument* est un nom de classe d'audit.
  - m Sélectionne toutes les instances d'un événement d'audit. L'*argument* est un événement d'audit.
- optional-file* Nom d'un fichier d'audit.

Pour obtenir la liste complète des options, reportez-vous à la page de manuel [auditreduce\(1M\)](#).

#### Exemple 28–28 Association et réduction des fichiers d'audit

La commande `audit reduce` peut éliminer les enregistrements moins intéressants, car elle combine les fichiers d'entrée. Par exemple, vous pouvez utiliser la commande `audit reduce` pour conserver uniquement les enregistrements de connexion et déconnexion dans les fichiers d'audit qui ont plus d'un mois. Si vous avez besoin de récupérer la piste d'audit complète, vous pouvez le faire à partir d'un média de sauvegarde.

```
# cd /var/audit/audit_summary
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

#### Exemple 28–29 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.

```
$ cd /var/audit/audit_summary
$ auditreduce -e tamiko -O tamiko
```

Vous pouvez rechercher des événements spécifiques dans ce fichier. L'exemple suivant permet de vérifier le moment où l'utilisateur s'est connecté et déconnecté le 7 septembre 2010, votre heure. Seuls les fichiers avec le nom d'utilisateur en tant que suffixe de fichier sont vérifiés. La forme abrégée de la date est *aaaammjj*.

```
# auditreduce -M tamiko -O tamikolo -d 20100907 -u tamiko -c lo
```

**Exemple 28–30** Copie des enregistrements sélectionnés dans un seul fichier

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 racine d'audit.

```
# auditreduce -c lo -d 20100827 -O /var/audit/audit_summary/logins
# ls /var/audit/audit_summary/*logins
/var/audit/audit_summary/20100827183936.20100827232326.logins
```

## ▼ Procédure d'affichage du contenu des fichiers d'audit binaires

La commande `praudit` vous permet de consulter le contenu de fichiers d'audit binaires. Vous pouvez envoyer la sortie de la commande `auditreduce` ou vous pouvez lire un fichier d'audit particulier. L'option `-x` est utile pour un traitement supplémentaire.

### Avant de commencer

Le profil de droits Audit Review (vérification d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

#### 2 Utilisez l'une des commandes `praudit` suivantes afin de produire la sortie la mieux adaptée à vos besoins.

Les exemples suivants représentent la sortie `praudit` depuis le même événement d'audit. La stratégie d'audit a été définie de façon à inclure les jetons `sequence` et `trailer`.

- La commande `praudit -s` affiche les enregistrements d'audit dans un format court, un jeton par ligne. Utilisez l'option `-l` pour placer chaque enregistrement sur une seule ligne.

```
$ auditreduce -c lo | praudit -s
header,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
```

- La commande `praudit -r` affiche les enregistrements d'audit au format brut, un jeton par ligne. Utilisez l'option `-l` pour placer chaque enregistrement sur une seule ligne.

```
$ auditreduce -c lo | praudit -r
21,69,2,6222,0x0000,10.132.136.45,1287070091,698391050
36,26700,0,10,26700,10,856,50036632,82 0 10.132.136.45
39,0,0
47,1298
```

- La commande `praudit -x` affiche les enregistrements d'audit au format XML, un jeton par ligne. Utilisez l'option `-l` pour placer la sortie XML pour un seul enregistrement sur une seule ligne. La liste suivante divise deux lignes de sortie pour tenir sur cette page d'impression :

```
$ 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>
```

### Exemple 28-31 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 28-32 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 28-33 Création d'enregistrements d'audit au format XML

Dans cet exemple, les enregistrements d'audit sont convertis au format XML.

```
# praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

Le fichier XML peut être affiché dans un navigateur. Le contenu du fichier peut être exécuté par un script pour extraire les informations pertinentes.

### Exemple 28-34 Traitement de la sortie praudit à l'aide d'un script

Si vous le souhaitez, vous pouvez traiter la sortie de la commande `praudit` en tant que lignes de texte. Cela peut être utile pour sélectionner des enregistrements que la commande `auditreduce` ne peut pas sélectionner. Un simple script shell suffit pour traiter la sortie de la commande `praudit`. L'exemple de script suivant place un enregistrement d'audit sur une seule ligne, recherche une chaîne de caractères spécifiée par l'utilisateur, puis renvoie le fichier d'audit dans sa forme d'origine.

```
#!/bin/sh
#
## This script takes an argument of a user-specified string.
# The sed command prefixes the header tokens with Control-A
# The first tr command puts the audit tokens for one record
# 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" \
| tr '\002' '\012'
```

*Finds the user-specified string*  
*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.

### Erreurs fréquentes

Un message semblable à celui-ci indique que vous ne disposez pas de tous les privilèges nécessaires pour utiliser la commande `praudit` :

```
praudit: Can't assign 20090408164827.20090408171614.sys1.1 to stdin.
```

Exécutez la commande `praudit` dans un shell de profil. Le profil de droits Audit Review (vérification d'audit) doit vous avoir été attribué.

## ▼ Procédure de 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 `audit reduce -O` pour donner au fichier le bon horodatage.

### Avant de commencer

Le profil de droits Audit Review (vérification d'audit) doit vous avoir été attribué.

#### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” à la page 175](#).

#### 2 Affichez la liste des fichiers avec la chaîne not\_terminated sur votre système de fichiers d'audit dans l'ordre de leur création.

```
# ls -Rlt audit-directory*/ * | grep not_terminated
```

-R     Répertoire les fichiers dans des sous-répertoires.

- t Répertorie les fichiers du plus récent au plus ancien.
- l Affiche la liste des fichiers dans une seule colonne.

### 3 Nettoyez l'ancien fichier `not_terminated`.

Spécifiez le nom de l'ancien fichier de la commande `audit reduce -O`.

```
# auditreduce -O system-name old-not-terminated-file
```

### 4 Supprimez l'ancien fichier `not_terminated`.

```
# rm system-name old-not-terminated-file
```

## Exemple 28–35 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 -Rlt */* | 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 -lt
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 -lt
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.

## ▼ Procédure de contrôle du dépassement de la piste d'audit

Si votre politique de sécurité exige que toutes les données d'audit soient enregistrées, empêchez la perte d'enregistrement d'audit.

### Avant de commencer

Vous devez être dans le rôle `root`.



**1 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 [Exemple 28–17](#).

**2 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 texte. Pour plus d'informations, reportez-vous à la page de manuel [logadm\(1M\)](#).

**3 Planifiez la suppression des fichiers d'audit archivés dans le système de fichiers d'audit.****4 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`.

**5 Consignez les fichiers d'audit qui ont été archivés.****6 Stockez correctement le média d'archivage.****7 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 “[Procédure de compression des fichiers d'audit sur un système de fichiers dédié](#)” à la page 638.

Reportez-vous également à la section “[Interactions entre les propriétés de compression, de suppression des doublons et de chiffrement ZFS](#)” du manuel *Administration d'Oracle Solaris : Systèmes de fichiers ZFS*.

**8 Réduisez le volume des données d'audit que vous pouvez stocker en créant des fichiers résumés.**

Vous pouvez extraire des fichiers résumés de la piste d'audit à l'aide d'options de la commande `auditreduce`. Les fichiers résumés contiennent uniquement les enregistrements de types spécifiés d'événements d'audit. Pour extraire les fichiers résumés, reportez-vous à l'[Exemple 28–28](#) et l'[Exemple 28–30](#).

## Dépannage du service d'audit (tâches)

Cette section couvre différents messages d'erreur et préférences de l'audit et décrit l'audit proposé par d'autres outils. Ces procédures peuvent vous aider à enregistrer les événements d'audit requis et à résoudre les problèmes d'audit.

### Dépannage du service d'audit (liste des tâches)

La liste des tâches suivante présente les procédures de dépannage de l'audit.

| Problème                                                                                                                                            | Solution                                                                                                                    | Voir                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Pourquoi les enregistrements d'audit ne se sont-ils pas consignés alors que j'ai configuré l'audit ?                                                | Dépannez le service d'audit.                                                                                                | <a href="#">“Procédure de vérification de l'exécution de l'audit” à la page 627</a>                                                     |
| Comment puis-je réduire la quantité d'informations d'audit collectées ?                                                                             | Auditez uniquement les événements que vous voulez contrôler.                                                                | <a href="#">“Procédure d'atténuation du volume des enregistrements d'audit produits” à la page 629</a>                                  |
| Comment puis-je auditer tout ce qu'un utilisateur fait sur le système ?                                                                             | Auditez un ou plusieurs utilisateurs pour chaque commande.                                                                  | <a href="#">“Procédure d'audit de toutes les commandes par les utilisateurs” à la page 631</a>                                          |
| Comment faire pour affecter aux sessions existantes les modifications que j'apporte actuellement aux événements d'audit en cours d'enregistrement ? | Mettez à jour un masque de présélection utilisateur.                                                                        | <a href="#">“Procédure de mise à jour du masque de présélection des utilisateurs connectés” à la page 635</a>                           |
| Comment accéder aux modifications apportées à un fichier particulier ?                                                                              | Auditez les modifications du fichier, puis utilisez la commande <code>audit reduce</code> pour rechercher un fichier donné. | <a href="#">“Procédure de recherche des enregistrements d'audit concernant des modifications de fichiers spécifiques” à la page 633</a> |
| Comment puis-je réduire la taille de mes fichiers d'audit ?                                                                                         | Limitez la taille du fichier d'audit binaire.                                                                               | <a href="#">“Procédure de limitation de la taille des fichiers d'audit binaires” à la page 637</a>                                      |
| Comment puis-je utiliser moins d'espace du système de fichiers pour les fichiers d'audit ?                                                          | Utilisez la compression et les quotas ZFS.                                                                                  | <a href="#">“Procédure de compression des fichiers d'audit sur un système de fichiers dédié” à la page 638</a>                          |
| Comment puis-je supprimer les événements d'audit du fichier <code>audit_event</code> ?                                                              | Mettez correctement à jour le fichier <code>audit_event</code> .                                                            | <a href="#">“Procédure de suppression de l'audit d'événements spécifiques” à la page 636</a>                                            |
| Comment puis-je auditer tous les noms d'utilisateur d'un système Oracle Solaris ?                                                                   | Auditez les connexions à partir de n'importe quel système.                                                                  | <a href="#">“Procédure d'audit des connexions à partir d'autres systèmes d'exploitation” à la page 639</a>                              |

| Problème                                                                                 | Solution                                                                             | Voir                                                                                     |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Pourquoi les enregistrements d'audit ne sont-ils pas conservés pour mes transferts FTP ? | Utilisez l'outil d'audit qui permet aux utilitaires de gérer leurs propres journaux. | <a href="#">“Procédure d'audit des transferts de fichiers FTP et SFTP” à la page 640</a> |

## ▼ Procédure de vérification de l'exécution de l'audit

L'audit est activé par défaut. Si vous croyez que l'audit n'a pas été désactivé, alors qu'aucun enregistrement d'audit n'est envoyé au plug-in actif, effectuez la procédure suivante pour isoler le problème.

**Avant de commencer**

Pour modifier un fichier système, vous devez posséder le rôle root. Pour configurer l'audit, le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

**1 Vérifiez que l'audit est en cours d'exécution.**

Choisissez l'une des méthodes suivantes :

■ **Vérifiez la condition d'audit en cours.**

La liste suivante indique que l'audit n'est pas en cours d'exécution :

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

La liste 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 liste suivante indique que l'audit n'est pas en cours d'exécution :

```
# svcs -x auditd
svc:/system/auditd:default (Solaris audit daemon)
State: disabled since Sun Oct 10 10:10:10 2010
Reason: Disabled by an administrator.
See: http://sun.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 liste suivante indique que le service d'audit est en cours d'exécution :

```
# svcs auditd
STATE      STIME      FMRI
online     10:10:10   svc:/system/auditd:default
```

Si le service d'audit n'est pas activé, activez-le. Pour connaître la procédure, reportez-vous à la section [“Procédure d'activation du service d'audit” à la page 614](#).

## 2 Vérifiez qu'au moins un plug-in est actif.

```
# audit -v
```

Si aucun plug-in n'est actif, activez-en un.

```
# auditconfig -setplugin audit_binfile active
```

## 3 Si vous avez créé une classe d'audit personnalisée, vérifiez que vous avez affecté des événements à cette classe.

Par exemple, la liste d'indicateurs suivante contient la classe `pf`, que le logiciel Oracle Solaris n'a pas fourni :

```
# auditconfig -getflags
active user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
configured user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
```

Pour obtenir une description de la création de la classe `pf`, reportez-vous à la section [“Procédure d'ajout d'une classe d'audit” à la page 595](#).

### a. Vérifiez que la classe est définie dans le fichier `audit_class`.

La classe d'audit doit être définie et son masque doit être unique.

```
# grep pf /etc/security/audit_class      Verify class exists
0x0100000000000000:pf:profile
# grep 0x08000000 /etc/security/audit_class  Ensure mask is unique
0x0100000000000000:pf:profile
```

Remplacez un masque qui n'est pas unique. Si la classe n'est pas définie, définissez-la. Sinon, exécutez la commande `auditconfig -setflags` avec les valeurs valides pour réinitialiser les indicateurs actuels.

### b. Vérifiez que les événements ont été affectés à la classe.

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 des événements ne sont pas affectés à la classe, affectez-y les événements appropriés.

- 4 Si aucun problème n'a été indiqué au cours des étapes précédentes, reportez-vous à votre messagerie et aux fichiers journaux.
  - a. 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`.
  - b. 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. Pour obtenir un exemple, reportez-vous à la liste de l'Étape 1.
  - c. 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.
- 5 Après avoir localisé et résolu les problèmes, activez ou redémarrez le service d'audit.  
# `audit -s`

## ▼ Procédure d'atténuation du volume des enregistrements d'audit produits

Une fois que vous avez déterminé les événements à auditer sur votre site, utilisez les suggestions suivantes pour créer des fichiers d'audit faciles à gérer.

### Avant de commencer

Pour présélectionner les classes d'audit et définir la stratégie d'audit, le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été affecté. Pour modifier les fichiers système et affecter les indicateurs d'audit aux utilisateurs, rôles et profils de droits, vous devez posséder le rôle `root`.

#### 1 Utilisez la stratégie d'audit par défaut.

Évitez en particulier d'ajouter des événements et des jetons d'audit à la piste d'audit. Les stratégies suivantes augmentent la taille de la piste d'audit.

- Stratégie `arge` : ajoute des variables d'environnement aux événements d'audit `execv`.
- Stratégie `argv` : ajoute des paramètres de commande aux événements d'audit `execv`.
- Stratégie `public` : si des événements de fichier sont en cours d'audit, ajoute un événement à la piste d'audit chaque fois qu'un événement auditable se produit dans un [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 552.

- Stratégie `path` : ajoute un jeton `path` aux événements d'audit qui comprennent un jeton `path` facultatif.
- Stratégie `group` : ajoute un jeton `group` aux événements d'audit qui comprennent un jeton `newgroups` facultatif.
- Stratégie `seq` : ajoute un jeton `sequence` à chaque événement d'audit.
- Stratégie `trailer` : ajoute un jeton `trailer` à chaque événement d'audit.
- Stratégie `windata_down` : sur un système configuré avec `Trusted Extensions`, ajoute les événements lorsque les informations dans une fenêtre étiquetée sont réduites.
- Stratégie `windata_up` : sur un système configuré avec `Trusted Extensions`, ajoute les événements lorsque les informations dans une fenêtre étiquetée sont détaillées.
- Stratégie `zonename` : ajoute le nom de zone à chaque événement d'audit. Si la zone globale est la seule zone configurée, ajoute la chaîne `zone, global` à chaque événement d'audit.

L'enregistrement d'audit suivant montre l'utilisation de l'instruction de la commande `ls`. La classe `ex` est auditée et la stratégie par défaut est en cours d'utilisation :

```
header,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
```

## 2 Utilisez le plug-in `audit_syslog` pour envoyer des événements d'audit à `syslog`.

Et 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`.

### 3 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` à la commande `roleadd`, `rolemod`, `useradd` et `usermod` afin d'auditer les événements pour des utilisateurs et des rôles spécifiques. Pour obtenir des exemples, reportez-vous à l'[Exemple 28–18](#) 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 les attributs de sécurité affectés](#)” à la page 217.

---

### 4 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 “[Procédure d'ajout d'une classe d'audit](#)” à la page 595.




---

**Attention** – Si vous modifiez des affectations de classes d'audit existantes, vos modifications seront peut-être conservées lors de la mise à niveau vers une version plus récente du SE Oracle Solaris. Toutefois, la version plus récente du fichier d'Oracle Solaris peut inclure des modifications que vous devrez incorporer manuellement dans l'installation. Consultez attentivement les journaux d'installation. Pour plus d'informations, reportez-vous à la description de `preserve=renamew` dans la page de manuel `pkg(5)`.

---

## ▼ Procédure d'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, le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été affecté. Pour affecter les indicateurs d'audit aux utilisateurs, rôles et profils de droits, vous devez posséder le rôle root .

## 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

## 2 Auditez les classes lo et ex.

La classe ex audite tous les appels des fonctions `exec()` et `execve()`.

La classe lo audite les connexions, déconnexions et blocages d'écran. La sortie suivante répertorie tous les événements des classes ex et lo.

```
% 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)
```

### ■ 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 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
```

### 4 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
```

## ▼ Procédure de 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 `audit reduce` pour localiser les fichiers.

#### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué pour utiliser la commande `auditconfig`. Le profil de droits Audit Review (vérification de l'audit) doit vous avoir été attribué pour utiliser la commande `audit reduce`. Pour affecter les indicateurs d'audit aux utilisateurs et rôles, vous devez posséder le rôle `root`.

**1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

**2 Effectuez un audit de la classe fw.**

L'ajout de la classe aux indicateurs d'audit d'un utilisateur ou d'un rôle génère moins d'enregistrements que si vous ajoutez la 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)
```

**3 Ou, 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)
```

- **Si les indicateurs à l'échelle du système effectuent l'audit pour la réussite ou l'échec, définissez des exceptions pour des utilisateurs et des rôles spécifiques.**

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

Les indicateurs à l'échelle du système ne sont toujours pas modifiés, mais le masque de présélection pour ces quatre rôles est modifié.

```
# auditconfig -getflags
active user default audit flags = lo,fw(0x1002,0x1000)
configured user default audit flags = lo,fw(0x1002,0x1000)
```

- 4 Pour trouver les enregistrements d'audit pour des fichiers spécifiques, utilisez 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`. Cette commande crée un fichier binaire avec le suffixe `filechg` qui contient tous les enregistrements incluant le chemin d'accès aux fichiers concernés. Reportez-vous à la page de manuel [auditreduce\(1M\)](#) pour plus d'informations sur la syntaxe de l'option `-o file=chemin`.

- 5 Pour lire le fichier `filechg`, utilisez la commande **praudit**.

```
# praudit *filechg
```

## ▼ Procédure de mise à jour du masque de présélection des utilisateurs connectés

Vous voulez que les utilisateurs qui sont déjà connectés fassent l'objet d'un audit pour les modifications apportées au masque de présélection d'audit à l'échelle du système.

### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué. Pour fermer les sessions utilisateur, vous devez posséder le profil de droits Process Management (gestion de processus).

- 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

- 2 Mettez à jour le masque de présélection des utilisateurs déjà connectés.

Deux options s'offrent à vous : Vous pouvez fermer les sessions existantes ou utiliser la commande `auditconfig` pour mettre à jour les masques de présélection.

#### ■ Fermez les sessions existantes de ces utilisateurs.

Les utilisateurs peuvent se déconnecter, puis se reconnecter. Ou bien, dans un rôle auquel est attribué le profil de droits Process Management (gestion de processus), vous pouvez mettre fin manuellement aux sessions actives. La nouvelle session va hériter du nouveau masque de présélection. Toutefois, l'arrêt des sessions utilisateurs n'est pas très pratique.

- **Modifiez dynamiquement le masque de présélection de chaque utilisateur connecté.**

Dans un rôle incluant le profil de droits Audit Configuration (configuration d'audit), supposons que vous avez modifié le masque de présélection d'audit à l'échelle du système de `lo` à `lo,ex`.

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

- a. **Répertoriez les utilisateurs réguliers 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)
```

- b. **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
```

- c. **Modifiez le masque de présélection de l'utilisateur.**

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

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

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

- d. **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
```

## ▼ Procédure de 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 être dans le rôle root.

## 1 Changez la classe de l'événement pour la classe no.

Par exemple, les événements 26 et 27 appartiennent à la classe pm.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):pm
27:AUE_SETPGRP:setpgrp(2):pm
28:AUE_SWAPON:swapon(2):no
...
```

Modifiez ces événements pour la classe no.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):no
27:AUE_SETPGRP:setpgrp(2):no
28:AUE_SWAPON:swapon(2):no
...
```

Si la classe pm est actuellement en cours d'audit, les sessions existantes sont toujours les événements d'audit 26 et 27. Pour 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 [“Procédure de mise à jour du masque de présélection des utilisateurs connectés”](#) à la page 635.



**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.
```

## ▼ Procédure de limitation de la taille des fichiers d'audit binaires

Les fichiers d'audit binaires augmentent sans limite. Pour faciliter la tâche de l'archivage et de la recherche, vous pouvez être amené à limiter la taille. Vous pouvez également créer de plus petits fichiers binaires à partir du fichier d'origine.

### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué pour définir l'attribut `pfs` size. Le profil de droits Audit Review (vérification de l'audit) doit vous avoir été attribué pour utiliser la commande `audit reduce`

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.
- 2 **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\(5\)](#).  
Reportez-vous à l'[Exemple 28–14](#).
- 3 **Utilisez la commande `audit reduce` pour sélectionner des enregistrements et les écrire dans un fichier plus petit pour une analyse plus approfondie.**  
Les options `audit reduce -minuscules` recherchent des enregistrements spécifiques.  
Les options `audit reduce -majuscules` écrivent vos sélections vers un fichier. Pour plus d'informations, reportez-vous à la page de manuel [auditreduce\(1M\)](#).

## ▼ **Procédure de 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 28–14](#). Dans cette procédure, vous réduisez la taille par compression.

### **Avant de commencer**

Les profils de droits ZFS System Management (gestion de système ZFS) et ZFS Storage Management (gestion de stockage ZFS) doivent vous être attribués. Le dernier profil vous permet de créer des pools de stockage.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**  
Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.
- 2 **Dédiez un système de fichiers ZFS aux fichiers d'audit.**  
Pour obtenir la procédure, reportez-vous à la section “[Procédure de création de systèmes de fichiers ZFS pour les fichiers d'audit](#)” à la page 598.
- 3 **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.

Pour définir la compression, utilisez la commande `zfs set compression=on dataset`. 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
# audit -s
# zfs get compressratio auditp/auditf
NAME          PROPERTY      VALUE      SOURCE
auditp/auditf compressratio  16.89x      -
```

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 6, “Gestion des systèmes de fichiers Oracle Solaris ZFS” du manuel \*Administration d'Oracle Solaris : Systèmes de fichiers ZFS\*](#).

## ▼ Procédure d'audit des connexions à partir d'autres systèmes d'exploitation

Le SE Oracle Solaris peut auditer les connexions, quelle que soit la source.

### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

- 1 **Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” à la page 175.

- 2 **Auditez la classe `lo` pour les événements attribuables et non attribuables.**

Cette classe audite les connexions, déconnexions, et blocages d'écran. Ces classes sont soumises à un audit par défaut.

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

### 3 Si les valeurs ont été modifiées, ajoutez l'indicateur `lo`.

```
# auditconfig -getflags
active user default audit flags = as,st(0x20800,0x20800)
configured user default audit flags = as,st(0x20800,0x20800)
# auditconfig -setflags lo,as,st
user default audit flags = as,lo,st(0x21800,0x21800)
# auditconfig -getnaflags
active non-attributable audit flags = na(0x400,0x400)
configured non-attributable audit flags = na(0x400,0x400)
# auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

---

**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 [“Secure Shell et le projet OpenSSH”](#) à la page 316.

---

## ▼ Procédure d'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.

#### Avant de commencer

Le profil de droits Audit Configuration (configuration d'audit) doit vous avoir été attribué.

### 1 Endossez le rôle d'administrateur et dotez-vous des attributs de sécurité nécessaires.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) à la page 175.

### 2 Pour consigner des commandes et transferts de fichiers du service FTP, reportez-vous à la page de manuel `proftpd`.

Pour connaître les options de journalisation disponibles, reportez-vous à la section concernant les fonctions de journalisation. Les options `log commands` et `log transfers` peuvent notamment fournir des journaux utiles.

### 3 Pour consigner les transferts de fichier et l'accès `sftp`, auditez la classe `ft`.

La classe `ft` comprend les transactions SFTP suivantes :

```
% auditrecord -c ft
file transfer: chmod ...
file transfer: chown ...
file transfer: download ...
file transfer: mkdir ...
file transfer: upload ...
```



```

file transfer: remove ...
file transfer: rename ...
file transfer: rmdir ...
file transfer: session start ...
file transfer: session end ...
file transfer: symlink ...
file transfer: utimes

```

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

Comme indiqué dans la sortie suivante, la connexion et la déconnexion du démon `ftpd` génèrent des enregistrements d'audit.

```

% auditrecord -c lo | more
...
in.ftpd
  program    /usr/sbin/in.ftpd    See ftp access
  event ID   6165                  AUE_ftpd
  class      lo                    (0x0000000000001000)
    subject
    [text]                  error message
    return

in.ftpd
  program    /usr/sbin/in.ftpd    See ftp logout
  event ID   6171                  AUE_ftpd_logout
  class      lo                    (0x0000000000001000)
    subject
    return
...

```



## Audit (référence)

---

Ce chapitre décrit les éléments importants de l'audit. Vous trouverez ci-après une liste des informations de référence citées dans ce chapitre.

- “Service d'audit” à la page 643
- “Pages de manuel du service d'audit” à la page 645
- “Profil de droits pour l'administration de l'audit” à la page 646
- “Audit et zones Oracle Solaris” à la page 647
- “Classes d'audit” à la page 647
- “Plug-ins d'audit” à la page 649
- “Stratégie d'audit” à la page 649
- “Caractéristiques de l'audit de processus” à la page 651
- “Piste d'audit” à la page 652
- “Conventions relatives aux noms de fichiers d'audit binaires” à la page 652
- “Structure d'enregistrement d'audit” à la page 653
- “Formats de jeton d'audit” à la page 654

Pour une présentation de l'audit, reportez-vous au [Chapitre 26, “Audit \(présentation\)”](#). Pour obtenir des suggestions de planification, reportez-vous au [Chapitre 27, “Planification de l'audit”](#). Pour connaître les procédures de configuration de l'audit sur votre site, reportez-vous au [Chapitre 28, “Gestion de l'audit \(tâches\)”](#).

## Service d'audit

Le service d'audit, `auditd`, est activé par défaut. Pour activer, actualiser ou désactiver le service, reportez-vous à la section [“Activation et désactivation du service d'audit \(tâches\)”](#) à la page 611.

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 l'endossement 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 [“Procédure d'affichage des paramètres par défaut du service d'audit”](#) à la page 583.

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 646.

Par défaut, toutes les zones font l'objet d'un audit identique. Reportez-vous à la section [“Audit et zones Oracle Solaris”](#) à la page 647.

# 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                   | Récapitulatif                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">audit(1M)</a>        | Commande qui contrôle les actions du service d'audit<br><br>audit -n démarre un nouveau fichier d'audit pour le plug-in audit_binfile .<br><br>audit -s active et actualise l'audit.<br><br>audit -t désactive l'audit.<br><br>audit -v vérifie qu'au moins un plug-in est actif.                                                                                                  |
| <a href="#">audit_binfile(5)</a> | Plug-in d'audit par défaut, qui envoie les enregistrements d'audit dans un fichier binaire. Reportez-vous également à la section “ <a href="#">Plug-ins d'audit</a> ” à la page 649.                                                                                                                                                                                               |
| <a href="#">audit_remote(5)</a>  | Plug-in d'audit qui envoie les enregistrements d'audit à un récepteur distant.                                                                                                                                                                                                                                                                                                     |
| <a href="#">audit_syslog(5)</a>  | Plug-in d'audit qui envoie les récapitulatifs au format texte des enregistrements d'audit à l'utilitaire syslog .                                                                                                                                                                                                                                                                  |
| <a href="#">audit_class(4)</a>   | 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 connaître l'effet de la modification de ce fichier sur la mise à niveau du système, reportez-vous à la section “ <a href="#">Procédure d'ajout d'une classe d'audit</a> ” à la page 595.                     |
| <a href="#">audit_event(4)</a>   | Fichier qui contient les définitions des événements d'audit et mappe les événements avec les classes d'audit. Le mappage peut être modifié. Pour connaître l'effet de la modification de ce fichier sur la mise à niveau du système, reportez-vous à la section “ <a href="#">Procédure de modification de l'appartenance à une classe d'un événement d'audit</a> ” à la page 596. |
| <a href="#">audit_flags(5)</a>   | 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.                                                                                                                                                                         |
| <a href="#">audit.log(4)</a>     | Décrit l'attribution de noms aux fichiers d'audit binaires, la structure interne d'un fichier et la structure de chaque jeton d'audit.                                                                                                                                                                                                                                             |
| <a href="#">audit_warn(1M)</a>   | 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 bien, vous pouvez indiquer comment gérer ces conditions automatiquement.     |
| <a href="#">auditconfig(1M)</a>  | Commande qui extrait et définit les paramètres de configuration d'audit.<br><br>Entrez auditconfig sans option pour obtenir une liste des paramètres qui peuvent être extraits et définis.                                                                                                                                                                                         |

| Page de manuel                  | Récapitulatif                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">auditrecord(1M)</a> | Commande qui affiche la définition d'événements d'audit dans le fichier <code>/etc/security/audit_event</code> . Vous trouverez un exemple de sortie à la section <a href="#">“Procédure d’affichage des définitions d’enregistrement d’audit”</a> à la page 615.                                                                                                                                                                                                                                                                                                                           |
| <a href="#">auditreduce(1M)</a> | <p>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.</p> <p>Les options en majuscules influent sur la sélection des fichiers. Les options en minuscules influent sur la sélection des enregistrements.</p>                                                                                                                                                         |
| <a href="#">auditstat(1M)</a>   | 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.                                                                                                                                                                                                                                                |
| <a href="#">praudit(1M)</a>     | <p>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 <code>auditreduce</code> 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 <code>tail -0f</code> pour un fichier d'audit actuel.</p> <p>Vous trouverez un exemple de sortie à la section <a href="#">“Procédure d’affichage du contenu des fichiers d’audit binaires”</a> à la page 621.</p> |
| <a href="#">syslog.conf(4)</a>  | Fichier configuré pour envoyer des résumés au format texte d'enregistrements d'audit à l'utilitaire <code>syslog</code> pour le plug-in <code>audit_syslog</code> .                                                                                                                                                                                                                                                                                                                                                                                                                         |

## 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. Pour modifier un fichier de configuration de l'audit, les privilèges `root` sont nécessaires.

- **Audit Configuration (configuration d'audit)** : permet à l'administrateur de configurer les paramètres du service d'audit et d'exécuter la commande `auditconfig`.
- **Audit Control (contrôle d'audit)** : permet à l'administrateur de démarrer, d'actualiser et de désactiver le service d'audit et d'exécuter la commande `audit` pour démarrer, actualiser ou arrêter le service.
- **Audit Review (vérification de l'audit)** : permet à l'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`.

- **System Administrator (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 [“Configuration initiale RBAC \(liste des tâches\)”](#) à la page 177.

## Audit et zones Oracle Solaris

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 à zones Oracle Solaris”](#) à la page 564 et [“Procédure de planification de l'audit par zone”](#) à la page 568.

Pour en savoir plus sur les zones, reportez-vous à la [Partie II, “Oracle Solaris Zones”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

## 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 [“Procédure d'ajout d'une classe d'audit”](#) à la page 595.



---

**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.
- Avec un caret (^) précédant un préfixe ou un indicateur d'audit, une présélection actuelle est modifiée. Par exemple,
  - 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` des 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`
  - Où envoyer les données binaires - attribut `p_dir`
  - L'espace minimal restant sur un disque avant que l'administrateur ne reçoive un avertissement d'espace limite - attribut `p_minfree`
  - La taille maximale d'un fichier d'audit - attribut `p_fsize`
- Plug-in `audit_remote`
  - Un serveur d'audit authentifié à distance auquel envoyer les données d'audit binaires - attribut `p_hosts`
  - Le nombre de tentatives à effectuer pour atteindre un serveur d'audit à distance authentifié - attribut `p_retries`
  - Le nombre de secondes entre les tentatives pour atteindre un serveur d'audit à distance authentifié - attribut `p_timeout`
- Plug-in `audit_syslog`
  - Une sélection de résumés au format texte des enregistrements d'audit à envoyer à `syslog` - attribut `p_flags`
- 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\(1M\)](#).

## 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, “Audit de Trusted Extensions \(présentation\)”](#) du manuel *Configuration et administration d'Oracle Solaris 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 650.

Les effets des différentes options de stratégie d'audit sont décrits à la section “[Assimilation des concepts de stratégie d'audit](#)” à la page 573. 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. Les combinaisons de ces stratégies ont les effets suivants :

- `-ahlt +cnt` est la stratégie adoptée par défaut. Cette valeur par défaut permet à un événement audité d'être traité même s'il ne peut pas être consigné.

La stratégie `-ahlt` indique que si un enregistrement d'audit d'un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise les événements et poursuit le traitement. Dans la zone globale, le compteur `as_dropped` enregistre le nombre correspondant.

La stratégie `+cnt` indique que si un événement synchrone survient et ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise l'événement et poursuit le traitement. Le compteur `as_dropped` de la zone enregistre le nombre correspondant.

La configuration `-ahlt +cnt` est généralement utilisée sur les sites où le traitement doit se poursuivre, même si celui-ci peut entraîner une perte d'enregistrements d'audit. Les champs `audits_tatdrop` 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. Des programmes semblent être bloqués jusqu'à ce que de l'espace d'audit devienne disponible. Le champ auditstat wblk indique à combien de reprises des threads ont été bloqués.

Toutefois, si un événement asynchrone se produit, le système va paniquer, entraînant une interruption de service. La file d'attente du noyau des événements d'audit peut être restaurée manuellement partir d'un vidage mémoire enregistré. L'événement asynchrone ne sera pas dans la file d'attente de l'audit et doit être récupéré à partir de pointeurs sur la pile des appels.

- La stratégie -ahlt -cnt indique que si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, l'événement sera comptabilisé et le traitement poursuivi. Lorsqu'un événement synchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le thread tentant de fournir l'événement sera bloqué. Le thread est placé dans une file d'attente de mise en veille jusqu'à ce que de l'espace d'audit devienne disponible. Aucun compte n'est conservé. Des programmes peuvent sembler bloqués jusqu'à ce que de l'espace d'audit devienne disponible.

La configuration -ahlt -cnt est généralement utilisée dans les sites où l'enregistrement de tous les événements d'audit synchrones est prioritaire sur la perte potentielle d'enregistrements d'audit asynchrones. Le champ auditstat wblk indique à combien de reprises des threads ont été bloqués.

- La stratégie +ahlt +cnt indique que si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système panique. Si un événement asynchrone ne peut pas être placé dans la file d'attente d'audit du noyau, le système comptabilise l'événement et poursuit le traitement.

## 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. Ce masque de présélection de processus détermine la création ou non d'enregistrements d'audit selon les événements de chaque classe d'audit.

L'algorithme suivant décrit la façon dont le système obtient le masque de présélection de processus utilisateur :

(system-wide default flags + always-audit-classes) - never-audit-classes

Ajoute les classes d'audit système issues des résultats de la commande `auditconfig -get flags` aux classes issues de la valeur *always-audit-classes* pour le mot-clé `always_audit` de l'utilisateur. Ensuite, du total, soustrait 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 endosse 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 de la piste 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 “[Procédure de nettoyage d'un fichier d'audit not\\_terminated](#)” à la page 623.

## Structure d'enregistrement d'audit

Un enregistrement d'audit est une séquence de jetons d'audit. Chaque jeton d'audit contient des informations sur les événements tels que l'ID utilisateur, la date et l'heure. Un jeton header commence un enregistrement d'audit et un jeton trailer peut éventuellement conclure l'enregistrement. D'autres jetons d'audit contiennent des informations relatives à l'événement d'audit. La figure suivante illustre un enregistrement d'audit standard au niveau du noyau et un enregistrement d'audit standard au niveau de l'utilisateur.

FIGURE 29-1 Structures d'enregistrement d'audit standard

|                   |                 |
|-------------------|-----------------|
| Jeton header      | Jeton header    |
| Jeton arg         | Jeton subject   |
| Jetons de données | [autres jetons] |
| Jeton subject     | Jeton return    |
| Jeton return      |                 |

## 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 “[Procédure d'affichage du contenu des fichiers d'audit binaires](#)” à la page 621.

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 654.

- 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 par les 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 29-1 Jetons d'audit pour l'audit

| Nom de variable         | Description                                                                                                                          | Voir                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <code>acl</code>        | Informations sur l'entrée de contrôle d'accès (ACE, Access Control Entry) et la liste de contrôle d'accès (ACL, Access Control List) | "Jeton <code>acl</code> " à la page 656                       |
| <code>arbitrary</code>  | Données avec informations de format et de type                                                                                       | Reportez-vous à la page de manuel <code>audit.log(4)</code> . |
| <code>argument</code>   | Valeur de l'argument d'appel système                                                                                                 | "Jeton <code>argument</code> " à la page 656                  |
| <code>attribut</code>   | Informations sur le fichier vnode                                                                                                    | "Jeton <code>attribute</code> " à la page 656                 |
| <code>cmd</code>        | Arguments de commande et variables d'environnement                                                                                   | "Jeton <code>cmd</code> " à la page 657                       |
| <code>exec_args</code>  | Arguments d'appel système Exec                                                                                                       | "Jeton <code>exec_args</code> " à la page 657                 |
| <code>exec_env</code>   | Variables d'environnement d'appel système Exec                                                                                       | "Jeton <code>exec_env</code> " à la page 657                  |
| <code>exit</code>       | Informations sur la sortie du programme                                                                                              | Reportez-vous à la page de manuel <code>audit.log(4)</code> . |
| <code>file</code>       | Informations sur le fichier d'audit                                                                                                  | "Jeton <code>file</code> " à la page 658                      |
| <code>fmri</code>       | Identificateur de ressource de gestion de structure                                                                                  | "Jeton <code>fmri</code> " à la page 658                      |
| <code>group</code>      | Informations sur les groupes de processus                                                                                            | "Jeton <code>group</code> " à la page 658                     |
| <code>header</code>     | Indique le début de l'enregistrement d'audit                                                                                         | "Jeton <code>header</code> " à la page 658                    |
| <code>ip</code>         | Informations sur l'en-tête IP                                                                                                        | Reportez-vous à la page de manuel <code>audit.log(4)</code> . |
| <code>ip address</code> | Adresse Internet                                                                                                                     | "Jeton <code>ip address</code> " à la page 659                |
| <code>ip port</code>    | Adresse du port Internet                                                                                                             | "Jeton <code>ip port</code> " à la page 659                   |

TABLEAU 29-1 Jetons d'audit pour l'audit (Suite)

| Nom de variable           | Description                                        | Voir                                                                                                                                                        |
|---------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipc                       | Informations sur l'IPC System V                    | "Jeton ipc" à la page 659                                                                                                                                   |
| IPC_perm                  | Informations sur l'accès à l'objet IPC System V    | "Jeton IPC_perm" à la page 660                                                                                                                              |
| opaque                    | Données non structurées (format non spécifié)      | Reportez-vous à la page de manuel <code>audit.log(4)</code> .                                                                                               |
| path                      | Informations relatives aux chemins                 | "Jeton path" à la page 660                                                                                                                                  |
| path_attr                 | Informations relatives aux chemins d'accès         | "Jeton path_attr" à la page 661                                                                                                                             |
| privilege                 | Informations sur le jeu de privilèges              | "Jeton privilege" à la page 661                                                                                                                             |
| process                   | Informations sur le processus                      | "Jeton process" à la page 661                                                                                                                               |
| return                    | Statut des appels système                          | "Jeton return" à la page 661                                                                                                                                |
| sequence                  | Numéro de séquence                                 | "Jeton sequence" à la page 662                                                                                                                              |
| socket                    | Types de socket et adresses                        | "Jeton socket" à la page 662                                                                                                                                |
| sujet                     | Informations sur subject (même format que process) | "Jeton subject" à la page 662                                                                                                                               |
| text                      | Chaîne de caractères ASCII                         | "Jeton text" à la page 663                                                                                                                                  |
| trailer                   | Indique la fin de l'enregistrement d'audit         | "Jeton trailer" à la page 663                                                                                                                               |
| use of authorization      | Utilisation d'autorisation                         | "Jeton use of authorization" à la page 663                                                                                                                  |
| use of privilege          | Utilisation de privilège                           | "Jeton use of privilege" à la page 664                                                                                                                      |
| user                      | ID utilisateur et nom de l'utilisateur             | "Jeton user" à la page 664                                                                                                                                  |
| xclient                   | Identification du client X                         | "Jeton xclient" à la page 664                                                                                                                               |
| zonename                  | Nom de la zone                                     | "Jeton zonename" à la page 664                                                                                                                              |
| Jetons Trusted Extensions | Informations sur le système Window X et label      | Reportez-vous à la section "Référence de l'audit Trusted Extensions" du manuel <i>Configuration et administration d'Oracle Solaris Trusted Extensions</i> . |

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. Ce jeton header indique l'endroit où l'enregistrement d'audit commence dans la piste d'audit. Dans le cas d'événements attribuables, les jetons `subject` et `process` font référence aux valeurs du processus qui ont causé l'événement. Dans le cas d'événements non attribuables, le jeton `process` fait référence au système.

## Jeton `acl`

Le jeton `acl` possède deux formes d'enregistrement d'informations sur ACE (Access Control Entries) pour un système de fichiers ZFS et ACL (Access Control Lists) pour un système de fichiers UFS.

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, aucun `vnode` ne permet d'obtenir les informations requises sur le fichier. Par conséquent, le jeton `attribute` n'est pas inclus dans l'enregistrement d'audit. La commande `praudit -x` affiche les champs du jeton `attribute`, 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 d'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 est renvoyée à des fins d'affichage.

```
<exec_env><env>_=/usr/bin/hostname</env>  
<env>LANG=C</env><env>PATH=/usr/bin:/usr/ucb</env>  
<env><env>LOGNAME=j doe</env><env>USER=j doe</env>  
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env>  
<env>HOME=/home/j doe</env><env>PWD=/home/j doe</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 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` :

```
<fmri service_instance="svc:/system/cryptosvc"></fmri>
```

## Jeton group

Le jeton `group` enregistre les entrées de groupe dans les données d'identification du processus.

La commande `praudit -x` affiche les champs du jeton `groups`, comme suit :

```
<group><gid>staff</gid><gid>other</gid></group>
```

---

**Remarque** – Le jeton `group` est sorti uniquement lorsque l'option de stratégie d'audit `group` est active.

---

## Jeton header

Le jeton `header` est spécial car il marque le début d'un enregistrement d'audit. Le jeton `header` se combine avec le jeton `trailer` pour entourer tous les autres jetons de l'enregistrement.

Parfois, un jeton `header` peut inclure un ou plusieurs modificateurs d'événement :

- `fe` indique un événement d'audit qui a échoué
- `fp` indique l'utilisation manquée 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 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.

**Remarque** – 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 29-2 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 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` :

```
<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 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 enregistrée pour les privilèges du jeu de base. Si un privilège a été supprimé du jeu de base par une action administrative, alors l'utilisation de ce privilège est enregistrée. Pour plus d'informations sur les privilèges, reportez-vous à la section “[Privilèges \(présentation\)](#)” à la page 158

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 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. Ce jeton est utile pour le débogage.

La commande `praudit -x` affiche le contenu du jeton `sequence` :

```
<sequence seq-num="1292"/>
```

---

**Remarque** – Le jeton `sequence` s'affiche en sortie uniquement lorsque l'option de stratégie d'audit `seq` est active.

---

## Jeton socket

Le jeton `socket` contient des informations qui décrivent un socket Internet. Dans certains cas, le jeton n'inclut que le port distant et l'adresse IP distante.

La commande `praudit` affiche l'instance du jeton `socket` de la manière suivante :

```
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 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 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` :

```
<text>booting kernel</text>
```

## Jeton trailer

Les deux jetons, `header` et `trailer`, sont spéciaux car ils distinguent les points de fin d'un enregistrement d'audit et entourent tous les autres jetons. Un jeton `header` commence par un enregistrement d'audit. Un jeton `trailer` se termine par un enregistrement d'audit. Le jeton `trailer` est facultatif. Le jeton `trailer` est ajouté en tant que dernier jeton de chaque enregistrement uniquement lorsque l'option de stratégie d'audit `trail` a été définie.

Lorsqu'un enregistrement d'audit est généré avec des blocs de fin activés, la commande `auditreduce` peut vérifier que le bloc de fin pointe correctement vers l'en-tête d'enregistrement. Le jeton `trailer` prend en charge les recherches en arrière dans la piste d'audit.

La commande `praudit` affiche le jeton `trailer` comme suit :

```
trailer,136
```

## Jeton use of authorization

Le jeton `use of authorization` enregistre l'utilisation d'autorisation.

La commande `praudit` affiche le jeton `use of authorization` de la manière suivante :

```
use of authorization,solaris.role.delegate
```

```
XXXX<use_of_authorization result="successful use of auth">solaris.role.delegate</use_of_auth>
```

## Jeton use of privilege

Le jeton use of privilege enregistre l'utilisation de privilège.

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 :

```
<zone name="graphzone"/>
```



# Glossaire

---

<b>AES</b>	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 <b>principal d'utilisateur</b> comme norme administrative.
<b>algorithme</b>	Algorithme cryptographique. Il s'agit d'une procédure de calcul récursive établie qui chiffre ou hache une entrée.
<b>algorithme cryptographique</b>	Voir <b>algorithme</b> .
<b>allocation de périphériques</b>	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.
<b>amorçe</b>	Valeur numérique de départ pour la génération de nombres aléatoires. Lorsque cette valeur provient d'une source aléatoire, l'amorçe est appelée <i>amorçe aléatoire</i> .
<b>application privilégiée</b>	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.
<b>attributs de sécurité</b>	Dans RBAC, remplace la stratégie de sécurité qui permet à une commande d'administration de s'exécuter correctement lorsque celle-ci est exécutée par un utilisateur autre que le superutilisateur. Dans le modèle de superutilisateur, les programmes <code>setuid</code> et <code>setgid</code> sont des attributs de sécurité. Lorsque ces attributs sont appliqués à une commande, la commande s'exécute correctement, quel que soit l'utilisateur qui l'exécute. Dans le modèle de privilège, les attributs de sécurité sont les privilèges. Quand un privilège est donné à une commande, celle-ci s'exécute correctement. Le modèle de privilège est compatible avec le modèle superutilisateur dans la mesure où le modèle de privilège considère également les programmes <code>setuid</code> et <code>setgid</code> comme des attributs de sécurité.
<b>authentificateur</b>	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.

<b>authentification</b>	Processus de vérification de l'identité déclarée d'un principal.
<b>autorisation</b>	<p>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.</p> <p>2. Dans le contrôle d'accès basé sur les rôles (RBAC), autorisation pouvant être attribuée à un rôle ou un utilisateur (ou intégrée dans un profil de droits) en vue de l'exécution d'une classe d'actions autrement interdites par la stratégie de sécurité.</p>
<b>Blowfish</b>	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.
<b>cache d'informations d'identification</b>	Espace de stockage (généralement un fichier) contenant des informations d'identification reçues de KDC.
<b>champ d'application du service de noms</b>	Champ d'application dans lequel un rôle est autorisé à fonctionner, c'est-à-dire un hôte individuel ou tous les hôtes desservis par un service de noms, tel que NIS ou LDAP.
<b>chiffrement par clé privée</b>	Dans le cas du chiffrement par clé privée, l'expéditeur et le destinataire utilisent la même clé de chiffrement. Voir également <a href="#">chiffrement par clé publique</a> .
<b>chiffrement par clé publique</b>	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 <a href="#">chiffrement par clé privée</a> .
<b>clé de service</b>	Clé de chiffrement partagée par un principal de service et le KDC, et distribuée en dehors des limites du système. Voir également <a href="#">key</a> .
<b>clé de session</b>	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 <a href="#">key</a> .
<b>clé privée</b>	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 <a href="#">key</a> .
<b>clé secrète</b>	Voir <a href="#">clé privée</a> .
<b>client</b>	<p>Au sens strict, il s'agit d'un processus utilisant un service réseau pour le compte d'un utilisateur, par exemple, une application utilisant <code>rlogin</code>. Dans certains cas, un serveur peut être lui-même le client d'un autre serveur ou service.</p> <p>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.</p> <p>Dans la pratique, ce terme désigne un principal utilisant un service.</p>
<b>confidentialité</b>	Voir <a href="#">confidentialité</a> .

<b>confidentialité</b>	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 <a href="#">authentification</a> , <a href="#">intégrité</a> , <a href="#">service</a> .
<b>conscient des privilèges</b>	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 <a href="#">privileges(5)</a> .
<b>consommateur</b>	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 <a href="#">fournisseur</a> .
<b>DES</b>	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.
<b>domaine</b>	<ol style="list-style-type: none"><li>1. Réseau logique desservi par une seule base de données Kerberos et un ensemble de centre de distribution des clés (KDC).</li><li>2. Troisième partie d'un nom de principal. Pour le nom de principal <code>jdoe/admin@ENG.EXAMPLE.COM</code>, le domaine est <code>ENG.EXAMPLE.COM</code>. Voir également <a href="#">nom de principal</a>.</li></ol>
<b>DSA</b>	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 <a href="#">SHA1</a> en entrée.
<b>écart d'horloge</b>	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 peut être spécifié dans le fichier <code>krb5.conf</code> .
<b>escalade des privilèges</b>	Accès aux ressources situées en dehors de la plage autorisée par les attributs de sécurité qui vous sont attribués, y compris les remplacements. Il en résulte qu'un processus peut effectuer des actions non autorisées.
<b>événement d'audit asynchrone</b>	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.
<b>événement d'audit asynchrone</b>	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.
<b>événement d'audit non allouable</b>	Événement d'audit dont l'initiateur ne peut pas être déterminé, tel que l'événement <code>AUE_BOOT</code> .
<b>fichier de ticket</b>	Voir <a href="#">cache d'informations d'identification</a> .

<b>fichier keytab</b>	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.
<b>fichier stash</b>	Un fichier stash contient une copie chiffrée de la clé principale pour le KDC. Cette clé principale est utilisée lorsqu'un serveur est redémarré pour authentifier automatiquement le KDC avant qu'il ne démarre les processus kadmind et krb5kdc. 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.
<b>fichiers d'audit</b>	Journaux d'audit binaires. Les fichiers d'audit sont stockés séparément dans un système de fichiers d'audit.
<b>fournisseur</b>	Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, service de chiffrement 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 <i>plug-ins</i> . Pour consulter des exemples de consommateurs, voir <a href="#">consommateur</a> .
<b>fournisseur de logiciel</b>	Dans la fonctionnalité Structure cryptographique d'Oracle Solaris, module logiciel de noyau ou bibliothèque PKCS#11 fournissant des services cryptographiques. Voir également <a href="#">fournisseur</a> .
<b>fournisseur de matériel</b>	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 <a href="#">fournisseur</a> .
<b>FQDN</b>	Nom de domaine complet. Par exemple, <code>central.example.com</code> (et pas simplement <code>denver</code> ).
<b>GSS-API</b>	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 <a href="#">authentification</a> , <a href="#">intégrité</a> , <a href="#">confidentialité</a> .
<b>hôte</b>	Système accessible par l'intermédiaire d'un réseau.
<b>hôte principal</b>	Instance particulière d'un principal de service dans lequel le principal (indiqué par le nom primaire <code>host</code> ) est configuré de manière à fournir une gamme de services réseau, tels que <code>ftp</code> , <code>rcp</code> ou <code>rlogin</code> . <code>host/central.example.com@EXAMPLE.COM</code> est un exemple d'hôte principal. Voir également <a href="#">principal de serveur</a> .
<b>image système unique</b>	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.
<b>informations d'identification</b>	Package d'informations comprenant un ticket et une clé de session correspondante. Informations utilisées pour authentifier l'identité d'un principal. Voir également <a href="#">ticket</a> , <a href="#">clé de session</a> .

<b>instance</b>	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 <code>host/central.example.com</code> . Pour les principaux d'utilisateur, une instance est facultative. Notez, cependant, que <code>jdoe</code> et <code>jdoe/admin</code> sont des principaux uniques. Voir également <a href="#">primaire</a> , <a href="#">nom de principal</a> , <a href="#">principal de service</a> , <a href="#">principal d'utilisateur</a> .
<b>intégrité</b>	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 <a href="#">authentification</a> , <a href="#">confidentialité</a> .
<b>jeu autorisé</b>	Jeu des privilèges disponibles pour l'utilisation par un processus.
<b>jeu de base</b>	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.
<b>jeu de privilèges</b>	Ensemble de privilèges. Chaque processus comporte quatre jeux de privilèges qui déterminent s'il peut utiliser un privilège particulier. Voir <a href="#">jeu limite</a> , <a href="#">jeu effectif</a> , <a href="#">jeu autorisé</a> et <a href="#">jeu hérité</a> .  De même, le <a href="#">jeu de base</a> de privilèges est l'ensemble des privilèges affectés aux processus d'un utilisateur au moment de la connexion.
<b>jeu effectif</b>	Jeu de privilèges actuellement en vigueur sur un processus.
<b>jeu hérité</b>	Jeu de privilèges dont un processus peut hériter en appelant <code>exec</code> .
<b>jeu limite</b>	Limite extérieure des privilèges disponibles pour un processus et ses enfants.
<b>KDC</b>	Centre de distribution de clés (Key Distribution Center). Machine disposant de trois composants Kerberos V5. <ul style="list-style-type: none"> <li>■ Principal et base de données de clés</li> <li>■ Service d'authentification</li> <li>■ Service d'octroi de tickets</li> </ul> <p>Chaque domaine dispose d'un KDC maître et doit avoir un ou plusieurs KDC esclaves.</p>
<b>KDC esclave</b>	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 <a href="#">KDC</a> , <a href="#">KDC maître</a> .
<b>KDC maître</b>	KDC maître dans chaque domaine, comprenant un serveur d'administration Kerberos, <code>kadmind</code> et un démon d'authentification et d'octroi de tickets, <code>krb5kdc</code> . 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.
<b>Kerberos</b>	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.

<b>key</b>	<p>1. En règle générale, l'un des deux principaux types de clés :</p> <ul style="list-style-type: none"><li>■ <i>clé symétrique</i> : clé de chiffrement identique à la clé de déchiffrement. Les clés symétriques sont utilisées pour chiffrer des fichiers.</li><li>■ <i>clé asymétrique</i> ou <i>clé publique</i> : 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 <i>secrète</i>. La clé publique est également qualifiée de clé <i>partagée</i> ou <i>commune</i>.</li><li>■ 2. Entrée (nom de principal) dans un fichier keytab. Voir également <a href="#">fichier keytab</a>.</li></ul> <p>3. Dans Kerberos, clé de chiffrement dont il existe trois types :</p> <ul style="list-style-type: none"><li>■ <i>Clé privée</i> : clé de chiffrement partagée par un principal et le KDC, et distribuée en dehors des limites du système. Voir également <a href="#">clé privée</a>.</li><li>■ <i>Clé de service</i> : clé remplissant la même fonction que la clé privée, mais utilisée par des serveurs et des services. Voir également <a href="#">clé de service</a>.</li><li>■ <i>Clé de session</i> : 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 <a href="#">clé de session</a>.</li></ul>
<b>kvno</b>	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.
<b>liste de contrôle d'accès (ACL)</b>	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.
<b>MAC</b>	<p>1. Voir <a href="#">MAC</a>.</p> <p>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.</p> <p>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.</p>
<b>MAC</b>	MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.
<b>MD5</b>	Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest.
<b>mécanisme</b>	<p>1. Package logiciel spécifiant des techniques cryptographiques pour assurer l'authentification ou la confidentialité des données. Exemples : Kerberos V5, clé publique Diffie-Hellman</p> <p>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.</p>

<b>mécanisme de sécurité</b>	Voir <a href="#">mécanisme</a> .
<b>minimisation</b>	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.
<b>modèle de privilège</b>	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.
<b>modèle de superutilisateur</b>	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.
<b>moindre privilège</b>	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 normaux 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.
<b>moteur d'analyse</b>	Application tierce, résidant sur un hôte externe, qui examine un fichier à la recherche de virus connus.
<b>nom de principal</b>	1. Nom d'un principal, au format <i>primary/instance@REALM</i> . Voir également <a href="#">instance</a> , <a href="#">primaire</a> , <a href="#">domaine</a> .  2. (RPCSEC_GSS API) Voir <a href="#">principal de client</a> , <a href="#">principal de serveur</a> .
<b>NTP</b>	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.
<b>objet public</b>	Fichier appartenant à l'utilisateur root et lisible par tout le monde, tel que n'importe quel fichier du répertoire /etc.
<b>PAM</b>	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
<b>phrase de passe</b>	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.

<b>piste d'audit</b>	Collection de tous les fichiers d'audit provenant de tous les hôtes.
<b>primaire</b>	Première partie du nom d'un nom de principal. Voir également <a href="#">instance</a> , <a href="#">nom de principal</a> , <a href="#">domaine</a> .
<b>principal</b>	<p>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 <a href="#">nom de principal</a>, <a href="#">principal de service</a>, <a href="#">principal d'utilisateur</a>.</p> <p>2. (RPCSEC_GSS API) Voir <a href="#">principal de client</a>, <a href="#">principal de serveur</a>.</p>
<b>principal admin</b>	Principal d'utilisateur dont le nom est au format <i>nom_utilisateur/admin</i> (comme dans <i>jdoe/admin</i> ). Un principal admin peut disposer de davantage de privilèges (de modification de stratégies par exemple) qu'un principal d'utilisateur standard. Voir également <a href="#">nom de principal</a> et <a href="#">principal d'utilisateur</a> .
<b>principal d'utilisateur</b>	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 ( <i>jdoe</i> ou <i>jdoe/admin</i> par exemple). Egalement appelé instance d'utilisateur. Voir également <a href="#">principal de service</a> .
<b>principal de client</b>	(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 <i>rpc_gss_principal_t</i> .
<b>principal de serveur</b>	(RPCSEC_GSS API) Principal fournissant un service. Le principal de serveur est stocké sous la forme d'une chaîne de caractères ASCII dont le format est <i>service@hôte</i> . Voir également <a href="#">principal de client</a> .
<b>principal de service</b>	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 <i>ftp</i> , et son instance est le nom d'hôte complet du système fournissant le service. Voir également <a href="#">hôte principal</a> , <a href="#">principal d'utilisateur</a> .
<b>privilège</b>	Droit discret dans le cadre d'un processus dans un système Oracle Solaris. Les privilèges offrent un contrôle des processus plus détaillé que <i>root</i> . Les privilèges sont définis et appliqués dans le noyau. Pour une description complète des privilèges, reportez-vous à la page de manuel <a href="#">privileges(5)</a> .
<b>profil de droits</b>	Egalement désigné par les termes "droit" ou "profil". Ensemble de valeurs de remplacement utilisées dans RBAC et pouvant être affectées à un rôle ou un utilisateur. Un profil de droits peut se composer d'autorisations, de privilèges, de commandes avec des attributs de sécurité et d'autres profils de droits.
<b>protocole Diffie-Hellman</b>	Egalement appelé cryptographie par clé publique. Protocole d'accord de clé cryptographique asymétrique mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par <a href="#">Kerberos</a> .
<b>QOP</b>	Qualité de la protection. Paramètre servant à sélectionner les algorithmes cryptographiques utilisés en association avec le service d'intégrité ou de confidentialité.
<b>RBAC</b>	Contrôle de l'accès basé sur le rôle, une fonction d'Oracle Solaris. Alternative au modèle tout ou rien des superutilisateurs. Le RBAC permet à une organisation de diviser les capacités du superutilisateur et de les affecter à des comptes utilisateur spéciaux appelés rôles. Les rôles peuvent être attribués à des individus spécifiques en fonction de leurs responsabilités.



<b>relation</b>	Variable ou relation de configuration définie dans les fichiers <code>kdc.conf</code> ou <code>krb5.conf</code> .
<b>rôle</b>	Identité spéciale destinée à l'exécution d'applications privilégiées et ne pouvant être prise que par des utilisateurs assignés.
<b>RSA</b>	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).
<b>SEAM</b>	Mécanisme d'authentification Sun Enterprise (Sun Enterprise Authentication Mechanism). Nom de produit des versions initiales d'un système d'authentification des utilisateurs d'un réseau, conçu à partir de la technologie Kerberos V5 développée par le Massachusetts Institute of Technology. Le produit est maintenant appelé le service Kerberos. SEAM fait référence à des parties du service Kerberos qui n'ont pas été incluses dans différentes versions de Solaris.
<b>sécurisation</b>	Modification de la configuration par défaut du système d'exploitation pour supprimer les failles de sécurité inhérentes à l'hôte.
<b>séparation des tâches</b>	Composante de la notion de <a href="#">moindre privilège</a> . La séparation des tâches permet d'empêcher un utilisateur d'exécuter ou d'approuver les actions terminant une transaction. Par exemple, dans <a href="#">RBAC</a> , 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.
<b>serveur</b>	Principal fournissant une ressource aux clients réseau. Si vous vous connectez par <code>ssh</code> au système <code>central.example.com</code> par exemple, ce système est le serveur fournissant le service <code>ssh</code> . Voir également <a href="#">principal de service</a> .
<b>serveur d'application</b>	Voir <a href="#">serveur d'application réseau</a> .
<b>serveur d'application réseau</b>	Serveur fournissant une application réseau, telle que <code>ftp</code> . Un domaine peut contenir plusieurs serveurs d'application réseau.
<b>service</b>	<ol style="list-style-type: none"> <li>1. Ressource fournie aux clients du réseau, souvent par plusieurs serveurs. Si vous vous connectez par <code>rlogin</code> à la machine <code>central.example.com</code> par exemple, cette machine est le serveur fournissant le service <code>rlogin</code>.</li> <li>2. Service de sécurité (d'intégrité ou de confidentialité) fournissant un niveau de protection supérieur à l'authentification. Voir également <a href="#">intégrité</a> et <a href="#">confidentialité</a>.</li> </ol>
<b>service de sécurité</b>	Voir <a href="#">service</a> .
<b>SHA1</b>	Secure Hashing Algorithm, algorithme de hachage sécurisé. L'algorithme s'applique à toute longueur d'entrée inférieure à $2^{64}$ afin d'obtenir une synthèse des messages. L'algorithme SHA1 sert d'entrée à <a href="#">DSA</a> .
<b>shell de profil</b>	Dans <a href="#">RBAC</a> , shell permettant à un rôle (ou un utilisateur) d'exécuter, à partir de la ligne de commande, toutes les applications privilégiées affectées au profil de droits du rôle. Les shells de profil sont <code>pfsh</code> , <code>pfcsch</code> et <code>pfksh</code> . Ils correspondent au shell Bourne ( <code>sh</code> ), au shell C ( <code>csh</code> ) et au shell Korn ( <code>ksh</code> ), respectivement.
<b>shell sécurisé</b>	Un protocole particulier pour une connexion à distance sécurisée et d'autres services de réseau sécurisé via un réseau non sécurisé.

<b>stratégie</b>	<p>En règle générale, plan ou ensemble d'actions qui influence ou détermine les décisions et actions. Pour les systèmes informatiques, la stratégie fait généralement référence à la stratégie de sécurité. La stratégie de sécurité de votre site constitue un ensemble de règles qui définissent la sensibilité des informations traitées et les mesures prises pour protéger les informations contre tout accès non autorisé. Par exemple, la stratégie de sécurité peut exiger que les systèmes soient audités, que les périphériques soient protégés par des privilèges et que les mots de passe soient modifiés toutes les six semaines.</p> <p>Pour la mise en oeuvre des stratégies dans des zones spécifiques du SE Oracle Solaris, reportez-vous à <a href="#">stratégie d'audit</a>, <a href="#">stratégie dans la structure cryptographique</a>, <a href="#">stratégie de périphériques</a>, <a href="#">stratégie Kerberos</a>, <a href="#">stratégie de mot de passe</a> et <a href="#">stratégie RBAC</a>.</p>
<b>stratégie d'audit</b>	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, <code>cnt</code> et <code>ahlt</code> , 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.
<b>stratégie dans la structure cryptographique</b>	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 <code>CKM_DES_CBC</code> provenant d'un fournisseur tel que DES.
<b>stratégie de mot de passe</b>	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 saisies d'un mot de passe erroné tolérées et d'autres considérations relatives à la sécurité. La stratégie de sécurité requiert des mots de passe. La stratégie de mot de passe peut requérir des mots de passe chiffrés avec l'algorithme MD5, et imposer d'autres exigences relatives à la force des mots de passe.
<b>stratégie de périphériques</b>	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 <a href="#">stratégie</a> .
<b>stratégie de sécurité</b>	Voir <a href="#">stratégie</a> .
<b>stratégie Kerberos</b>	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.
<b>stratégie pour technologies à clé publique</b>	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.
<b>stratégie RBAC</b>	Stratégie de sécurité associée à une commande. Actuellement, <code>solaris</code> est la stratégie valide. La stratégie <code>solaris</code> reconnaît les privilèges, les autorisations et les attributs de sécurité <code>setuid</code> .
<b>synthèse</b>	Voir <a href="#">synthèse de message</a> .
<b>synthèse de message</b>	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.

<b>TGS</b>	Service d'octroi de tickets (Ticket-Granting Service) Partie du KDC responsable de l'émission des tickets.
<b>TGT</b>	Ticket d'octroi de tickets (Ticket-Granting Ticket) Ticket émis par le KDC, permettant au client de demander des tickets pour d'autres services.
<b>ticket</b>	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 authenticateur. Voir également <a href="#">authentificateur</a> , <a href="#">informations d'identification</a> , <a href="#">service</a> , <a href="#">clé de session</a> .
<b>ticket initial</b>	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 <i>initiaux</i> afin d'assurer que le client peut démontrer qu'il connaît 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.
<b>ticket non valide</b>	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 <code>VALIDATE</code> , après l'heure de début. Voir également <a href="#">ticket postdaté</a> .
<b>ticket postdaté</b>	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 <i>non valide</i> 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 <i>renouvelable</i> , sa durée de vie est normalement égale à la durée de vie entière du ticket d'octroi de tickets. Voir également <a href="#">ticket non valide</a> , <a href="#">ticket renouvelable</a> .
<b>ticket renouvelable</b>	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 <i>renouvelables</i> . 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.
<b>ticket transmissible</b>	Ticket pouvant être utilisé par un client pour demander un ticket sur un hôte distant sans devoir se soumettre au processus complet d'authentification sur l'hôte concerné. Par exemple, si l'utilisateur david obtient un ticket transmissible sur la machine de l'utilisateur jennifer, il peut se connecter à sa propre machine sans devoir demander un nouveau ticket (et donc s'authentifier à nouveau). Voir également <a href="#">ticket utilisable avec proxy</a> .

<b>ticket utilisable avec proxy</b>	Ticket pouvant être utilisé par un service pour le compte d'un client afin d'effectuer une opération pour ce dernier. On dit alors que le service agit en tant que proxy du client. Grâce à ce ticket, le service peut adopter l'identité du client. Le service peut utiliser un tel ticket afin d'obtenir un ticket de service d'un autre service, mais non un ticket d'octroi de tickets. La différence entre un ticket utilisable avec proxy et un ticket transmissible réside dans le fait que le premier n'est valide que pour une seule opération. Voir également <a href="#">ticket transmissible</a> .
<b>variante</b>	Historiquement, les termes <i>variante de sécurité</i> et <i>variante d'authentification</i> désignaient la même chose, à savoir une variante indiquant 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.
<b>variante de sécurité</b>	Voir <a href="#">variante</a> .
<b>VPN</b>	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

---

## Nombres et symboles

- [ ] (crochets), audit record, sortie, 654
- \$\$ (symbole double dollar), Numéro du processus de shell parent, 210
- \* (astérisque)
  - Caractère générique
  - Autorisation RBAC, 219
  - device\_allocate, fichier, 99, 100
  - Vérification dans les autorisations RBAC, 189
- \ (backslash)
  - device\_allocate, fichier, 100
  - device\_maps, fichier, 99
- ^ (caret), Modificateur de préfixe de classe d'audit, 648
- ^ (caret) dans les préfixes de classe d'audit, 586–590, 634
- .(point)
  - Affichage de fichier caché, 133
  - Séparateur des noms d'autorisations, 219
- ;(point-virgule), device\_allocate, fichier, 99
- @ (signe arobase), device\_allocate, fichier, 100
- # (signe dièse)
  - device\_allocate, fichier, 100
  - device\_maps, fichier, 99
- = (signe égal), Symbole d'autorisations de fichier, 129
- (signe moins)
  - Fichier su\_log, 69
  - Préfixe de classe d'audit, 648
  - Symbole d'autorisations de fichier, 129
  - Symbole de type de fichier, 124
- + (signe plus)
  - Fichier su\_log, 69
  - Préfixe de classe d'audit, 648
- + (signe plus) (*Suite*)
  - Symbole d'autorisations de fichier, 129
- + (signe plus) dans les préfixes de classe d'audit, 605
- > (rediriger la sortie), Interdiction, 48
- >> (ajouter la sortie), Interdiction, 48
- /etc/security/audit\_event, fichier, Événements d'audit, 554
- ~/.gkadmin, fichier, Description, 531
- ~/.k5login, fichier, Description, 531
- ~/.rhosts, fichier, Description, 343
- ~/.shosts, fichier, Description, 343
- ~/.ssh/authorized\_keys, fichier
  - Description, 343
  - Remplacement, 344
- ~/.ssh/config, fichier
  - Description, 344
  - Remplacement, 344
- ~/.ssh/environment, fichier
  - Description, 343
- ~/.ssh/id\_dsa, fichier, Remplacement, 344
- ~/.ssh/id\_rsa, fichier, Remplacement, 344
- ~/.ssh/identity, fichier, Remplacement, 344
- ~/.ssh/known\_hosts, fichier
  - Description, 343
  - Remplacement, 344
- ~/.ssh/rc, fichier, Description, 344
- 3des, algorithme de chiffrement, Fichier
  - ssh\_config, 337
- 3des-cbc, algorithme de chiffrement, Fichier
  - ssh\_config, 337

**A**

- A, option, `audit reduce`, commande, 618–619
- a, option
  - `audit record`, commande, 616
  - Commandes utilisant Kerberos, 525
  - `digest`, commande, 247
  - `encrypt` commande, 251
  - `mac`, commande, 249
- Absolu, mode
  - Définition des autorisations spéciales, 130
  - Modification des autorisations de fichier, 128, 137–138
  - Modification des autorisations de fichier spéciales, 138–139
- Accès
  - Accès au serveur
    - Kerberos, 541–544
  - Accès root
    - Affichage des tentatives sur la console, 70–71
    - Contrôle des tentatives de la commande `su`, 69–70
    - Restriction, 70–71
  - Authentification de la connexion avec Secure Shell, 327–328
  - Authentification RPC sécurisé, 287
  - Liste de contrôle
    - Voir* ACL
  - Obtention pour un service spécifique, 543–544
  - Octroi pour votre compte, 522–524
  - Partage de fichiers, 51
  - Restriction
    - Matériel système, 71–73
    - Périphérique, 43–46, 82
  - Restriction de l'accès aux serveurs KDC, 453
  - root, accès
    - Restriction, 52
    - Surveillance des tentatives de commande `su`, 46
- Sécurité
  - ACL, 51
  - ACL UFS, 130–131
  - Authentification de la connexion, 327–328
  - Configuration du pare-feu, 55–56
  - Contrôle de connexion, 38
  - Contrôle de l'utilisation du système, 46–50

*Accès, Sécurité (Suite)*

- Contrôle réseau, 52–56
- Définition de la variable `PATH`, 47
- Enregistrement des connexions ayant échoué, 63–64
- Génération de rapports sur les problèmes, 57
- Matériel système, 71–73
- NFS client-serveur, 289–292
- Périphérique, 44, 82
- Restriction d'accès aux fichiers, 48
- Restriction d'accès par connexion, 38
- Restrictions d'accès par connexion, 38
- Sécurité physique, 38
- `setuid`, programme, 48
- Suivi de connexion `root`, 46
- Surveillance de l'utilisation du système, 50
- Système distant, 313

## ACL

- Voir* ACL
- Description, 51, 130–131
- Format des entrées, 130–131
- `kadm5.acl`, fichier, 487, 489, 493
- Restrictions sur copie d'entrées, 131

`acl`, jeton d'audit, Format, 656

## Activation

- Abandon clavier, 72–73
- Allocation de périphériques, 86
- Applications utilisant Kerberos uniquement, 452
- Audit, 614
- Mécanisme cryptographique, 261
- Mécanisme et fonction d'un fournisseur de matériel, 266
- Service d'audit, 614
- Utilisation d'un fournisseur de logiciels noyau, 262

## Actualisation

- Service d'audit, 611–613
- Services cryptographiques, 267–268

`add_drv`, commande, Description, 95

`admin_server`, section

Fichier `krb5.conf`, 381, 387

Administrateur système (RBAC), Rôle recommandé, 147

## Administrateurs

Limitation des droits, 199–201

## Administrateurs (*Suite*)

Limitation des droits des utilisateurs, 198–199

## Administration

Algorithmes de mot de passe, 66–69

### Audit

Activation, 614

Actualisation, 611–613

audit -s, commande, 611–613, 614

audit -t, commande, 613–614

audit\_remote, plug-in, 604–605

audit\_syslog, plug-in, 605–606

auditconfig, commande, 582–583, 585–586

auditreduce, commande, 617–619

Classe d'audit, 555–556

Configuration, 582–583

Contrôle des coûts, 576

Contrôles de file d'attente, 592–594

Dépassement de la piste d'audit, 624–625

Désactivation, 613–614

Description, 564

Enregistrement d'audit, 557

Événements d'audit, 554

Fichiers d'audit, 621–623

Liste des tâches, 581

Plug-ins, 604–605

praudit, commande, 621–623

Profils de droits requis, 646–647

Réduction de l'espace requis, 577–578

Stratégie, 590–592

Zone, 564–565

Zones, 607–610, 647

Audit par zone, 568–569

Autorisation de fichier, 132–141

Commande de la structure

cryptographique, 235–236

Connexion distante avec Secure Shell, 323–325

### Kerberos

Keytab, 508–514

Principal, 480–494

Stratégie, 494–503

Liste des tâches de la structure

cryptographique, 254

Liste des tâches du RPC sécurisé, 292–293

Metaslot, 235–236

## Administration (*Suite*)

Mot de passe d'un rôle, 193–194

Mot de passe utilisateur pour utiliser le profil de droits, 201

Privilèges, 209

Profils de droits, 186–187

Utilisateur, 201

Propriétés de sécurité

Anciennes applications, 188–189

Profil de droits, 186–187

Rôle, 193–194, 194–195, 201–202

Utilisateur, 196–197

Propriétés RBAC, 186–187

Rôle remplaçant le superutilisateur, 178–180

### Secure Shell

Client, 336

Liste des tâches, 318

Présentation, 333–335

Serveur, 336

Sécurité des fichiers NFS client-serveur, 289–292

Stratégie de périphériques, 82

Structure cryptographique et zones, 237

Utilisation du mot de passe utilisateur pour endosser un rôle, 201–202

Adresse IP, Vérification Secure Shell, 337

Adresses IP, Exceptions aux valeurs par défaut Secure Shell, 321–322

AES, fournisseur de noyau, 255

aes128-cbc, algorithme de chiffrement, Fichier ssh\_config, 337

aes128-cen, algorithme de chiffrement, Fichier ssh\_config, 337

### Affectation

Privilèges à l'utilisateur, 197

Privilèges à un rôle, 195

Profil de droits

Rôle, 194–195

### Affichage

Attribut d'un principal, 484–486

Attributs de stratégie, 497–499

Autorisation de fichier, 133–134

Contenu de profil de droits, 217

Contrôles de file d'attente d'audit, 593

Contrôles des files d'attente d'audit, 583–585

*Affichage (Suite)*

- Définition d'enregistrement d'audit, 615–617
- Définitions de privilèges, 205–206
- Enregistrement d'audit au format XML, 622
- Enregistrement d'audit sélectionné, 617–619
- Enregistrements d'audit, 621–623
- Etat de connexion d'un utilisateur, 61–62
- Exceptions à l'audit à l'échelle du système, 583–585
- Fichier, informations connexes, 124
- Fournisseurs dans la structure
  - cryptographique, 255–258
- Informations de fichier, 133–134
- Informations sur l'allocation de périphériques, 88
- Liste de principaux, 482–484
- Liste de stratégies, 495–497
- Liste détaillée des mécanismes
  - cryptographiques, 257
- MAC d'un fichier, 249–250
- Mécanisme cryptographique
  - Disponible, 257, 262
  - Existant, 255, 256, 262
- Mécanisme cryptographique disponible, 257, 262
- Mécanisme cryptographique existant, 256, 262
- Mécanismes cryptographiques
  - Objectif, 257
- Paramètres par défaut de l'audit, 583–585
- Paramètres par défaut de la stratégie
  - d'audit, 583–585
- Périphérique allouable, 88
- Privilège attribué directement, 206
- Privilège dans un shell, 207, 210
- Privilège sur un processus, 210
- Privilèges, 204–205
- Rôle disponible, 223
- Rôle endossable, 174
- Sous-liste de principaux (Kerberos), 483
- Stratégie de périphériques, 82–83
- Stratégies d'audit, 590
- Synthèse d'un fichier, 248
- Tampon de la liste de clés à l'aide de la commande
  - list, 512
- Tampon de la liste de clés avec la commande
  - list, 513
- Tentative d'accès root, 70–71

*Affichage (Suite)*

- Tentative de la commande su, 70–71
- Ticket, 517–518
- Utilisateur sans mot de passe, 62
- Utilisateurs sans mot de passe, 62
- Vos droits RBAC, 171–174
- ahlt, stratégie d'audit
  - Avec la stratégie cnt, 650–651
  - Définition, 591
  - Description, 574
- Aide
  - Outil SEAM, 478
  - URL d'aide en ligne, 373
- Aide contextuelle, Outil SEAM, 478
- Aide en ligne
  - Outil SEAM, 478
  - URL, 373
- Ajout
  - Attributs de sécurité
    - Anciennes applications, 188–189
    - Rôles, 194–195
    - Utilisateurs, 196–197
- Audit
  - Rôles, 184–185
  - Utilisateurs individuels, 586–590, 631
  - Zones, 567–573
- Authentification DH de systèmes de fichiers
  - montés, 292
- Classe d'audit, 595–596
- Fournisseur de logiciels, 258–260
- Fournisseur de logiciels au niveau de
  - l'utilisateur, 259–260
- Mécanisme et fonction d'un fournisseur de
  - matériel, 266
- Module PAM, 301
- Nouveaux profils de droits, 186–187
- Périphérique allouable, 86
- Plug-in de bibliothèque, 259–260
- Plug-ins
  - Audit, 604–605, 605–606
  - KME, 283–284
  - Structure cryptographique, 258–260
- Principal d'administration (Kerberos), 382, 389



*Ajout (Suite)*

- Principal de service au fichier keytab (Kerberos), 509–510
- Privilèges
  - Commande, 187
  - Directement à l'utilisateur, 197
  - Directement à un rôle, 195
- Propriétés RBAC
  - Anciennes applications, 188–189
- Rôle cryptomgt, 184
- Rôle lié à la sécurité, 184
- Rôles, 181–183
- Sécurité des périphériques, 83–84, 85–90
- Sécurité du matériel système, 71–72
- Stratégie d'audit, 590–592
- Stratégie d'audit temporaire, 591–592
- Systèmes de fichiers d'audit, 598–601
- Utilisateurs privilégiés, 197

*Algorithme*

- Chiffrement de fichier, 250–253
- Mot de passe
  - Configuration, 66–67

*Algorithmes*

- Chiffrement de mot de passe, 40
- Définition dans la structure cryptographique, 233
- Liste dans la structure cryptographique, 255–258
- Protection par phrase de passe dans
  - ssh-keygen, 316

all, classe d'audit, Précaution d'utilisation, 648

All (tous), RBAC, Profil de droits, 216

*allocate, commande*

- Autorisation requise, 224
- Autorisation utilisateur, 87
- Autorisations, 98
- Etat d'erreur d'allocation, 98
- Lecteur de bande, 91–92
- Utilisation, 91–92

*Allocation de périphériques*

- Activation, 86
- Affichage d'informations, 88
- Ajout de périphérique, 85–86
- Allocation forcée de périphériques, 88–89
- Audit, 90
- Autorisation de dépannage, 88

*Allocation de périphériques (Suite)*

- Autorisation des utilisateurs à allouer, 87
- Autorisation pour les commandes, 97–98
- Autorisations, 96–97
- Commande, 97
- Composant du mécanisme, 96
- deallocate, commande
  - Script de nettoyage de périphériques, 102
  - Utilisation, 93–94
- Demande d'autorisation, 89–90
- Démontage de périphériques alloués, 94
- Dépannage, 92, 93
- Désactivation, 86
- device\_allocate, fichier, 99–101
- device\_maps, fichier, 98–99
- Etat d'erreur d'allocation, 98
- Exemple, 91–92
- Fichier de configuration, 98
- Forcée, 88–89
- Gestion des périphériques, 85–86
- Interdiction, 90
- Libération de périphériques, 93–94
- Libération forcée de périphériques, 89
- Liste des tâches, 85–86
- Modification des périphériques allouables, 89–90
- Montage de périphériques, 92–93
- Ne requérant pas d'autorisation, 89
- Par les utilisateurs, 91–92
- Périphérique allouable, 100, 101
- Procédure pour allouer des périphériques, 91–92
- Procédures utilisateur, 85–90
- Profils de droits, 96–97
- Rendre un périphérique allouable, 86
- Script de nettoyage de périphériques
  - Description, 101–102
  - Ecriture de nouveaux scripts, 102
  - Lecteur de bande, 101
  - Option, 102
  - Périphérique audio, 102
  - Unité de CD-ROM, 102
  - Unité de disquette, 102
- Service SMF, 96
- Utilisation, 85–90
- Utilisation de la commande allocate, 91–92

- AllowGroups, mot-clé, Fichier `sshd_config`, 337
- AllowTcpForwarding, mot-clé
  - Fichier `sshd_config`, 337
  - Modification, 321
- AllowUsers, mot-clé, Fichier `sshd_config`, 337
- ALTSHELL dans Secure Shell, 341
- always-audit*, classes, Masque de présélection de processus, 651
- Analyse de virus
  - Configuration, 77–80
  - Description, 76
  - Fichiers, 75–76
  - Moteurs, 75–76
- Appel système
  - `exec_args`, jeton d'audit, 657
  - `exec_env`, jeton d'audit, 657–658
  - `ioctl` pour nettoyer les périphériques audio, 102
  - `return`, jeton d'audit, 661–662
- Appels système, argument, jeton d'audit, 656
- Application privilégiée
  - Description, 149
  - Vérification d'ID, 154
  - Vérification de privilège, 154
  - Vérification des autorisations, 155
- `arcfour`, algorithme de chiffrement, Fichier `ssh_config`, 337
- ARCFOUR, fournisseur de noyau, 255
- Archivage, Fichier d'audit, 624–625
- `arge`, stratégie d'audit
  - Définition, 633
  - Description, 574
  - `exec_env`, jeton, 657–658
- argument, jeton d'audit, Format, 656
- `argv`, stratégie d'audit
  - Définition, 633
  - Description, 574
  - `exec_args`, jeton, 657
- Astérisque (\*)
  - Caractère générique
    - Autorisation RBAC, 219
  - `device_allocate`, fichier, 99, 100
  - Vérification dans les autorisations RBAC, 189
- `at`, commande, Autorisation requise, 224
- `atq`, commande, Autorisation requise, 224

- Attribut, Mot-clé dans BART, 120
- Attribut de sécurité
  - Considération lors de l'affectation directe, 157–158
  - ID spécial sur les commandes, 154
  - Privilège sur les commandes, 154
  - Profil de droits Network Security (sécurité réseau), 151
  - Utilisation pour monter des périphériques alloués, 87
  - Vérification, 154
- Attribut du fichier de règles, *Voir* Mots-clés
- `attribute`, jeton d'audit, 656
- Attribution
  - Privilège pour des commandes d'un script, 213–214
  - Privilèges ajoutés aux commandes dans un profil de droits, 187
  - Rôle attribué à un utilisateur localement, 183–184
- Attributs de sécurité
  - Considérations d'utilisation lors de l'affectation directe, 158
  - Description, 150
  - Liste de tous les RBAC, 170–171
  - Ordre de recherche, 217
- Audit
  - Activation, 614
  - Ajout d'indicateurs d'audit à un groupe d'utilisateurs, 589–590
  - Allocation de périphériques, 90
  - Configuration
    - identique pour toutes les zones, 607–609
    - Par zone, 609–610
    - Toutes les zones, 582–597
    - Zone globale, 591
  - Configuration d'une zone globale, 568
  - Connexion, 639–640
  - Définition de la postsélection, 554
  - Définition de la présélection, 554
  - Définition des contrôles de file d'attente, 592–594
  - Dépannage, 626–627
  - Dépannage de la commande `praudit`, 623
  - Désactivation, 613–614
  - Mise à jour des informations, 611–613
  - Modification de la stratégie de périphériques, 84
  - Modifications dans la version actuelle, 565–566

*Audit (Suite)*

- Modules enfichables, 557–558
- Obtention des contrôles de file d'attente, 592–594
- Planification, 567–573
- Planification par zone, 568–569
- Privège, 227
- Profil de droits, 646–647
- Récapitulatifs de page de manuel, 645–646
- Recherche de modifications apportées à des fichiers spécifiques, 633–635
- Rôles, 184–185
- Suppression des indicateurs spécifiques à l'utilisateur, 589
- Toutes les commandes par les utilisateurs, 631–633
- Transfert de fichiers sftp, 640–641
- Utilisateurs uniquement, 588–589
- Valeurs par défaut, 643–644
- Vérification de l'exécution, 627–629
- Zone, 564–565
- Zones, 647
- audit*, commande
  - Actualisation du service d'audit, 611–613
  - Désactivation du service d'audit, 613–614
  - Options, 645
- audit -s*, commande, 611–613, 614
- audit -t*, commande, 613–614
- audit\_binfile*, plug-in, 557–558
  - Définition d'attributs, 601–604
  - Définition de l'avertissement lié à l'espace libre, 603–604
  - Obtention d'attributs, 602
  - obtention d'attributs, 603
  - Suppression de la taille de la file d'attente, 603
- audit\_class*, fichier
  - Ajout d'une classe, 595–596
  - Dépannage, 596
- audit\_event*, fichier
  - Description, 554
  - Modification de l'appartenance à une classe, 596–597
  - Suppression d'événements en toute sécurité, 636–637
- audit\_flags*, mot-clé, 585

*audit\_flags*, mot-clé (*Suite*)

- Spécification des exceptions utilisateur à la présélection d'audit, 586–590
- Utilisation, 648
- Utilisation du préfixe de caret (^), 588
- audit.notice*, entrée, *syslog.conf*, fichier, 605
- audit\_remote*, plug-in, 557–558
  - Définition des attributs, 604–605
  - Obtention des attributs, 604–605
- audit\_syslog*, plug-in, 557–558
- audit\_warn*, script
  - Configuration, 594–595
  - Description, 645
- auditconfig*, commande
  - Affichage de la présélection d'audit par défaut, 585–586
  - Affichage des paramètres par défaut, 583–585
  - Ajout de systèmes de fichiers d'audit, 601–604
  - Classes d'audit en tant qu'arguments, 556
  - Configuration de la stratégie, 590–592
  - Configuration des contrôles de file d'attente, 592–594
  - Définition *audit\_binfile*, attributs, 601–604
  - Définition *audit\_remote*, attributs, 604–605
  - Définition de la stratégie d'audit active, 591–592
  - Définition de la stratégie d'audit temporairement, 591–592
  - Définition de paramètres d'audit à l'échelle du système, 556
  - Définition de stratégie d'audit, 633
  - Description, 645
  - Envoi de fichiers dans un référentiel distant, 604–605
  - getplugin, option, 604–605, 605–606
  - Options de contrôle de file d'attente, 592–594
  - Options de stratégie, 590–592
  - Présélection des classes d'audit, 585–586
  - setflags, option, 585–586
  - setnaflags, option, 585–586
  - setplugin, option, 604–605, 605–606
- auditd*, démon
  - Actualisation du service d'audit, 611, 612
- auditlog*, fichier, Enregistrements d'audit au format texte, 605

**auditrecord, commande**

- [ ] (Crochets) dans la sortie, 654
- Affichage des définitions d'enregistrement d'audit, 615–617
- Description, 646
- Exemple, 616
- Jetons facultatifs ([ ]), 654
- Liste de tous les formats, 616
- Liste des formats de classe, 616–617
- Liste des formats de programme, 616

**auditreduce, commande**

- A, option, 618–619
- b, option, 620
- C, option, 618
- c, option, 621
- D, option, 619
- d, option, 621
- e, option, 620
- Exemple, 617–619
- Fusion d'enregistrements d'audit, 617–619
- Jeton de bloc de fin, 663
- M, option, 619
- Nettoyage de fichiers d'audit, 623–624
- O, option, 617–619, 620
- Options de filtrage, 619
- Sélection des enregistrements d'audit, 619–621
- Utilisation d'option majuscules, 618
- Utilisation d'options minuscules, 619
- Utilisation de l'horodatage, 617

**auditreduce commande, Description, 646****auditstat, commande, Description, 646****auth\_attr, base de données**

- Description, 221
- Résumé, 220

**AUTH\_DES, authentification, Voir AUTH\_DH, authentification****AUTH\_DH, authentification, NFS, 287****Authenticateur**

- Kerberos, 536, 542

**Authentification**

- AUTH\_DH, session client-serveur, 289–292
- Authentification DH, 288–292
- Configuration inter-domaine, 397–400
- Désactivation à l'aide de l'option -X, 526

**Authentification (Suite)**

- Description, 53–55, 314
- Fichier monté via NFS, 296
- Fichiers montés via NFS, 295
- Kerberos et, 349
- Présentation de Kerberos, 540
- RPC sécurisé, 287
- Secure Shell
  - Méthode, 314–315
  - Processus, 334–335
- Sécurité réseau, 53–55

**authentification, Services de noms, 287****Authentification**

- Terminologie, 535–536
- Type, 53–55
- Utilisation avec NFS, 287

**Authentification avec clé publique, Secure Shell, 314****Authentification basée sur l'hôte, Configuration dans Secure Shell, 318–320****Authentification DH**

- Client NIS, 293–294
- Configuration dans NIS, 293–294
- Description, 288–292
- Montage de fichiers, 296
- Partage de fichiers, 295–296

**Authentification Diffie-Hellman, Voir Authentification DH****Authentification du mot de passe, Secure Shell, 314****Authentification inter-domaine,**

- Configuration, 397–400

**Authentification Kerberos, RPC sécurisé, 288****authlog, fichier, Enregistrement des tentatives de connexion ayant échoué, 64–66****authorized\_keys, fichier, Description, 343****AuthorizedKeysFile, mot-clé, Fichier sshd\_config, 337****auths, commande, Description, 223****AUTHS\_GRANTED, mot-clé, policy.conf, fichier, 222****auto\_transition, option, SASL, 311****Automatisation de création de principal, 481****Autorisation**

- ACL, 51
- ACL UFS, 130–131

**Autorisation (*Suite*)**

- Autorisation de fichier
    - Autorisation spéciale, 127, 130
    - Description, 125
    - Mode absolu, 128, 137–138
    - Mode symbolique, 128, 129, 136
    - Modification, 128–130, 136
  - Autorisation de fichier spéciale, 130
  - Autorisation du répertoire, 125
  - Autorisation spéciale, 127
  - Autorisations de fichier spéciales, 125–127
  - Classe d'utilisateur, 124
  - Défaut, 127–128
  - Modification des autorisations de fichier
    - chmod, commande, 124
    - Mode absolu, 128, 137–138
    - Mode symbolique, 128, 129, 136
  - Recherche de fichiers avec autorisations
    - setuid, 139
  - setgid, autorisation
    - Description, 126–127
    - Mode absolu, 130, 139
    - Mode symbolique, 129
  - setuid, autorisation
    - Description, 126
    - Mode absolu, 130, 139
    - Mode symbolique, 129
    - Risque de sécurité, 126
  - Sticky bit, 127
  - Type, 53–55
  - Valeur umask, 127–128
- Autorisation (RBAC)**
- Allocation de périphériques, 87, 97–98
  - Base de données, 220–223
  - Commandes nécessitant des autorisations, 224–225
  - Convention de nommage, 219
  - Définition, 152–153
  - Délégation, 219
  - Description, 149, 218–219
  - Granularité, 219
  - Non requise pour l'allocation de périphériques, 89
  - solaris.device.allocate, 87, 97
  - Vérification dans une application privilégiée, 155
- Autorisation d'écriture, Mode symbolique, 129**

- Autorisation d'exécution, Mode symbolique, 129
- Autorisation de fichier, mode
  - Mode absolu, 128
  - Mode symbolique, 129
- Autorisation de lecture, Mode symbolique, 129
- Autorisation spéciale
  - setgid, autorisation, 126–127
  - setuid, autorisation, 126
  - Sticky bit, 127
- Autorisations
  - Allocation de périphériques, 96–97
  - Dépannage, 189–192
  - Kerberos et, 349
- Autorisations (RBAC)
  - Recherche de caractères génériques, 189
  - solaris.device.revoke, 98
- auxprop\_login, option, SASL, 311
- Avertissement d'expiration de ticket, 421

**B**

- b, option, auditreduce, commande, 620
- Banner, mot-clé, sshd\_config, fichier, 337
- BART
  - Composant, 104–106
  - Considérations de sécurité, 107
  - Liste des tâches, 107–108
  - Présentation, 103–106
  - Sortie détaillée, 121
  - Sortie programmatique, 121
- bart, commande, 103
- bart compare, commande, 105
- bart create, commande, 104–105, 108
- Base de données
  - auth\_attr, 221
  - Clé secrète NFS, 289
  - Création de KDC, 382
  - cred pour RPC sécurisé, 289
  - exec\_attr, 222
  - prof\_attr, 222
  - publickey pour RPC sécurisé, 289
  - RBAC, 220–223
  - Sauvegarde et propagation de KDC, 433–434
  - user\_attr, 220–221

Base de données utilisateur (RBAC), *Voir* `user_attr`,  
base de données  
Bases de données, Propagation de KDC, 369  
Basic Solaris User (utilisateur Solaris de base), RBAC,  
Profil de droits, 216  
Batchmode, mot-clé, Fichier `ssh_config`, 337  
Bibliothèque PKCS #11  
Ajout d'une bibliothèque de fournisseurs, 259–260  
Structure cryptographique, 233  
Bibliothèques, Fournisseurs au niveau de  
l'utilisateur, 255  
BindAddress, mot-clé, Fichier `ssh_config`, 337  
Blowfish, algorithme de chiffrement  
Autorisation dans un environnement  
hétérogène, 67  
Fichier `ssh_config`, 337  
Blowfish, algorithme de chiffrement, Fournisseur de  
noyau, 255  
Blowfish, algorithme de chiffrement  
`policy.conf`, fichier, 67  
blowfish-cbc, algorithme de chiffrement, Fichier  
`ssh_config`, 337

## C

-C, option, `auditreduce`, commande, 618  
Shell C, Version privilégiée, 156–157  
-c, option  
auditrecord, commande, 616–617  
auditreduce, commande, 621  
Cache, Informations d'identification, 540  
Calcul  
Clé DH, 294  
Clé secrète, 240–242, 243–247  
MAC d'un fichier, 248–250  
Synthèse d'un fichier, 247–248  
canon\_user\_plugin, option, SASL, 311  
Caractère générique  
Autorisation RBAC, 219  
Hôte de Secure Shell, 331  
Caractéristiques d'un audit, ID de session, 652  
Caractéristiques d'un audit de processus, ID de session  
d'audit, 652

Caractéristiques de l'audit  
ID du terminal, 652  
ID utilisateur d'audit, 652  
Masque de présélection de processus  
utilisateur, 651  
Processus, 651–652  
Caractéristiques de l'audit de processus  
ID du terminal, 652  
ID utilisateur d'audit, 652  
Masque de présélection de processus, 651  
caret (^), Modificateur de préfixe de classe d'audit, 648  
caret (^) dans les préfixes de classe d'audit, 586–590  
Caret (^) dans les préfixes de classe d'audit, 634  
Carte Sun Crypto Accelerator 1000, Liste des  
mécanismes, 265–267  
Carte Sun Crypto Accelerator 6000  
Liste des mécanismes, 264–265  
Plug-in matériel dans la structure  
cryptographique, 233  
Secure Shell et FIPS-140, 317  
cdrw, commande, Autorisation requise, 224  
Certificat  
Export pour l'utilisation par un autre  
système, 276–277  
Génération avec la commande `pktool`  
gencert, 273–274  
Importation dans le keystore, 274–275  
Certificat X.509 v3, Génération, 282–283  
Certificats  
Signature d'une CSR PKCS #10  
Utilisation de la commande `pktool`, 282–283  
ChallengeResponseAuthentication, mot-clé, *Voir*  
KbdInteractiveAuthentication, mot-clé  
Champ d'application (RBAC), Description, 157  
CheckHostIP, mot-clé, `ssh_config`, fichier, 337  
Cheval de Troie, 47  
chgrp, commande  
Description, 124  
Syntaxe, 135  
Chiffrement  
Algorithme  
Kerberos, 372  
Algorithme de mot de passe, 40  
Algorithme DES, 288

Chiffrement (*Suite*)

- Clé privée des utilisateurs NIS, 294
  - Communication entre hôtes, 326
  - encrypt, commande, 250–253
  - Fichier, 51
  - Fichiers, 240, 250–253
  - Génération de la clé symétrique
    - Utilisation de la commande dd, 240–242
    - Utilisation de la commande pktool, 243–247
  - Liste des algorithmes de mot de passe, 40
  - Modes
    - Kerberos, 372
  - Mots de passe, 66–69
  - NFS sécurisé, 288
  - Option -x, 526
  - Service de confidentialité, 349
  - Spécification de l'algorithme de mot de passe
    - Localement, 66–69
  - Spécification des algorithmes dans le fichier
    - ssh\_config, 337
  - Spécification des algorithmes de mot de passe dans le
    - fichier policy.conf, 40
  - Trafic réseau entre hôtes, 313–315
  - Types
    - Kerberos, 372, 544–546
  - Utilisation des commandes au niveau de
    - l'utilisateur, 236
- Chiffrement DES, NFS sécurisé, 288
- chkey, commande, 289, 294
- chmod, commande
- Description, 124
  - Modification des autorisations spéciales, 138–139, 139
  - Syntaxe, 138
- Choix, Votre mot de passe, 519–520
- chown, commande, Description, 124
- ChrootDirectory, mot-clé, ssh\_config, fichier, 337
- Cipher, mot-clé, Fichier ssh\_config, 337
- Ciphers, mot-clé, Secure Shell, 337
- Classe d'audit
- Ajout, 595–596
  - Description, 552
  - Mappage d'événements, 556
  - Modification des valeurs par défaut, 595–596

Classe d'audit (*Suite*)

- Présélection, 554
  - Présentation, 555–556
  - Syntaxe, 648
- Classe d'utilisateur, fichier, 124
- Classes, *Voir* Classes d'audit
- Classes d'audit
- Affichage des paramètres par défaut, 583–585
  - Configuration, 647–648
  - Description, 554
  - Exceptions aux paramètres à l'échelle du
    - système, 556
  - Exceptions utilisateur, 586–590
  - Masque de présélection de processus, 651
  - Postsélection, 554
  - Préfixes, 648
  - Présélection
    - Portant sur l'échec, 588
    - Portant sur la réussite, 588
    - Pour l'échec, 606
    - pour l'échec, 605
    - Pour la réussite, 605, 606
    - Réussite ou échec, 585–586
  - Remplacement, 585–586
  - Syntaxe, 648
- Clé
- Création d'une clé DH pour utilisateur
    - NIS, 294–295
  - Création pour Secure Shell, 323–325
  - Génération de la clé symétrique
    - Utilisation de la commande dd, 240–242
    - Utilisation de la commande pktool, 243–247
  - Génération pour Secure Shell, 323–325
  - Utilisation pour le code MAC, 249–250
- Clé commune
- Authentification DH, 288–292
  - Calcul, 291
- Clé de conversation
- Déchiffrement dans le RPC sécurisé, 291
  - Génération dans le RPC sécurisé, 290
- Clé privée
- Voir aussi* Clé secrète
  - Fichier d'identité Secure Shell, 342



- Clé publique
  - Authentification DH, 288–292
  - Fichier d'identité Secure Shell, 342
  - Génération d'une paire de clés, 323–325
  - Modification de la phrase de passe, 325
- Clé secrète
  - Création, 240–242, 243–247
  - Génération
    - Utilisation de la commande `dd`, 240–242
    - Utilisation de la commande `pktool`, 243–247
  - Génération pour le RPC sécurisé, 289
- `clear`, niveau de protection, 527
- `ClearAllForwardings`, mot-clé, Transmission de port Secure Shell, 337
- Clés
  - Clé de service, 508–514
  - Clés de session
    - Authentification Kerberos, 540
    - Définition dans Kerberos, 535
    - Génération d'une paire de clés
      - Utilisation de la commande `pktool`, 278–282
- Clés de service
  - Définition dans Kerberos, 535
  - Keytab, fichier, 508–514
- Clés de session
  - Authentification Kerberos, 540
  - Définition dans Kerberos, 535
- Clés privées, Définition dans Kerberos, 535
- Client
  - `AUTH__DH`, session client-serveur, 289–292
  - Configuration de Kerberos, 410–427
  - Configuration pour Secure Shell, 334, 336
  - Définition dans Kerberos, 535
- `ClientAliveCountMax`, mot-clé, Fichier `ssh_config`, 337
- `ClientAliveInterval`, mot-clé, Fichier `ssh_config`, 337
- `clntconfig`, principal
  - Création, 383, 390
- `cmd`, jeton d'audit, 657
- `cnt`, stratégie d'audit
  - Avec la stratégie `ahlt`, 650–651
  - Description, 575
- Code d'authentification des messages (MAC), Calcul pour un fichier, 248–250
- Combinaison de fichiers d'audit
  - `auditreduce`, commande, 617–619
  - Différentes zones, 647
- Commande
  - Commande cryptographique au niveau de l'utilisateur, 236
  - Commande d'administration RBAC, 223–224
  - Commande d'allocation de périphériques, 97
  - Commande de la stratégie de périphériques, 95
  - Commande de la structure cryptographique, 235–236
  - Commande de protection de fichier, 123
  - Commande du RPC sécurisé, 289
  - Commande Secure Shell, 344–346
  - Détermination des commandes privilégiées d'un utilisateur, 207–208
  - Kerberos, 533–534
  - Privilège d'administration, 225
  - Vérification des privilèges, 154
- Commande Kerberos, Activation d'applications utilisant Kerberos uniquement, 452
- Commande `kpasswd`, Commande `passwd`, 520
- Commande `shell`, Transfert de numéro de processus de `shell`, 210
- Commandes
  - Voir aussi* Commandes individuelles
  - Affectant des privilèges, 164
- Composant
  - BART, 104–106
  - Mécanisme d'allocation de périphériques, 96
  - RBAC, 149–151
  - Session utilisateur Secure Shell, 335
- Compression, les Fichiers d'audit sur le disque, 638–639
- Compression, mot-clé, Secure Shell, 337
- `CompressionLevel`, mot-clé, Fichier `ssh_config`, 337
- Compte utilisateur
  - Voir aussi* Utilisateur
  - Affichage de l'état de connexion, 61–62
  - Affichage de l'état de connexion, 61–62
- Comptes utilisateur, Modification du mot de passe `root`, 61



- Computer Emergency Response Team/Coordination Center (CERT/CC), 57
- Confidentialité
  - Disponibilité, 527
  - Kerberos et, 349
  - Service de sécurité, 357
- Configuration
  - ahlt, stratégie d'audit, 591
  - Allocation de périphériques, 85–86
  - Audit, 582–597
  - audit\_class, fichier, 595–596
  - Audit de zones, 647
  - audit\_event, fichier, 596–597
  - Audit identique pour les zones non globales, 607–609
  - Audit par zone, 564–565, 609–610
  - audit\_warn, script, 594–595
  - Authentification basée sur l'hôte pour Secure Shell, 318–320
  - Classes d'audit, 585–586
  - Clé DH dans NIS, 293–294
  - Clé DH pour utilisateur NIS, 294–295
  - Contrôle du dépassement de la piste d'audit, 624–625
  - Contrôles de file d'attente d'audit, 592–594
  - Espace pour la piste d'audit, 601–604
  - Exceptions aux valeurs par défaut du système Secure Shell, 321–322
  - Kerberos
    - Ajout de principal d'administration, 382, 389
    - Authentification inter-domaine, 397–400
    - Client, 410–427
    - Liste des tâches, 375–376
    - Présentation, 375–454
    - Serveur KDC esclave, 391–392, 392–393, 393–396
    - Serveur KDC maître, 378–379, 379–380, 380–384
    - Serveur KDC maître utilisant LDAP, 384–391
    - Serveurs NFS, 404–405
  - Liste des tâches de l'audit, 582–583
  - Liste des tâches de périphériques, 81
  - Liste des tâches des journaux d'audit, 597–598
  - Liste des tâches RBAC, 177–178
- Configuration (*Suite*)
  - Liste des tâches Secure Shell, 318
  - Mot de passe pour l'accès au matériel, 71–72
  - perzone, stratégie d'audit, 592
  - Profils de droits, 186–187
  - RBAC, 177–192
  - Résumés textuels des enregistrements d'audit, 605–606
  - Rôle root en tant qu'utilisateur, 202–204
  - Rôles, 181–183, 194–195
  - Secure Shell, 317
    - Client, 336
    - Serveur, 336
  - Sécurité du matériel, 71–73
  - Stratégie d'audit, 590–592
  - Stratégie d'audit active, 591–592
  - Stratégie d'audit permanente, 590–592
  - Stratégie d'audit temporaire, 590–592
  - Stratégie d'audit temporairement, 591–592
  - Stratégie de périphériques, 82
  - Stratégie du service d'audit, 590–592
  - Transfert de port dans Secure Shell, 321
  - Utilisateurs privilégiés, 197
- Configuration automatique
  - Kerberos
    - Serveur KDC esclave, 391–392
    - Serveur KDC maître, 378–379
- Configuration des serveurs d'application, 400–403
- Configuration du pare-feu Internet, 55–56
- Configuration du service de noms, Restrictions de l'accès de connexion, 38
- Configuration interactive
  - Kerberos
    - Serveur KDC esclave, 392–393
    - Serveur KDC maître, 379–380
- Configuration manuelle
  - Kerberos
    - Serveur KDC esclave, 393–396
    - Serveur KDC maître, 380–384
    - Serveur KDC maître utilisant LDAP, 384–391
- ConnectionAttempts, mot-clé, Fichier ssh\_config, 337
- ConnectTimeout, mot-clé, ssh\_config, fichier, 337

## Connexion

- Affichage de l'état de connexion d'un utilisateur, 61–62
- Audit des connexions, 639–640
- Contrôle des échecs, 63–64
- Désactivation temporaire, 63
- Jeu de privilèges de base des utilisateurs, 163
- Liste des tâches, 60–61
- root, connexion

- Suivi, 46

- Secure Shell, 325–326

### Sécurité

- Contrôle d'accès au système, 38
  - Contrôle d'accès des périphériques, 43
  - Enregistrement des tentatives ayant échoué, 63–64
  - Restriction d'accès, 38
  - Restrictions d'accès, 38
  - Suivi de connexion root, 46

## Connexion à distance

- Empêcher le superutilisateur, 70–71
- Sécurité, 291

## Connexion automatique

- Activation, 525
- Désactivation, 526

## Connexion distante

- Authentification, 53–55
- Autorisation, 53–55

## Connexion sécurisée

- Connexion, 325–326
- Pare-feu, 330

## Console, Affichage des tentatives de la commande su, 70–71

## CONSOLE dans Secure Shell, 341

## CONSOLE\_USER, mot-clé, `policy.conf`, fichier, 222

## Console User (utilisateur de la console), RBAC, Profil de droits, 216

## Consommateurs, Définition dans la structure cryptographique, 234

## Consultation

- Définition d'enregistrement d'audit, 615–617
- Enregistrements d'audit XML, 622
- Fichiers d'audit binaires, 621–623

## Contrôle

- Accès système, 59–60
- Connexion ayant échoué, 63–64
- Superutilisateur, 69–71
- Tentative d'accès superutilisateur, 70–71
- Tentative de la commande su, 69–70
- Utilisation du système, 46–50

## Contrôle d'accès basé sur les rôles, Voir RBAC

## Contrôle de ressources

- Privilège, 162
- `project.max-locked-memory`, 162
- `zone.max-locked-memory`, 162

## Contrôle des coûts, Audit, 576

## Contrôle du dépassement, Piste d'audit, 624–625

## Contrôle du dépassement de stockage, Piste d'audit, 624–625

## Contrôles de file d'attente d'audit, Obtention, 592–594

## Contrôles de la file d'attente d'audit, Affichage des paramètres par défaut, 583–585

## Convention de nommage

- Autorisation RBAC, 219
- Fichier d'identité Secure Shell, 342
- Périphérique, 88

## Conventions de nommage, Fichiers d'audit, 652

## Conversion, Enregistrement d'audit dans un format lisible, 622

## Copie, Fichier à l'aide de Secure Shell, 329–330

## Copie de messages dans un fichier unique, 621

## Courrier, Utilisation avec Secure Shell, 329

## Coût du stockage, Audit, 577–578

## Coût du temps de traitement, Service d'audit, 576

## `crammd5.so.1`, plug-in, SASL, 310

## Création

- Clé secrète
  - Chiffrement, 240–242, 243–247
- Clé Secure Shell, 323–325
- Espace de stockage pour les fichiers d'audit binaires, 598–601
- Fichier stash, 396, 443
- Nouveau principal (Kerberos), 486–488
- Nouveau script de nettoyage de périphériques, 102
- Nouvelle stratégie (Kerberos), 486, 499–500
- Paire de clés, 278–282
- Piste d'audit, 652

**Création (Suite)**

- Profil de droits pour un groupe d'utilisateurs, 589–590
- Profils de droits, 186–187
- Rôles, 181–183
- root, utilisateur, 202–204
- Synthèse de fichier, 247–248
- Table d'informations d'identification, 405–406
- Tickets avec kinit, 516
- Utilisateurs privilégiés, 197
- cred, base de données, Authentification DH, 288–292
- cred, table
  - Authentification DH, 289
  - Informations stockées par le serveur, 291
- Crochets ([ ]), audit record, sortie, 654
- crontab, fichier, Autorisation requise, 224
- crypt, commande, Sécurité de fichier, 51
- CRYPT\_ALGORITHMS\_ALLOW, mot-clé, policy.conf, fichier, 41
- CRYPT\_ALGORITHMS\_DEPRECATED, mot-clé, policy.conf, fichier, 41
- crypt\_bsdbf, algorithme de mot de passe, 40
- crypt\_bsdmd5, algorithme de mot de passe, 40
- CRYPT\_DEFAULT, mot-clé, policy.conf, fichier, 41
- CRYPT\_DEFAULT, variable système, 66
- crypt\_sha256, algorithme de mot de passe, 40
- crypt\_sha256, algorithme de mots de passe, 66–69
- crypt\_sunmd5, algorithme de mot de passe, 40
- crypt\_unix, algorithme de mot de passe, 40
- cryptoadm, commande
  - Désactivation de mécanismes cryptographiques, 260, 262
  - Désactivation de mécanismes matériels, 265–267
  - Description, 235
  - Installation d'une bibliothèque PKCS #11, 260
  - Liste des fournisseurs, 255
  - m, option, 260, 262
  - p, option, 260, 262
  - Restauration d'un fournisseur de logiciels noyau, 262
- cryptoadm install, commande, Installation d'une bibliothèque PKCS #11, 260
- Cryptographie par clé publique
  - AUTH\_\_DH, session client-serveur, 289–292

**Cryptographie par clé publique (Suite)**

- Base de données de clés publiques pour le RPC sécurisé, 289
- Clé commune
  - Calcul, 291
- Clé secrète NFS, 289
- Génération de clés
  - Clé de conversation pour NFS sécurisé, 290
  - Utilisation de Diffie-Hellman, 289
- Modification des clés publiques NFS et clés secrètes, 289
- Cryptoki, Voir Bibliothèque PKCS #11
- csh, commande, Version privilégiée, 156–157
- CSR PKCS #10
  - Signature
    - Utilisation de la commande pktool, 282–283

**D**

- D, option
  - auditreduce, commande, 619
  - ppriv, commande, 211
- d, option
  - auditreduce, commande, 620, 621
- Data Encryption Standard, Voir Chiffrement DES
- dd, commande, Génération de clés secrètes, 240–242
- deallocate, commande
  - Autorisation requise, 225
  - Autorisations, 98
  - Etat d'erreur d'allocation, 98
  - Script de nettoyage de périphériques, 102
  - Utilisation, 93–94
- Débogage, Privilège, 211
- Débogage du numéro de séquence, 662
- Déchiffrement
  - Clé de conversation pour le RPC sécurisé, 291
  - Clé secrète, 289
  - Clé secrète NFS, 289
  - Fichier, 252
- Décision de configuration
  - Audit
    - Personne et objet à auditer, 570–573
    - Stockage de fichiers, 569–570
    - Stratégie, 573–576

Décision de configuration, Audit (*Suite*)

Zone, 568–569

## Kerberos

Client, 369–370

KDC, serveur, 371

Synchronisation d'horloge, 369

## Décisions de configuration

Algorithme de mot de passe, 40

## Kerberos

Domaines, 364–365

Hiérarchie de domaine, 365

KDC esclaves, 367

Mappage de noms d'hôtes sur domaines, 365

Nombre de domaines, 364–365

Noms de clients et de principal de service, 366

Noms de domaines, 364

Ports, 367

Propagation de base de données, 369

Types de chiffrement, 372

## decrypt, commande

Description, 236

Syntaxe, 252

## default/login, fichier, Description, 343

## default\_realm, section

Fichier krb5.conf, 381, 387

## Défaut, Valeur umask, 127–128

## Définition

arge, stratégie, 633

argv, stratégie, 633

Contrôles de file d'attente d'audit, 592–594

Stratégie d'audit, 590–592

## Délégation, Autorisation (RBAC), 219

## delete\_entry, commande, ktutil, commande, 513

Demandes de signature de certificat (CSR), *Voir*

## Certificats

## Démarrage

Allocation de périphériques, 86

Audit, 614

Démon KDC, 396, 443

Serveur de clés RPC sécurisé, 293

## Démon

Exécution avec des privilèges, 161

nscd (name service cache daemon, démon cache de service de noms), 223

Démon (*Suite*)

ssh-agent, 327–328

sshd, 333–335

Table de Kerberos, 534

## Démon de l'agent, Secure Shell, 327–328

## Démons

kcfd, 235

keyserv, 293

## Démontage, Périphériques alloués, 94

## DenyGroups, mot-clé, Fichier sshd\_config, 337

## DenyUsers, mot-clé, Fichier sshd\_config, 337

## Dépannage

Accès superutilisateur à distance, 71

Allocation d'un périphérique, 92

Audit, 626–627

## Classe d'audit

Personnalisation, 596

Personnalisée, 628

## Désactivation de l'utilisation de piles exécutables par

les programmes, 141

## encrypt, commande, 253

## Kerberos, 470

## list\_devices, commande, 88

## Montage d'un périphérique, 93

## Plug-in actif, 628

## praudit, commande, 623

## Privilège manquant, 211–213

## Privilège requis, 211–213

## Propriétés de sécurité, 189–192

## Recherche de fichiers avec autorisations

setuid, 139

## root en tant que rôle, 204

## Tentative d'intrusion dans un ordinateur, 63–64

## Terminal d'origine de la commande su, 69

## Utilisateur exécutant des commandes

privilégiées, 207–208

## DES, chiffrement, Fournisseur de noyau, 255

## Désactivation

Abandon clavier, 72–73

Accès root à distance, 70–71

Allocation de périphériques, 86

Arrêt clavier, 72–73

Connexion utilisateur, 63

**Désactivation (*Suite*)**

- Fichiers exécutables 32 bits causant des problèmes de sécurité, 131–132
- Journalisation des messages de pile exécutable, 141
- Mécanisme cryptographique, 260
- Mécanisme matériel, 265–267
- Piles exécutables, 141
- Séquence d'abandon, 72–73
- Séquence d'abandon système, 72–73
- Service d'audit, 613–614
- Service sur un hôte (Kerberos), 512–514
- Stratégie d'audit, 590–592
- Temporaire des connexions, 63
- Utilisation de pile exécutable par un programme, 141

Désinstallation, Fournisseur cryptographique, 261

Destruction, Ticket avec `kdestroy`, 518

Détermination

- ID d'audit d'un utilisateur, 636
- Liste des tâches des privilèges, 204
- Privilèges sur un processus, 209–211

Déterminer, Fichiers avec autorisations `setuid`, 139

`/dev/arp`, périphérique, Récupération d'informations IP MIB-II, 84–85

`/dev/urandom`, périphérique, 240–242

`devfsadm`, commande, Description, 95

`device_allocate`, fichier

- Description, 99–101
- Exemple, 89, 99
- Format, 100

`device_maps`, fichier

- Description, 98
- Exemple d'entrée, 98
- Format, 98

`digest`, commande

- Description, 236
- Exemple, 248
- Syntaxe, 247

`digestmd5.so.1`, plug-in, SASL, 310

Diminution, Espace disque requis pour les fichiers d'audit, 638–639

`DisableBanner`, mot-clé, `ssh_config`, fichier, 337

Disque dur, Espace requis pour l'audit, 577–578

`dminfo`, commande, 98

DNS, Kerberos, 366

`domain_realms`, section

- Fichier `krb5.conf`, 381, 387
- `krb5.conf`, fichier, 365

Domaine (Kerberos)

- Configuration de l'authentification inter-domaine, 397–400
- Direct, 399–400
- Hiérarchique, 397–398

Domaine direct, 399–400

Domaine hiérarchique, Configuration, 397–398

Domaines (Kerberos)

- Contenu, 356
- Décisions de configuration, 364–365
- Hiérarchie, 365
- Hiérarchiques ou non hiérarchiques, 355–356
- Mappage de noms d'hôtes, 365
- Nombre, 364–365
- Noms, 364
- Noms de principal, 355
- Serveurs, 356
- Ticket requis pour un domaine spécifique, 526

Domaines hiérarchiques, Kerberos, 355–356

Domaines non hiérarchiques, Kerberos, 355–356

Droit, *Voir* Profil de droits

Droits

- Limitation d'un administrateur aux droits affectés de manière explicite, 199–201
- Limitation des utilisateurs aux applications de bureau, 198–199

`DSAAuthentication`, mot-clé, *Voir*

- `PubkeyAuthentication`, mot-clé

Duplication, Principaux (Kerberos), 489

Durée de vie du ticket, Kerberos, 538–539

`DynamicForward`, mot-clé, Fichier `ssh_config`, 337

**E**

- `-e`, option
  - `auditreduce`, commande, 620
  - `ppriv`, commande, 211
- Ecart d'horloge
  - Kerberos, 427–428
  - Planification Kerberos, 369

- ECC, fournisseur de noyau, 255
- Echange de KDC maître et esclaves, 428–433
- Echec, Préfixe de classe d'audit, 648
- eprom, commande, 38, 71–73
- Efficacité, Audit, 578
- eject, commande, Nettoyage d'un périphérique, 102
- elfsign, commande, Description, 236
- Emplacement, Définition dans la structure
  - cryptographique, 235
- encrypt, commande
  - Dépannage, 253
  - Description, 236
  - Messages d'erreur, 253
  - Syntaxe, 241
- Endossement d'un rôle
  - Fenêtre de terminal, 174–175
  - Procédure, 177–192
- Enregistrement, Tentative de connexion ayant échoué, 63–64
- Enregistrement d'audit
  - Affichage au format XML, 622
  - Affichage des formats d'une classe d'audit, 616–617
  - Conversion dans un format lisible, 622
  - Description, 553
  - Événement générateur, 562
  - Format, 653
  - Fusion, 617–619
  - Présentation, 557
  - Réduction de fichiers d'audit, 617–619
  - Séquence de jetons, 653
- Enregistrement des fournisseurs, Structure cryptographique, 237
- Enregistrements d'audit
  - Affichage, 621–623
  - Affichage des définitions
    - Procédure, 615–617
  - Affichage des formats d'un programme, 616
  - Copie dans un fichier unique, 621
  - Exemple de formatage, 616
  - Modificateurs d'événement, 658
  - /var/adm/auditlog, fichier, 605
- Equivalents de ligne de commande de l'outil SEAM, 477
- Erreur, Etat d'erreur d'allocation, 98
- EscapeChar, mot-clé, Fichier ssh\_config, 337
- Esclaves, KDC, Echange avec un KDC maître, 428–433
- Espace disque, Pour les fichiers d'audit binaires, 598–601
- Espace disque requis, Fichiers d'audit, 577–578
- Etat d'erreur d'allocation, 98
- /etc/default/kbd, fichier, 72–73
- /etc/default/login, fichier
  - Description, 343
  - Paramètre de connexion par défaut, 64
  - Restriction de l'accès root à distance, 70–71
  - Secure Shell, 341–342
- /etc/default/su, fichier
  - Affichage des tentatives de la commande su, 70–71
  - Contrôle de la commande su, 69–70
  - Contrôle des tentatives d'accès, 70–71
- /etc/hosts.equiv, fichier, Description, 343
- /etc/krb5/kadm5.acl, fichier, Description, 531
- /etc/krb5/kadm5.keytab, fichier, Description, 532
- /etc/krb5/kdc.conf, fichier, Description, 532
- /etc/krb5/kpropd.acl, fichier, Description, 532
- /etc/krb5/krb5.conf, fichier, Description, 532
- /etc/krb5/krb5.keytab, fichier, Description, 532
- /etc/krb5/warn.conf, fichier, Description, 532
- /etc/logindevperm, fichier, 43
- /etc/nologin, fichier
  - Désactivation temporaire des connexions utilisateur, 63
  - Description, 343
- /etc/pam.conf, fichier, Kerberos, 532
- /etc/publickey, fichier, Authentification DH, 289
- /etc/security/device\_allocate, fichier, 99
- /etc/security/device\_maps, fichier, 98
- /etc/security/policy.conf, fichier, Configuration des algorithmes, 66–67
- /etc/ssh/crsh, fichier, Description, 344
- /etc/ssh\_host\_dsa\_key.pub, fichier,
  - Description, 343
- /etc/ssh\_host\_key.pub, fichier, Description, 343
- /etc/ssh\_host\_rsa\_key.pub, fichier,
  - Description, 343
- /etc/ssh/les, fichier, Remplacement, 344
- /etc/ssh/shosts.equiv, fichier, Description, 343

- /etc/ssh/ssh\_config, fichier
    - Configuration de Secure Shell, 336
    - Description, 344
    - Mot-clé, 336–342
    - Paramètre spécifique à l'hôte, 341
    - Remplacement, 344
  - /etc/ssh/ssh\_host\_dsa\_key, fichier,
    - Description, 342
  - /etc/ssh/ssh\_host\_key, fichier, Remplacement, 344
  - /etc/ssh/ssh\_host\_rsa\_key, fichier,
    - Description, 342
  - /etc/ssh/ssh\_known\_hosts, fichier
    - Contrôle de la distribution, 342
    - Description, 343
    - Distribution sécurisée, 342
  - /etc/ssh/sshd\_config, fichier
    - Description, 342
    - Mot-clé, 336–342
  - /etc/syslog.conf, fichier
    - Audit, 605, 646
    - Connexion ayant échoué, 64–66
    - Message de pile exécutable, 132
    - PAM, 302
  - Événement, Description, 554
  - Événement d'audit
    - Mappage avec des classes, 556
    - Modification de l'appartenance à une classe, 596–597
    - Résumé, 552
    - Sélection dans une piste d'audit dans les zones, 647
    - Sélection de piste d'audit, 619–621
  - Événements d'audit
    - Asynchrones, 650–651
    - audit\_event, fichier, 554
    - Consultation dans les fichiers binaires, 621–623
    - Description, 554
    - Suppression du fichier audit\_event, 636–637
  - Événements d'audit asynchrones, 650–651
  - exec\_args, jeton d'audit, argv, stratégie, 657
  - exec\_args; jeton d'audit, Format, 657
  - exec\_attr, base de données
    - Description, 222
    - Résumé, 220
  - exec\_env, jeton d'audit, Format, 657–658
  - Exécutable, pile, Désactivation de la journalisation des messages, 141
  - Exécution des commandes, Secure Shell, 335
  - Exigence en matière de réutilisation des objets
    - Script de nettoyage de périphériques
    - Écriture de nouveaux scripts, 102
  - Exigences en matière de réutilisation des objets
    - Script de nettoyage de périphériques
    - Lecteur de bande, 101
  - export, sous-commande, pktool,
    - commande, 276–277
- ## F
- f, option
    - Commandes utilisant Kerberos, 525, 527–528
    - st\_clean, script, 102
  - F, option
    - Commandes utilisant Kerberos, 526, 527–528
    - deallocate, commande, 98
  - FallBackToRsh, mot-clé, Fichier ssh\_config, 337
  - fd\_clean, script, Description, 102
  - fe, modificateur d'événement d'audit, 658
  - Fichier
    - Administration de Secure Shell, 342
    - Affichage d'informations, 124
    - Affichage de fichier caché, 133
    - Affichage des informations de fichier, 133–134
    - Audit des modifications, 633–635
    - Autorisation
      - Défaut, 127–128
      - Description, 125
      - Mode absolu, 128, 137–138
      - Mode symbolique, 128, 129, 136
      - Modification, 124, 128–130, 136
      - setgid, 126–127
      - setuid, 126
      - Sticky bit, 127
      - Valeur umask, 127–128
    - BART, manifeste, 118–119
    - Calcul d'une synthèse, 247–248
    - Calcul de synthèses, 247–248, 248
    - Chiffrement, 250–253
    - Copie avec Secure Shell, 329–330



**Fichier (*Suite*)**

- Déchiffrement, 252
- Fichier, spécial, 125–127
- kdc.conf, 538
- Manifeste (BART), 118–119
- Modification de propriété, 124, 134–135
- Modification de propriété de groupe, 135
- Modification des autorisations de fichier spéciales, 138–139
- Montage avec authentification DH, 296
- Partage avec authentification DH, 295–296
- PKCS #12, 276
- Privilège lié à, 160
- Propriété
  - setgid, autorisation, 126–127
  - setuid, autorisation, 126
- Protection avec les autorisations UNIX, 132–133
- Sécurité
  - ACL, 51
  - Affichage des informations de fichier, 124, 133–134
  - Autorisation de fichier, 125
  - Autorisation de fichier spéciale, 130
  - Autorisation du répertoire, 125
  - Autorisation UNIX, 123–130
  - Chiffrement, 51
  - Classe d'utilisateur, 124
  - Modification de propriété, 134–135
  - Modification des autorisations, 128–130, 136
  - Restriction d'accès, 48
  - Type de fichier, 124
    - umask par défaut, 127–128
  - Symbole de type de fichier, 124
  - Synthèse, 247–248
  - Type de fichier, 124
  - Vérification de l'intégrité avec digest, 247–248
- Fichier, autorisation
  - Autorisation de fichier
    - Mode symbolique, 136
- fichier, jeton d'audit, Format, 658
- Fichier, système
  - Sécurité
    - Système de fichiers TMPFS, 127
  - TMPFS, 127

**Fichier d'audit**

- Combinaison, 617–619
- Gestion, 624–625
- Impression, 622
- Limitation de la taille, 637–638
- Réduction, 617–619
- Réduction de l'espace requis, 577–578
- Fichier d'identité (Secure Shell), Convention de nommage, 342
- Fichier de configuration
  - device\_maps, fichier, 98
  - Informations sur les privilèges, 226–227
  - Algorithme de mot de passe, 40
  - policy.conf, fichier, 40, 66–67, 223
  - Secure Shell, 334
  - syslog.conf, fichier, 64–66, 226
- Fichier de configuration PAM, Ajout de la pile su, 176
- Fichier de règles (BART), 105–106
- Fichier journal
  - BART
    - Sortie détaillée, 121–122
    - Sortie programmatique, 121–122
  - Contrôle de la commande su, 69–70
  - Enregistrement d'audit, 622
  - Tentative de connexion ayant échoué, 64–66
- Fichier keystab
  - Ajout de l'hôte principal au KDC maître, 384, 390
- Fichier ticket, *Voir* Cache d'informations d'identification
- Fichiers
  - audit\_class, 645
  - audit\_event, 645
  - Calcul du code MAC de, 248–250
  - Chiffrement, 240
  - Hachage, 240
  - Informations sur les privilèges, 226–227
  - Kerberos, 531–533
  - Objets publics, 554
  - Recherche de fichiers avec autorisations
    - setuid, 139
  - Sécurité
    - Chiffrement, 240
  - syslog.conf, 646



**Fichiers d'audit**

- Compression sur disque, 638–639
- Copie de messages dans un fichier unique, 621
- Création de fichiers de résumé, 620, 621
- Création des fichiers de résumé, 620
- Effets de temps universel (UTC), 617
- Horodatages, 652
- Lecture avec praudit, 621–623
- Réduction de l'espace de stockage requis, 578
- Réserver de l'espace disque, 598–601
- Systèmes de fichiers ZFS, 598–601, 638–639

**Fichiers de configuration, Audit, 645–646****Fichiers exécutables 32 bits, Protection contre les problèmes de sécurité, 131–132****Fichiers journaux**

- Configuration pour le service d'audit, 605–606
- Enregistrements d'audit, 558
- syslog, enregistrements d'audit, 646
- /var/adm/messages, 629
- /var/log/syslog, 629

**FILE, privilège, 160****File d'attente d'audit, Événements inclus, 556****find, commande, Recherche de fichiers avec autorisations setuid, 139****flags, ligne, Masque de présélection du processus, 652****Flèche d'ajout (>>), Interdiction d'ajout, 48****Flèche de redirection (>), Interdiction de redirection, 48****fmri, jeton d'audit, Format, 658****Format d'enregistrements d'audit, auditrecord, commande, 616****Format de fichier de règles (BART), 119–120****Format lisible, Conversion des enregistrements d'audit, 622****Format XML, Enregistrement d'audit, 622****ForwardAgent, mot-clé, Authentification transmise Secure Shell, 338****ForwardX11, mot-clé, Transmission de port Secure Shell, 338****ForwardX11Trusted, mot-clé, Transfert de port Secure Shell, 338****Fournisseur**

- Ajout d'un fournisseur de logiciels au niveau de l'utilisateur, 259–260

**Fournisseur (Suite)**

- Ajout d'une bibliothèque, 259–260
- Définition en tant que plug-in, 233
- Désactivation de mécanismes matériels, 265–267
- Enregistrement, 237
- Interdiction de l'utilisation d'un fournisseur de logiciels noyau, 262–264
- Liste dans la structure cryptographique, 255–258
- Restauration de l'utilisation d'un fournisseur de logiciels noyau, 262

**Fournisseur de matériel**

- Activation de mécanismes et de fonctions, 266
- Chargement, 264
- Désactivation de mécanismes cryptographiques, 265–267

**Fournisseurs**

- Ajout de fournisseur de logiciels, 258–260
- Connexion à la structure cryptographique, 237
- Définition dans la structure cryptographique, 234
- Définition en tant que plug-ins, 233
- Liste des fournisseurs de matériel, 264–265
- Signature, 237

**Fournisseurs de matériel, Liste, 264–265****Fournisseurs de noyau, Liste, 255****fp, modificateur d'événement d'audit, 658****ftp, commande**

- Définition du niveau de protection, 527
- Journalisation du transfert de fichiers, 640–641
- Kerberos, 524–527, 533

**ftpd, démon, Kerberos, 534****Fusion, Enregistrement d'audit binaire, 617–619****G****GatewayPorts, mot-clé, Secure Shell, 338****gencert, sous-commande, pktool commande, 273–274****Génération**

- Certificat avec la commande pktool, 273–274
- Certificat X.509 v3, 282–283
- Clé pour Secure Shell, 323–325
- Clé secrète NFS, 289
- Clé Secure Shell, 323–325

Génération (*Suite*)

## Clé symétrique

Utilisation de la commande `dd`, 240–242Utilisation de la commande `pktool`, 243–247

## Nombre aléatoire

Utilisation de la commande `dd`, 240–242Utilisation de la commande `pktool`, 243–247

## Paire de clés

Utilisation de la commande `pktool`, 278–282Phrase de passe avec la commande `pktool`, 277–278

## Gestion

*Voir aussi* Gestion

Allocation de périphériques, 85–86

Audit, 581

Efficacité, 578

Audit de zones, 647

Audit par zone, 564–565

Autorisation de fichier, 132–141

Dépassement de la piste d'audit, 624–625

Fichier d'audit, 617–619, 624–625

Keystore avec KMF, 271

Liste des tâches de l'allocation de  
périphériques, 85–86

Liste des tâches de privilèges, 209

Liste des tâches des enregistrements d'audit, 615

Liste des tâches RBAC, 192–193

Mot de passe avec Kerberos, 519–524

Périphériques, 85–86

Sans privilège, 161

Gestion de la cryptographie (RBAC), Création d'un  
rôle, 184Gestion des droits de processus, *Voir* PrivilègesGestion des droits des utilisateurs, *Voir* PrivilègeGestion des périphériques, *Voir* Stratégie de  
périphériques`getdevpolicy`, commande, Description, 95`getent`, commande, Description, 223`-getflags`, option`auditconfig`, commande, 583–585, 585–586`-getnaflags`, option`auditconfig`, commande, 583–585, 585–586`-getplugin`, option`auditconfig`, commande, 583–585, 604–605,  
605–606`-getpolicy`, option`auditconfig`, commande, 583–585, 590–592`-getqctrl`, option, `auditconfig`,

commande, 583–585

`gkadmin`, commande*Voir aussi* Outil SEAM

Description, 533

`.gkadmin`, fichier

Description, 531

Outil SEAM, 477

`GlobalKnownHostsFile`, mot-clé*Voir* `GlobalKnownHostsFile`, mot-cléFichier `ssh_config`, 338`group`, jeton d'audit

Format, 658

Stratégie de groupe, 658

`group`, stratégie d'audit

Description, 575

`group`, jeton, 658`groups`, jeton, 575

Groupe, Modification de propriété de fichier, 135

Groupes, Exceptions aux valeurs par défaut Secure  
Shell, 321–322

## GSS-API

Authentification dans Secure Shell, 314

Informations d'identification dans Secure Shell, 334

Kerberos, 350

`gssapi.so.1`, plug-in, SASL, 310`GSSAPIAuthentication`, mot-clé, Secure Shell, 338`GSSAPIDelegateCredentials`, mot-clé, Fichier  
`ssh_config`, 338`GSSAPIKeyExchange`, mot-clé, Secure Shell, 338`GSSAPIStoreDelegatedCredentials`, mot-clé, Fichier  
`sshd_config`, 338`gsscred`, commande, Description, 533`gsscred`, table, Utilisation, 546`gssd`, démon, Kerberos, 534

## H

`-h`, option, `auditrecord`, commande, 616

## Hachage

Algorithmes

Kerberos, 372

## Hachage (*Suite*)

- Fichiers, 240
- HashKnownHosts, mot-clé, ssh\_config, fichier, 338
- header, jeton d'audit
  - Format, 658–659
  - Modificateurs d'événement, 658
  - Ordre dans l'enregistrement d'audit, 658–659
- Hiérarchie de domaine, Kerberos, 365
- hmac-md5, algorithme, Fichier ssh\_config, 339
- hmac-sha1, algorithme de chiffrement, Fichier ssh\_config, 339
- Horodatages, Fichiers d'audit, 652
- Host, mot-clé
  - Fichier ssh\_config, 338, 341
- host principal
  - Création, 383, 390
- HostbasedAuthentication, mot-clé, Secure Shell, 338
- HostbasedUsesNameFromPacketOnly, mot-clé, Fichier sshd\_config, 338
- HostKey, mot-clé, Fichier sshd\_config, 338
- HostKeyAlgorithms, mot-clé, Fichier ssh\_config, 338
- HostKeyAlias, mot-clé, Fichier ssh\_config, 338
- HostName, mot-clé, Fichier ssh\_config, 338
- hosts.equiv, fichier, Description, 343
- Hôte
  - Hôte de confiance, 56
  - Hôte Secure Shell, 314
- Hôte de confiance, 56
- Hôtes
  - Désactivation du service Kerberos, 512–514
  - Exceptions aux valeurs par défaut Secure Shell, 321–322

## I

- I, option
  - bart create, commande, 108
  - st\_clean, script, 102
- i, option
  - bart create, commande, 108, 111
  - encrypt, commande, 251
  - st\_clean, script, 102

## ID

- Audit
  - Mécanisme, 652
  - Présentation, 551–552
  - De session d'audit, 652
  - Mappage UNIX sur les principaux Kerberos, 546
- ID de session, Audit, 652
- ID de session d'audit, 652
  - Présentation, 551–552
- ID du terminal, Audit, 652
- ID utilisateur
  - ID d'audit, 551–552, 652
  - Services NFS, 405–406
- ID utilisateur (UID), Comptes spéciaux, 42
- ID utilisateur d'audit
  - Mécanisme, 652
  - Présentation, 551–552
- IgnoreIfUnknown, mot-clé, ssh\_config, fichier, 338
- IgnoreRhosts, mot-clé, Fichier sshd\_config, 338
- IgnoreUserKnownHosts, mot-clé, Fichier sshd\_config, 338
- import, sous-commande, pktool,
  - commande, 274–275
- Impression, Journal d'audit, 622
- in.ftpd, démon, Kerberos, 534
- in.rlogind, démon, Kerberos, 534
- in.rshd, démon, Kerberos, 534
- in.telnetd, démon, Kerberos, 534
- Indicateur de contrôle binding, PAM, 304
- Indicateur de contrôle include, PAM, 304
- Indicateur de contrôle optional, PAM, 304
- Indicateur de contrôle required, PAM, 305
- Indicateur de contrôle requisite, PAM, 305
- Indicateur de contrôle suffisant, PAM, 305
- Indicateurs d'audit, Résumé, 552
- Informations d'identification
  - Cache, 540
  - Description, 290, 536
  - Mappage, 368
  - Obtention pour un serveur, 542–543
  - Obtention pour un TGS, 541–542
  - Tickets, 351
- install, sous-commande, cryptoadm,
  - commande, 260

- Installation, Secure by Default, 49
- Instance, Nom de principal, 355
- Intégrité
  - Kerberos et, 349
  - Service de sécurité, 357
- Interdiction
  - Utilisation d'un fournisseur de logiciels noyau, 262–264
  - Utilisation de mécanisme matériel, 265–267
- `ioctl()`, appel système, `AUDIO_SETINFO()`, 102
- `ip address`, jeton d'audit, Format, 659
- IP MIB-II, Récupération d'informations de `/dev/arp`, 84–85
- `ip port`, jeton d'audit, Format, 659
- `ipc`, jeton d'audit, 659–660
  - Format, 659–660
- IPC, privilège, 160
- `IPC_perm`, jeton d'audit, Format, 660
- IPC System V
  - `ipc`, jeton d'audit, 659–660
  - `IPC_perm`, jeton d'audit, 660
- IPC system V, Privilège, 160

## J

- Jeton, Définition dans la structure cryptographique, 235
- Jeton d'audit
  - Ajouté par stratégie d'audit, 649
  - Description, 553, 557
  - Format, 654
  - Format d'enregistrement d'audit, 653
  - Liste, 654
- Jeton d'audit du fichier `vnode`, 656
- Jeton Internet, `socket`, jeton, 662
- Jetons d'audit
  - Voir aussi* Noms de jeton d'audit individuels
  - `xcclient`, jeton, 664
- Jetons Internet
  - `ip address`, jeton, 659
  - `ip port`, jeton, 659
- Jeu de privilèges
  - Ajout de privilèges, 165
  - De base, 163

- Jeu de privilèges (*Suite*)
  - Effectif, 162
  - Héritable, 163
  - Limite, 163
  - Liste, 163
  - Permis, 162
  - Suppression de privilèges, 166
- Jeu de privilèges autorisés, 162
- Jeu de privilèges de base, 163
- Jeu de privilèges de limite, 163
- Jeu de privilèges effectif, 162
- Jeu de privilèges héritable, 163
- Journalisation
  - `AUTH__DH`, 289
  - Connexion `root`
    - Restriction sur la console, 70–71
  - Journal des connexions ayant échoué, 64–66
  - Transfert de fichiers `ftp`, 640–641
- Journaux d'audit
  - Voir aussi* Fichiers d'audit
  - Comparaison des résumés binaires et textuels, 558
  - Configuration, 597–606
  - Configuration des journaux d'audit de résumé textuel, 605–606
  - Modes, 558

## K

- k, option
  - Commandes utilisant Kerberos, 526
  - `encrypt`, commande, 251
  - `mac`, commande, 249
- K option
  - `encrypt`, commande, 251
  - `mac`, commande, 249
- K, option
  - Commandes utilisant Kerberos, 526
  - `rolemod`, commande, 195
  - `usermod`, commande, 197
- `.k5.REALM`, fichier, Description, 532
- `.k5login`, fichier
  - Au lieu de révéler le mot de passe, 523
  - Description, 522–524, 531

- kadm5.acf, fichier
  - Description, 531
  - Entrée de KDC maître, 382, 388, 431
  - Format des entrées, 493
  - Nouveaux principaux, 487, 489
- kadm5.keytab, fichier, Description, 532
- kadmin, commande
  - Création de l'host principal, 383, 390
  - Description, 533
  - ktadd, commande, 509–510
  - ktremove, commande, 511
  - Outil SEAM, 476
  - Suppression de principaux d'un fichier keytab, 511
- kadmin.local, commande
  - Ajout de principal d'administration, 382, 389
  - Automatisation de création de principal, 481
  - Description, 533
- kadmin.log, fichier, Description, 532
- kadmind, démon
  - KDC maître, 535
  - Kerberos, 534
- kbd, fichier, 72–73
- KbdInteractiveAuthentication, mot-clé, Secure Shell, 338
- kcfcd, démon, 235, 267–268
- kclient, commande, Description, 533
- kdb5\_ldap\_util, commande, Description, 533
- kdb5\_util, commande
  - Création de base de données KDC, 382
  - Création du fichier stash, 396, 443
  - Description, 533
- KDC
  - Configuration d'esclave
    - Manuelle, 393–396
  - Configuration d'un KDC esclave
    - Automatique, 391–392
    - Interactive, 392–393
  - Configuration d'un KDC maître
    - Automatique, 378–379
    - Interactive, 379–380
    - Manuelle, 380–384
  - Configuration du maître
    - Avec LDAP, 384–391
- KDC (*Suite*)
  - Copie de fichiers d'administration de l'esclave au maître, 394, 441
  - Création de base de données, 382
  - Création de l'host principal, 383, 390
  - Démarrage du démon, 396, 443
  - Echange entre maître et esclave, 428–433
  - Esclave, 367
    - Définition, 534
  - Esclave ou maître, 356, 377
  - Maître
    - Définition, 534
  - Planification, 367
  - Ports, 367
  - Propagation de base de données, 369
  - Restriction de l'accès aux serveurs, 453
  - Sauvegarde et propagation, 433–434
  - Synchronisation d'horloge
    - KDC esclave, 396, 443
    - KDC maître, 384, 391
- kdc.conf, fichier
  - Description, 532
  - Durée de vie de ticket, 538
- KDC esclaves
  - Configuration, 393–396
  - Configuration automatique, 391–392
  - Configuration interactive, 392–393
  - Définition, 534
  - KDC maître, 356
  - Maître, 377
  - Planification, 367
- kdc.log, fichier, Description, 532
- KDC maître
  - Configuration automatique, 378–379
  - Configuration avec LDAP, 384–391
  - Configuration interactive, 379–380
  - Configuration manuelle, 380–384
  - Définition, 534
  - Echange avec un KDC esclave, 428–433
  - KDC esclaves, 356, 377
- kdcmgr, commande
  - Configuration d'un KDC esclave
    - Automatique, 391
    - Interactive, 392

**kdcmgr, commande (*Suite*)**

## Configuration d'un KDC maître

Automatique, 378

Interactive, 379

Etat du serveur, 380

**kdestroy, commande, Kerberos, 533****kdestroy commande, Exemple, 518****KeepAlive, mot-clé, Secure Shell, 338****Kerberos**

## Activation d'applications utilisant Kerberos

uniquement, 452

Administration, 475–514

Aide en ligne, 373

Application distante, 354

Commande, 524–530, 533–534

Composant, 358–359

Configuration des serveurs KDC, 377–397

Décisions de configuration, 363–373

Démon, 534

Dépannage, 470

Domaines

*Voir* Domaines (Kerberos)

## Exemple d'utilisation de commande utilisant

Kerberos, 529–530

Fichiers, 531–533

Gestion des mots de passe, 519–524

Message d'erreur, 455–470

Obtention d'accès au serveur, 541–544

Octroi de l'accès à votre compte, 522–524

Option de commande utilisant Kerberos, 525

Outil d'administration

*Voir* Outil SEAM

Planification, 363–373

Présentation

Commandes utilisant Kerberos, 524–527

Système d'authentification, 350–356, 540

Protocole Kerberos V5, 349

Référence, 531–547

Tableau des options de commandes réseau, 526

Terminologie, 534–540

Types de chiffrement

Présentation, 372

Utilisation, 544–546

Utilisation, 515–530

**Kerberos, commande, 524–530**

Exemple, 529–530

**kern.notice, entrée, syslog.conf, fichier, 132****Key Distribution Center (centre de distribution des clés), *Voir* KDC****KEYBOARD\_ABORT, variable système, 72–73****keylogin, commande, Utilisation pour le RPC sécurisé, 289****KeyRegenerationInterval, mot-clé, Fichier****sshd\_config, 338****keyserv, démon, 293****Keystore**

Exportation de certificats, 276–277

Géré par KMF, 270

Importation de certificats, 274–275

Liste du contenu, 273

Prise en charge par KMF, 270, 271

Protection avec mot de passe dans KMF, 277–278

**Keytab, fichier**

Administration, 508–514

Administration avec la commande **ktutil**, 509

Affichage du contenu avec la commande

**ktutil**, 511, 512Affichage du tampon de la liste de clés à l'aide de la commande **list**, 512, 513

Ajout d'un principal de service, 509–510

**keytab, fichier, Ajout d'un principal de service, 508****Keytab, fichier**

Désactivation du service d'un hôte avec la

commande **delete\_entry**, 513

Lecture dans le tampon de keytab avec la commande

**read\_kt**, 512, 513

Suppression d'un principal de service, 511

Suppression de principaux avec la commande

**ktremove**, 511**keytab, option, SASL, 311****kgcmgr, commande, Description, 534****kinit, commande**

Durée de vie de ticket, 538

**-F Option, 516**

Kerberos, 533

**kinit commande, Exemple, 516****klist, commande**

Exemple, 517–518





`list` plugin, sous-commande, `kmcfg`,  
commande, 283–284

## Liste

- Contenu du keystore, 273
- Fournisseurs dans la structure  
cryptographique, 255–258
- Fournisseurs de matériel, 264–265
- Fournisseurs de structure  
cryptographique, 264–265
- Fournisseurs disponibles dans la structure  
cryptographique, 255–258
- Rôle disponible, 223
- Rôle endossable, 174
- Stratégie de périphériques, 82–83
- Tous les attributs de sécurité RBAC, 170–171
- Utilisateurs sans mot de passe, 62
- Vos droits RBAC, 171–174

## Liste des tâches

- Accès système, 59–60
- Administration de la structure  
cryptographique, 254–255
- Administration du RPC sécurisé, 292–293
- Allocation de périphériques, 85–86
- Audit, 581
- Configuration de l'audit, 582–583
- Configuration de la stratégie de périphériques, 82
- Configuration de RBAC, 177–178
- Configuration de Secure Shell, 318
- Configuration de serveurs Kerberos NFS, 403
- Configuration des journaux d'audit, 597–598
- Configuration des périphériques, 81
- Configuration Kerberos, 375–376
- Dépannage de l'audit, 626–627
- Gestion de l'allocation des périphériques, 85–86
- Gestion de la stratégie de périphériques, 82
- Gestion des enregistrements d'audit, 615
- Gestion RBAC, 192–193
- PAM, 299
- Périphérique, 81
- Principaux d'administration (Kerberos), 480–481
- Protection contre les programmes présentant des  
risques de sécurité, 139
- Protection de fichiers à l'aide d'autorisations  
UNIX, 132

## Liste des tâches (*Suite*)

- Protection de fichiers avec des mécanismes  
cryptographiques, 240
- Secure Shell, 317
- Sécurisation des connexions et des mots de  
passe, 60–61
- Sécurisation des systèmes, 59–60
- Stratégie de périphériques, 82
- Structure cryptographique, 239
- Utilisation de la configuration RBAC par  
défaut, 170
- Utilisation de la liste des tâches BART, 107–108
- Utilisation de la structure cryptographique, 239
- Utilisation de la structure de gestion des clés (liste  
des tâches), 272–273
- Utilisation de RBAC, 169–170
- Utilisation de Secure Shell, 322–323

## Liste des tâches de l'audit, 581

`ListenAddress`, mot-clé, Fichier `sshd_config`, 339

## Listes de contrôle d'accès (ACL), Voir ACL

## Listes des tâches

- Administration de stratégies (Kerberos), 494–495
- Gestion et utilisation des privilèges, 204
- Maintenance Kerberos, 376
- Planification de l'audit, 567–573

`log_level`, option, SASL, 311

`logadm`, commande, Archivage de fichiers d'audit de  
résumé, 625

## Logiciel antivirus, Voir Analyse des virus

`login`, fichier

- Paramètre de connexion par défaut, 64
- Restriction de l'accès root à distance, 70–71

`login`, variable d'environnement, Secure  
Shell, 341–342

`LoginGraceTime`, mot-clé, Fichier `sshd_config`, 339

`loginlog`, fichier, Enregistrement des tentatives de  
connexion ayant échoué, 63–64

## logins, commande

- Affichage de l'état de connexion d'un  
utilisateur, 61–62
- Affichage des utilisateurs sans mot de passe, 62
- Syntaxe, 61

`LogLevel`, mot-clé, Secure Shell, 339



LookupClientHostnames, mot-clé, Fichier  
 sshd\_config, 339  
 -lspolicy, option, auditconfig,  
 commande, 590–592

## M

-M, option, auditreduce, commande, 619  
 -m, option  
   Commandes utilisant Kerberos, 526  
   cryptoadm, commande, 260, 262

mac, commande  
   Description, 236  
   Syntaxe, 248

MACS, mot-clé, Secure Shell, 339

Manifestes

*Voir aussi* bart create  
   Contrôle, 103  
   Format de fichier, 118–119  
   Personnalisation, 110–111  
   Test, 105

Manifestes de contrôle (BART), 103

Manifestes de test, 105

Mappage

  Événement et classe (audit), 556  
   Noms d'hôtes sur domaines (Kerberos), 365  
   UID sur principaux Kerberos, 546

Mappage d'informations d'identification GSS, 368

Mappages événements-classes d'audit,  
   Modification, 596–597

Masque (audit), Description de la présélection de  
   processus, 651

Masque de présélection (audit), Description, 651

Masque de présélection d'audit

  Modification pour chaque utilisateur, 586–590  
   Modification pour les utilisateurs  
   existants, 635–636

Masque de présélection de processus, Description, 651

Match, blocs, Exceptions aux valeurs par défaut Secure  
 Shell, 321–322

Match, mot-clé, sshd\_config, fichier, 339

Matériel

  Liste d'accélérateurs de matériels  
   connectés, 264–265

Matériel (*Suite*)

  Mot de passe obligatoire pour l'accès, 71–72

  Protection, 38, 71–73

Matériel système, Contrôle de l'accès, 71–73

max\_life, valeur, Description, 538

max\_renewable\_life, valeur, Description, 539

MaxStartups, mot-clé, Fichier sshd\_config, 339

MD4, algorithme de chiffrement, Fournisseur de  
   noyau, 255

MD5, algorithme de chiffrement

  Autorisation dans un environnement  
   hétérogène, 67

MD5, algorithme de chiffrement, Fournisseur de  
   noyau, 255

MD5, algorithme de chiffrement

  policy.conf, fichier, 66–67, 67

Mécanisme

  Activation sélective sur le fournisseur de  
   matériel, 266

  Définition dans la structure cryptographique, 234

  Désactivation de tous les fournisseurs de  
   matériel, 265–267

Mécanisme de sécurité, Spécification avec l'option  
   -m, 526

mech\_dh, mécanisme, Informations d'identification de  
   GSS-API, 334

mech\_krb, mécanisme, Informations d'identification de  
   GSS-API, 335

mech\_list, option, SASL, 311

Message d'erreur

  Avec kpasswd, 520

  Kerberos, 455–470

messages, fichier, Message de pile exécutable, 132

Messages d'erreur, encrypt, commande, 253

Metaslot, Administration, 235–236

metaslot, Définition dans la structure  
   cryptographique, 234

Méthode d'authentification

  Basée sur l'hôte dans Secure Shell, 318–320

  Basée sur l'hôte Secure Shell, 315

  Clés publiques dans Secure Shell, 315

  Informations d'identification GSS-API dans Secure  
   Shell, 314

  Secure Shell, 314–315

- Méthodes d'authentification, Mot de passe Secure Shell, 315
- Microphone
  - Allocation, 91
  - Libération, 94
- Mode, Définition dans la structure cryptographique, 234
- Mode absolu, Description, 128
- Mode de sécurité, Configuration d'environnement avec des modes de sécurité multiples, 408–409
- Mode symbolique, Modification des autorisations de fichier, 129
- Modificateurs d'événement, Enregistrements d'audit, 658
- Modification
  - Algorithme de mot de passe pour un domaine, 67–68
  - Algorithme de mots de passe par défaut, 66–69
  - Attributs de sécurité utilisateur, 586–590
  - audit\_class, fichier, 595–596
  - audit\_event, fichier, 596–597
  - Autorisation de fichier
    - Mode absolu, 137–138
    - Mode symbolique, 136
    - Spécial, 138–139
  - Autorisation de fichier spéciale, 138–139
  - Clé secrète NFS, 289
  - Contenu du profil de droits, 186–187
  - Liste des tâches d'algorithme de mots de passe, 66–69
  - Mot de passe d'un rôle, 193–194
  - Mot de passe de principal (Kerberos), 490–491
  - Mot de passe root, 61
  - Paramètres par défaut de l'audit, 585–586
  - Périphérique allouable, 89–90
  - Phrase de passe pour Secure Shell, 325
  - Principaux (Kerberos), 490–491
  - Propriété de fichier, 134–135
  - Propriété de groupe de fichier, 135
  - Propriétés de rôle, 194–195
  - Rôle root en utilisateur, 202–204
  - Rôles (RBAC), 194–195
  - Stratégie de périphériques, 83–84
  - Stratégies (Kerberos), 501–502

- Modification (*Suite*)
  - Utilisateurs (RBAC), 196–197
  - Votre mot de passe avec kpasswd, 520
  - Votre mot de passe avec passwd, 520
- Module d'authentification enfichable, *Voir* PAM
- Modules, Chiffrement de mot de passe, 40
- Modules PAM, 176
- Moindre privilège, Principe, 160
- Montage
  - CD-ROM alloué, 93
  - Fichier avec authentification DH, 296
  - Périphérique alloué, 92–93
- Mot-clé
  - Voir aussi* Mot-clé spécifique
  - Attribut dans BART, 120
  - Options de ligne de commande de substitution dans Secure Shell, 345
  - Secure Shell, 336–342
- Mot-clé LocalForward, Fichier ssh\_config, 339
- Mot de passe
  - Accès au matériel, 71–72
  - Affichage des utilisateurs sans mot de passe, 62
  - Authentification dans Secure Shell, 314
  - Chiffrement des mots de passe, 66–69
  - Connexion au système, 39
  - Déchiffrement de clé secrète pour le RPC sécurisé, 289
  - Elimination dans Secure Shell, 327–328
  - Gestion, 519–524
  - LDAP, 40
    - Spécification d'un nouvel algorithme de mot de passe, 68–69
  - Liste des tâches, 60–61
  - Local, 39
  - Mode de sécurité de la PROM, 38, 71–73
  - Modification avec la commande kpasswd, 520
  - Modification avec la commande passwd, 520
  - NIS, 39
    - Spécification d'un nouvel algorithme de mot de passe, 67–68
  - Obligatoire pour l'accès au matériel, 71–72
  - Octroi de l'accès sans révélation, 522–524
  - Protection
    - Fichier PKCS #12, 276

## Mot de passe, Protection (*Suite*)

Keystore, 276

Recherche des utilisateurs sans mot de passe, 62

Sécurité de connexion, 38, 39

Spécification d'un algorithme

Service de noms, 67–68

Spécification de l'algorithme, 66–67

Suggestions de choix, 519–520

UNIX et Kerberos, 519–524

Utilisation de l'algorithme de chiffrement

MD5, 66–67

## Mots de passe

Algorithmes de chiffrement, 40

Contrainte des algorithmes de chiffrement dans un environnement hétérogène, 67

Modification à l'aide de la commande `passwd -r`, 39

Modification du mot de passe, 193–194

Modification du mot de passe d'un

principal, 490–491

Spécification de l'algorithme

Localement, 66–69

Stratégies, 520

Utilisation de Blowfish dans un environnement hétérogène, 67

Utilisation du mot de passe utilisateur pour endosser un rôle, 201–202

Utilisation du nouvel algorithme, 67

`mount`, commande, Attribut de sécurité, 87

`mt`, commande, Nettoyage de périphériques à bande, 101

## N

`-n`, option, `bart create`, commande, 108

`na`, modificateur d'événement d'audit, 659

NET, privilège, 160

`netservices limited`, option d'installation, 49

Nettoyage, Fichier d'audit, 623–624

Nettoyage forcé, `st_clean`, script, 102

Nettoyage standard, `st_clean`, script, 102

`never-audit`, classes, Masque de présélection de processus, 651

`newkey`, commande

Création de clés pour utilisateurs NIS, 294–295

`newkey`, commande (*Suite*)

Génération de clés, 289

NFS sécurisé, 288

`nisaddcred`, commande, Génération de clés, 289

Niveau de protection

`clear`, 527

Définition dans `ftp`, 527

`private`, 527

`safe`, 527

`nobody`, utilisateur, 52

`noexec_user_stack`, variable, 131, 141

`noexec_user_stack_log`, variable, 132, 141

`NoHostAuthenticationForLocalHost`, mot-clé, Fichier `ssh_config`, 339

`nologin`, fichier, Description, 343

Nom

Nom de périphérique

`device_maps`, fichier, 99, 100

Nom de domaine complet (FQDN, fully qualified domain name), Kerberos, 366

Nombre aléatoire

`dd`, commande, 240–242

`pktool`, commande, 243–247

Noms d'hôtes, Mappage sur domaines, 365

Noms de clients, Planification pour Kerberos, 366

Nouvelle fonctionnalité

Amélioration de l'audit, 565–566

Amélioration de Secure Shell, 316–317

SASL, 309

Nouvelles fonctionnalités, Secure Shell et

FIPS-140, 317

`nscd` (name service cache daemon, démon cache de service de noms), Utilisation, 223

NSS, Gestion de keystore, 271

NTP

KDC esclave, 396, 443

KDC maître, 384, 391

Planification Kerberos, 369

NTP (Network Time Protocol), Voir NTP

`NumberOfPasswordPrompts`, mot-clé, Fichier `ssh_config`, 339

**O**

- O, option
  - auditreduce, commande, 617–619, 620
- o, option, encrypt, commande, 251
- Objets publics, Audit, 554
- Obtaining, Ticket transmissible, 516
- Obtention
  - Accès à un service spécifique, 543–544
  - Commandes privilégiées, 194–195
  - Informations d'identification pour un serveur, 542–543
  - Informations d'identification pour un TGS, 541–542
  - Privilège, 164
  - Privilèges, 164, 195, 197
  - Privilèges sur un processus, 209–211
  - Tickets avec kinit, 516
- Octroi de l'accès à votre compte, 522–524
- OpenSSH, *Voir* Secure Shell
- OpenSSL
  - Gestion de keystore, 271
  - Version, 270
- Opérateur (RBAC), Rôle recommandé, 147
- Operator (opérateur), RBAC, Profil de droits, 216
- Option d'installation Secure by Default, 49
- Options de commande utilisant Kerberos, 525
- Ordre de recherche
  - Attributs de sécurité, 217
  - Attributs de sécurité utilisateur, 218
- Outil de génération de rapports, *Voir* bart compare
- Outil de génération de rapports d'audit de base, *Voir* BART
- Outil SEAM
  - Affichage d'une sous-liste de principaux, 483
  - Affichage de la liste de principaux, 482–484
  - Affichage de la liste de stratégies, 495–497
  - Affichage des attributs d'un principal, 484–486
  - Affichage des attributs d'une stratégie, 497–499
  - Aide, 478
  - Aide contextuelle, 478
  - Aide en ligne, 478
  - Création d'un nouveau principal, 486–488
  - Création d'une stratégie, 486, 499–500
  - Démarrage, 479–480

**Outil SEAM (Suite)**

- Duplication d'un principal, 489
- Equivalents de ligne de commande, 477
- et privilèges d'administration limités, 506–508
- Et X Window System, 477
- Fenêtre de connexion, 479
- Fichiers modifiés, 477
- Filtre, zone de motif, 483
- gkadmin, commande, 475
- .gkadmin, fichier, 477
- Impact des privilèges, 507
- kadmin, commande, 475
- Modification d'un principal, 490–491
- Modification d'une stratégie, 501–502
- ou commande kadmin, 476
- Panneau, description, 503–506
- Paramétrage des valeurs de principal par défaut, 492–493
- Présentation, 476–480
- Privilèges, 507
- Privilèges de liste, 507
- Sommaire de l'aide, 478
- Suppression d'un principal, 491
- Suppression de stratégies, 502–503
- Table des panneaux, 503–506
- Valeur par défaut, 479

ovsec\_admin.xxxxx, fichier, Description, 532

**P**

- p, option
  - auditrecord, commande, 616
  - Commande logins, 62
  - cryptoadm, commande, 260, 262
- p option, bart create, 111
- Pages de manuel, Service d'audit, 645–646
- Paires de clés
  - Création, 278–282
  - Génération
    - Utilisation de la commande pktool, 278–282
- PAM
  - Ajout d'un module, 301
  - /etc/syslog.conf, fichier, 302

PAM (*Suite*)

- Fichier de configuration
  - Diagramme de superposition, 305
  - Exemple de superposition, 307
  - Explication de la superposition, 303
  - Indicateur de contrôle, 304
  - Kerberos, 532
  - Présentation, 302
  - Syntaxe, 303
- Kerberos, 359
- Liste des tâches, 299
- Pile pour la mise en cache de l'authentification, 176
- Planification, 300
- Présentation, 297
- Structure, 298
- pam.conf, fichier, *Voir* Fichier de configuration PAM
- pam\_roles, commande, Description, 223
- pam\_tty\_tickets.so.1, module, PAM, 176
- PAMServiceName, mot-clé, sshd\_config, fichier, 339
- PAMServicePrefix, mot-clé, sshd\_config, fichier, 339
- Panneau, Table de l'outil SEAM, 503–506
- Paramétrage, Valeurs de principal par défaut (Kerberos), 492–493
- Partage de fichiers
  - Authentification DH, 295–296
  - Sécurité du réseau, 51
- Passerelle, *Voir* Système pare-feu
- PASSREQ dans Secure Shell, 341
- passwd, commande
  - Commande kpasswd, 520
  - Modification du mot de passe d'un rôle, 193–194
  - Services de noms, 39
  - Syntaxe, 61
- PasswordAuthentication, mot-clé, Secure Shell, 339
- path, jeton d'audit, Format, 660
- path, stratégie d'audit, Description, 575
- PATH, variable d'environnement, Sécurité, 47
- path\_attr, jeton d'audit, 661
- PATH dans Secure Shell, 342
- Périphérique
  - Affichage d'informations sur l'allocation, 88
  - Ajout d'une stratégie de périphériques, 83–84
  - Allocation de périphériques
    - Voir* Allocation de périphériques

Périphérique (*Suite*)

- Allocation forcée, 88–89
- Audit de l'allocation, 90
- Audit des modifications de stratégie, 84
- Autorisation d'allocation des utilisateurs, 87
- Commande de la stratégie, 95
- Contrôle d'accès par connexion, 43
- Démontage de périphériques alloués, 94
- /dev/urandom, périphérique, 240–242
- Gestion, 82
- Gestion de l'allocation, 85–86
- Interdiction d'utilisation, 90
- Interdiction d'utilisation de tous les périphériques, 90
- Libération d'un périphérique, 93–94
- Libération forcée, 89
- Liste des noms de périphérique, 88
- Modèle de privilège, 166–167
- Modèle de superutilisateur, 166–167
- Modification de la stratégie de périphériques, 83–84
- Modification des périphériques allouables, 89–90
- Montage de périphériques alloués, 92–93
- Ne requérant pas d'autorisation pour l'utilisation, 89
- Protection assurée par l'allocation des périphériques, 44
- Protection dans le noyau, 43
- Récupération d'informations IP MIB-II, 84–85
- Sécurité, 43–46
- Suppression de stratégie, 84
- Zone, 44
- Périphérique audio, Sécurité, 102
- Périphérique SCSI, st\_clean, script, 101
- Périphériques
  - Affichage de la stratégie de périphériques, 82–83
  - Allocation pour utilisation, 85–90
  - Allouable, 86
  - Liste, 82–83
- PermitEmptyPasswords, mot-clé, Fichier sshd\_config, 339
- PermitRootLogin, mot-clé, Fichier sshd\_config, 339
- PermitUserEnvironment, mot-clé, Fichier sshd\_config, 339
- Personnalisation, Manifestes, 110–111

- Personnalisation d'un rapport (BART), 116–117
- perzone, stratégie d'audit
  - Définition, 592
  - Description, 575
  - Utilisation, 564–565, 569, 609–610, 647
- pfcs, commande, Description, 156–157
- pfexec, commande, Description, 223
- pfksh, commande, Description, 156–157
- pfsh, commande, Description, 156–157
- Phrase de passe
  - encrypt, commande, 251
  - Exemple, 326
  - Génération dans KMF, 277–278
  - mac, commande, 249
  - Modification pour Secure Shell, 325
  - Stockage en toute sécurité, 252
  - Utilisation dans Secure Shell, 327–328
  - Utilisation pour un MAC, 249
- PidFile, mot-clé, Secure Shell, 339
- Pile exécutable, Journalisation de message, 132
- Piles exécutable, Protection contre les processus
  - 32 bits, 131
- Piles exécutables, Protection, 141
- Pilote N2CP
  - Liste des mécanismes, 264–265
  - Plug-in matériel dans la structure cryptographique, 233
- Pilote NCP
  - Liste des mécanismes, 264–265
  - Plug-in matériel dans la structure cryptographique, 233
- Piste d'audit
  - Affichage d'événements à partir de différentes zones, 647
  - Ajout d'espace disque, 601–604
  - Aucun objet public, 554
  - Consultation des événements, 621–623
  - Contrôle du dépassement, 624–625
  - Coût de l'analyse, 577
  - Création
    - Fichiers de résumé, 620
  - Description, 554
  - Diminution de la taille, 638–639
  - Effet de la stratégie d'audit, 573
- Piste d'audit (*Suite*)
  - Envoi de fichiers à un référentiel distant, 604–605
  - Nettoyage de fichiers non terminés, 623–624
  - Présentation, 563
  - Réduction de la taille, 629–631
  - Sélection des événements, 619–621
  - Surveillance en temps réel, 578
- PKCS #12, fichier, Protection, 276
- pkcs11\_kernel.so, fournisseur au niveau de l'utilisateur, 255
- pkcs11\_softtoken.so, fournisseur au niveau de l'utilisateur, 255
- PKI
  - Géré par KMF, 269
  - Stratégie gérée par KMF, 271
- pktool, commande
  - Création d'un certificat autosigné, 273–274
  - export, sous-commande, 276–277
  - gencert, sous-commande, 273–274
  - Génération de clés secrètes, 243–247
  - Génération de paires de clés, 278–282
  - Gestion des objets PKI, 270
  - import, sous-commande, 274–275
  - list, sous-commande, 273
  - setpin, sous-commande, 277–278
  - Signature d'une CSR PKCS #10, 282–283
- plain.so.1, plug-in, SASL, 310
- Planification
  - Audit, 567–573
  - Audit par zone, 568–569
  - Kerberos
    - Décisions de configuration, 363–373
    - Domaines, 364–365
    - Hierarchie de domaine, 365
    - KDC esclaves, 367
    - Nombre de domaines, 364–365
    - Noms de clients et de principal de service, 366
    - Noms de domaines, 364
    - Ports, 367
    - Propagation de base de données, 369
    - Synchronisation d'horloge, 369
  - Liste des tâches de l'audit, 567–573
  - PAM, 300
  - RBAC, 178–180

- Plug-in, SASL, 310
- Plug-in audit\_binfile, Limitation de la taille du fichier d'audit, 602
- Plug-in audit\_syslog, Définition des attributs, 605–606
- Plug-in d'audit, Résumé, 649
- Plug-in de mécanisme de sécurité EXTERNE, SASL, 310
- Plug-in INTERNE, SASL, 310
- Plug-ins
  - Ajout à la KMF, 283–284
  - Audit, 557–558
  - Gérés dans KMF, 271
  - Structure cryptographique, 233
  - Suppression de la KMF, 283–284
- Plug-ins d'audit
  - audit\_binfile, plug-in, 592–594
  - audit\_binfile, plugin, 601–604
  - audit\_remote, plug-in, 604–605
  - audit\_syslog, plug-in, 605–606
  - Description, 553
  - qsize, attribut, 592–594
  - Récapitulatif, 645–646
- plugin\_list, option, SASL, 311
- Point (.)
  - Affichage de fichier caché, 133
  - Séparateur des noms d'autorisations, 219
- Point-virgule (;), device\_allocate, fichier, 99
- policy.conf, fichier
  - Description, 222–223, 223
- Mot-clé
  - Algorithme de mot de passe, 41
  - Autorisations RBAC, 222
  - Privilège, 222
  - Profil de droits, 222
- Mots-clés
  - Privilèges, 226
  - Propriétaire de station de travail, 222
- Spécification d'un algorithme de mot de passe
  - Service de noms, 67–68
- Spécification des algorithmes de chiffrement, 66–67
- Spécification des algorithmes de mot de passe, 66–67
- Port, mot-clé, Secure Shell, 339
- Port privilégié, Alternative à RPC sécurisé, 54
- Ports, Pour Kerberos KDC, 367
- Postsélection et audit, 554
- ppriv, commande, Débogage, 211
- ppriv, commande, Liste des privilèges, 209
- praudit, commande
  - Chaînage de la sortie auditreduce, 622
  - Consultation des enregistrements d'audit, 621–623
  - Conversion des enregistrements d'audit dans un format lisible, 622
  - Description, 646
  - Format XML, 622
  - Utilisation d'un script, 622–623
- PreferredAuthentications, mot-clé, Fichier ssh\_config, 339
- Préfixe de caret (^), Utilisation dans la valeur audit\_flags, 588
- Préfixe de classe d'audit, 648
- Présélection, Classes d'audit, 585–586
- Présélection des classes d'audit
  - Effet sur les objets publics, 554
- Présélection et audit, 554
- PreUserauthHook, mot-clé, ssh\_config, fichier, 339
- Prévention, Dépassement de la piste d'audit, 624–625
- Primaire, Nom de principal, 355
- Principal
  - Administration, 475–514
  - Affichage d'une sous-liste de principaux, 483
  - Affichage de la liste, 482–484
  - Affichage des attributs, 484–486
  - Ajout d'administration, 382, 389
  - Ajout d'un principal de service à keytab, 508
  - Ajout d'un principal de service à un fichier keytab, 509–510
  - Automatisation de création, 481
  - Comparaison d'ID utilisateur, 405–406
  - Création, 486–488
  - Création clntconfig, 383, 390
  - Création de l'host, 383, 390
  - Duplication, 489
  - Kerberos, 355
  - Liste des tâches d'administration, 480–481
  - Modification, 490–491



**Principal (Suite)**

- Nom de principal, 355
- Outil SEAM, panneau pour, 503–506
- Paramétrage des valeurs par défaut, 492–493
- Principal d'utilisateur, 355
- Principal de service, 355
- Suppression, 491
- Suppression d'un principal de service d'un fichier keytab, 511
- Suppression du fichier keytab, 511
- `principal`, fichier, Description, 532
- Principal d'utilisateur, Description, 355
- Principal de service
  - Ajout à un fichier keytab, 508, 509–510
  - Description, 355
  - Planification des noms, 366
  - Suppression d'un fichier keytab, 511
- `principal.kadm5`, fichier, Description, 532
- `principal.kadm5.lock`, fichier, Description, 532
- `principal.ok`, fichier, Description, 532
- `principal.ulong`, fichier, Description, 532
- Principe du moindre privilège, 160
- Printer Management (gestion des imprimantes) - RBAC), Profil de droits, 216
- `PrintLastLog`, mot-clé, Fichier `ssh_config`, 339
- `PrintMotd`, mot-clé, Fichier `sshd_config`, 339
- Prise en charge FIPS-140, Utilisation d'une carte &scsa6 par Secure Shell, 317
- `priv.debug`, entrée, `syslog.conf`, fichier, 226
- `PRIV_DEFAULT`, mot-clé
  - `policy.conf`, fichier, 222, 226
- `PRIV_LIMIT`, mot-clé
  - `policy.conf`, fichier, 222, 226
- `PRIV_PROC_LOCK_MEMORY`, privilège, 162
- `private`, niveau de protection, 527
- Privilège
  - Affectation à un script, 166
  - Audit, 227
  - Catégorie, 160
  - Commande, 225
  - Débogage, 167, 211
  - Description, 149, 160
  - Détermination des privilèges attribués directement, 206–207

**Privilège (Suite)**

- Différences avec le modèle superutilisateur, 161
- Exigence en matière de débogage, 211–213
- Hérité par les processus, 164
- Mise en oeuvre dans des jeux, 162
- Périphérique, 166–167
- `PRIV_PROC_LOCK_MEMORY`, 162
- Processus avec privilèges affectés, 164
- Protection des processus noyau, 159
- Recherche des privilèges manquants, 212
- Suppression d'un utilisateur, 166
- Suppression dans le jeu limite, 197
- Utilisation dans un script shell, 213–214
- `privilege`, jeton d'audit, 661
- Privilège de processus, 160
- Privilèges
  - Administration, 209
  - Affectation à l'utilisateur, 197
  - Affectation à un rôle, 195
  - Affectation à un utilisateur, 164
  - Affectation à une commande, 164
  - Ajout à une commande, 187
  - Comparés au modèle de superutilisateur, 158–167
  - Débogage
    - Utilisateurs, 189–192
  - Description, 160
  - Effet sur l'outil SEAM, 507
  - Escalade, 227
  - Exécution de commandes disposant d'un privilège, 165
  - Fichiers, 226–227
  - Liste, 205–206
  - Liste des tâches, 204
  - Liste sur un processus, 209–211
  - Programme conscient des privilèges, 164
  - Restriction d'utilisation dans un profil de droits, 187
  - Suppression du jeu de base, 187
  - Suppression du jeu limite, 187
  - Utilisation, 204
- Privilèges de liste, Outil SEAM, 507
- `PROC`, privilège, 160
- Procédure utilisateur
  - Calcul de la synthèse d'un fichier, 247–248
  - Chiffrement de clé privée des utilisateurs NIS, 294



- Procédure utilisateur (*Suite*)
  - chkey, commande, 295
  - Création d'un certificat autosigné, 273–274
  - Exportation de certificats, 276–277
  - Génération d'une clé symétrique
    - Utilisation de la commande dd, 240–242
  - Génération de phrase de passe pour keystore, 277–278
  - Importation de certificats, 274–275
  - Utilisation Secure Shell, 322–323
- Procédures utilisateur
  - Ajout de plug-ins à la KMF, 283–284
  - Allocation de périphériques, 85–90
  - Calcul du code MAC d'un fichier, 248–250
  - Chiffrement de fichiers, 240, 250–253
  - Endossement d'un rôle, 174–175
  - Génération d'une clé symétrique
    - Utilisation de la commande pktool, 243–247
  - Utilisation d'un rôle affecté, 174–175
  - Utilisation de la commande pktool, 272–273
- process, jeton d'audit, Format, 661
- Processus shell, Liste des privilèges, 209–211
- prof\_attr, base de données
  - Description, 222
  - Résumé, 220
- Profil, *Voir* Profil de droits
- Profil de droit Audit Control (contrôle d'audit),
  - Actualisation du service d'audit, 611–613
- Profil de droits
  - Affichage du contenu, 217
  - Base de données
    - Voir* Bases de données prof\_attr et exec\_attr
  - Contenu typique, 215
  - Description, 150, 155
  - Description des principaux profils de droits, 215
  - Printer Management (gestion des imprimantes), 216
- Profil de droits Audit Configuration (configuration d'audit), 646
  - Audit d'un rôle, 184–185
  - Configuration de la stratégie d'audit, 590–592
- Profil de droits Audit Control (contrôle d'audit), 646
  - Activation du service d'audit, 614
  - Désactivation du service d'audit, 613–614
- Profil de droits Audit Review (vérification de l'audit), 646
- Profil de droits de configuration de l'audit, Présélection des classes d'audit, 585–586
- Profil de droits Device Management (gestion de périphériques), 96–97
- Profil de droits Device Security (sécurité des périphériques), 86, 96–97
- Profil de droits Media Backup (sauvegarde des médias)
  - Attribution à des utilisateurs de confiance, 148, 180
- Profil de droits Media Restore (restauration des médias), Attribution à des utilisateurs de confiance, 180
- Profil de droits User Security (sécurité utilisateur),
  - Modification de la présélection d'audit pour les utilisateurs, 586–590
- Profil de droits ZFS File System Management (gestion de système de fichiers ZFS), Création de systèmes de fichiers d'audit, 598–601
- Profil de droits ZFS Storage Management (gestion de stockage ZFS), Création de pools pour les fichiers d'audit, 598–601
- Profil des droits de configuration de l'audit, Affichage des paramètres par défaut de l'audit, 583–585
- profiles, commande, Description, 223
- Profils de droits
  - All (tous), 216
  - Attribution à des utilisateurs de confiance, 148, 180
  - Service d'audit, 646–647
  - Authentification à l'aide du mot de passe utilisateur, 201
  - Basic Solaris User (utilisateur Solaris de base), 216
  - Console User (utilisateur de la console), 216, 218
  - Dépannage, 189–192
  - Device Management (gestion de périphériques), 96–97
  - Device Security (sécurité des périphériques), 86, 96–97
  - Modification, 186–187
  - Modification du contenu, 186–187
  - Operator (opérateur), 216
  - Ordre de recherche, 217
  - Prévention de l'escalade des privilèges, 148, 180
  - Stop (arrêt), 216, 218

Profils de droits (*Suite*)

- System Administrator (administrateur système), 216

- Utilisation du profil de droits System Administrator (administrateur système), 71

PROFS\_GRANTED, mot-clé, `policy.conf`, fichier, 222

## Programme

- Conscient des privilèges, 163, 164

- Recherche d'autorisations RBAC, 189

`project.max-locked-memory`, contrôle de ressources, 162

PROM, mode de sécurité, 71–73

## Propagation

- Base de données KDC, 369

- Base de données Kerberos, 433–434

## Propriété, fichier

- ACL UFS, 130–131

- Modification, 124, 134–135

- Modification de propriété de groupe, 135

Propriété de fichiers, ACL, 51

Propriété système, Privilège lié à, 160

## Protection

- BIOS, pointeur, 71–72

- Contenu de keystore, 276

- Fichiers avec structure cryptographique, 240

- Par mot de passe avec structure cryptographique, 272–273

- Problèmes de sécurité causés par des fichiers exécutables 32 bits, 131–132

- PROM, 71–72

- Système pour les programmes à risque, 139

## Protection, fichier

- ACL UFS, 130–131

- Autorisation UNIX, 132–133

- Liste des tâches des autorisations UNIX, 132

- Procédures utilisateur, 132–133

Protection de fichier, Autorisation UNIX, 123–130

Protocol, mot-clé, Secure Shell, 339

ProxyCommand, mot-clé, Fichier `ssh_config`, 339

pseudo-tty, Utilisation dans Secure Shell, 335

PubkeyAuthentication, mot-clé, Secure Shell, 340

Public, répertoire, Sticky bit, 127

public, stratégie d'audit

- Description, 575

public, stratégie d'audit (*Suite*)

- Événement en lecture seule, 575

publickey, carte, Authentification DH, 288–292

`pwcheck_method`, option, SASL, 311

**Q**

qsize, attribut, Plug-in d'audit, 592–594

**R**

-R, option

- `bart create`, 108, 111

- `ssh`, commande, 328–329

-r, option

- `bart create`, 111

- `passwd`, commande, 39

Rapports, BART, 103

## RBAC

- Affichage de tous les attributs de sécurité

  - RBAC, 170–171

- Affichage de vos droits, 171–174

- Ajout d'utilisateurs privilégiés, 197

- Ajout de rôles, 181–183

- Audit des rôles, 184–185

- Autorisation, 152–153

- Base de données, 220–223

- Base de données d'autorisations, 221

- Base de données de profils de droits, 222

- Commande d'administration, 223–224

- Commande pour la gestion, 223–224

- Comparé au modèle de superutilisateur, 145–149

- Concept de base, 149–151

- Configuration, 177–192

- Création de profils de droits, 186–187

- Dépannage, 189–192

- Élément, 149–151

- Limitation des droits, 199–201

- Limitation des utilisateurs aux applications de bureau, 198–199

- Modification de rôles, 194–195

- Modification des mots de passe de rôle, 193–194

- Modification des utilisateurs, 196–197

RBAC (*Suite*)

- Obtention des droits d'administration, 175–177
- Planification, 178–180
- Profil d'audit, 647
- Profil de droits, 155
- Recherche d'autorisations dans un script ou un programme, 189
- Sécurité de scripts, 188
- Service de noms, 220
- Shell de profil, 156–157
- Utilisation du mot de passe utilisateur pour endosser un rôle, 201–202
- Utilisation du mot de passe utilisateur pour utiliser le profil de droits, 201
- Valeurs par défaut, 170–177

RC4, *Voir* Fournisseur de noyau ARCFOUR

## rcp, commande

- Kerberos, 524–527, 533

## rd, modificateur d'événement d'audit, 659

## read\_kt, commande, 512, 513

## reauth\_timeout, option, SASL, 311

## Redémarrage

- Services cryptographiques, 267–268
- ssh, service, 321
- sshd, démon, 321

## Réduction

- Espace de stockage requis pour les fichiers d'audit, 578

- Fichier d'audit, 617–619

## Référentiel, Installation de fournisseurs tiers, 259

## RekeyLimit, mot-clé, ssh\_config, fichier, 340

## rem\_drv, commande, Description, 95

## RemoteForward, mot-clé, Fichier ssh\_config, 340

## Remplacement

- Classes d'audit présélectionnées, 585–586
- Superutilisateur avec des rôles, 178–180

## Répertoire

- Voir aussi* Fichier

- Affichage des fichiers et d'informations connexes, 124, 133–134

## Autorisation

- Défaut, 127–128
- Description, 125

## Répertoire public, 127

## Répertoire d'audit, Création de systèmes de fichiers, 598–601

## Répertoires publics, Audit, 554

## Réseau, Privilège lié à, 160

## Restauration, Fournisseur cryptographique, 262

## Restriction

- Accès superutilisateur à distance, 70–71
- Privilèges d'utilisateur, 187
- Superutilisateur, 69–71
- Utilisation des privilèges dans un profil de droits, 187

## Restriction de l'accès aux serveurs KDC, 453

## Restrictions de l'accès de connexion,

- svc:/system/name-service/switch:default, 38

## RETRIES dans Secure Shell, 341

## return, jeton d'audit, Format, 661–662

## Réussite, Préfixe de classe d'audit, 648

## Réutilisation des objets, Périphériques, 101–102

## rewoffl, option

- mt, commande

- Nettoyage de périphériques à bande, 101

## .rhosts, fichier, Description, 343

## RhostsAuthentication, mot-clé, Secure Shell, 340

## RhostsRSAAuthentication, mot-clé, Secure Shell, 340

## rlogin, commande

- Kerberos, 524–527, 533

## rlogind, démon, Kerberos, 534

## Rôle

- Attribution avec la commande usermod, 183–184

- Description, 155–156

- Détermination des commandes privilégiées d'un rôle, 208

- Détermination des privilèges attribués directement, 207

- Endosser après connexion, 156

- Endosser dans une fenêtre de terminal, 156–157

- Liste des rôles locaux, 174, 223

- Résumé, 150

- Rôle recommandé, 146

- Rôle root endossé, 174–175

- Utilisation, RBAC, 146

- Utilisation pour accéder au matériel, 71–72

## Rôle endossé, root, 174–175

## Rôle root

- Modification du mot de passe, 61

- Rôle fourni, 147

## Rôle root, Transformation de l'utilisateur root, 203

## roLeadd, commande

- Description, 224

- Utilisation, 181

## roLeauth, mot-clé, Mots de passe pour les

- rôles, 201–202

## roLemod, commande

- Description, 224

- Modification des propriétés de rôle, 195, 200

- Mots de passe pour les rôles, 201–202

## Rôles

- Affectation de privilèges, 195

- Ajout à un utilisateur, 196

- Audit, 184–185

- Authentification à l'aide du mot de passe utilisateur, 201–202

- Création, 181–183

  - Gestion de la cryptographie, rôle, 184

- Endossement, 174–175

- Endossement dans une fenêtre de terminal, 174–175

- Modification, 194–195

- Modification des propriétés, 194–195

- Modification du mot de passe, 193–194

- Modification du rôle root en utilisateur, 202–204

## rôles, utilisant le mot de passe utilisateur, 151

## Rôles

- Utilisation d'un rôle affecté, 174–175

## roles, commande

- Description, 223

- Utilisation, 174

## root, compte, Description, 42

## root, principal, Ajout au fichier keytab de l'hôte, 508

## root, rôle, Modification en utilisateur root, 202–204

## root, rôle (RBAC)

- Dépannage, 204

- Rôle endossé, 174–175

## root, utilisateur

- Affichage des tentatives d'accès sur la console, 70–71

- Contrôle des tentatives de la commande su, 69–70

root, utilisateur (*Suite*)

- Remplacement dans RBAC, 156

- Restriction d'accès, 52

- Restriction de l'accès à distance, 70–71

- Suivi des connexions, 46

- Surveillance des tentatives de commande su, 46

## RPC sécurisé

- Alternative, 54

- Description, 287

- Kerberos, 288

- Mise en oeuvre, 289–292

- Présentation, 53–55

- Serveur de clés, 289

## RSA, fournisseur de noyau, 255

## RSAAuthentication, mot-clé, Secure Shell, 340

## rsh, commande

- Kerberos, 524–527, 533

## rsh, commande (shell restreint), 47

## rshd, démon, Kerberos, 534

## rstchown, variable système, 135

**S**

- S, option, st\_clean, script, 102

- s, option

  - audit, commande, 611–613, 614

- safe, niveau de protection, 527

## SASL

- Option, 311–312

- Plug-in, 310

- Présentation, 309

- Variable d'environnement, 310

- saslauthd\_path, option, SASL, 311

## Sauvegarde

- Base de données Kerberos, 433–434

- KDC esclaves, 367

## scp, commande

- Copie de fichiers, 329–330

- Description, 345

## Script

- Exécution avec des privilèges, 166

- Nettoyage de périphériques, 101–102

- Recherche d'autorisations RBAC, 189

**Script (Suite)**

- Script de nettoyage de périphériques
  - Voir aussi* Script de nettoyage de périphériques
- Sécurité, 188
- Traitement de la sortie praudit, 622–623
- Utilisation de privilèges, 213–214

**Script de nettoyage de périphériques**

- Description, 101–102
- Écriture de nouveaux scripts, 102
- Lecteur de bande, 100, 101
- Options, 102
- Périphérique audio, 102
- Réutilisation des objets, 101–102
- Unité de CD-ROM, 102
- Unité de disquette, 102

**Script de nettoyage de périphériques du lecteur de bande Archive, 101****Script de nettoyage de périphériques du lecteur de bande Xylogics, 101****Script shell, Privilège d'écriture, 213****Scripts**

- `audit_warn`, script, 594–595, 645
- Exemple de surveillance des fichiers d'audit, 578

**Secure Shell**

- Administration, 333–335
- Authentification
  - Conditions requises, 314–315
- Authentification avec clé publique, 314
- Base d'OpenSSH, 316–317
- Configuration des clients, 336
- Configuration du serveur, 336
- Configuration du transfert de port, 321
- Connexion à un hôte distant, 325–326
- Connexion au travers d'un pare-feu, 330
- Connexion en moins d'invites, 327–328
- Connexion extérieure au pare-feu
  - Fichier de configuration, 330–332
  - Ligne de commande, 332
- Copie de fichiers, 329–330
- Création de clés, 323–325
- Description, 313
- Exécution des commandes, 335
- Fichier, 342
- Génération de clés, 323–325

**Secure Shell (Suite)**

- Liste des tâches de l'administrateur, 317, 318
- Méthode d'authentification, 314–315
- Modification dans la version actuelle, 316–317
- Modification de la phrase de passe, 325
- Mot-clé, 336–342
- Nommage des fichiers d'identité, 342
- Procédure d'authentification, 334–335
- Procédure utilisateur, 322–323
- `scp`, commande, 329–330
- Session standard, 333–335
- Spécification d'exceptions aux valeurs par défaut du système, 321–322
- TCP, 321
- Transfert d'un message, 329
- Transfert de port distant, 329
- Transfert de port local, 329
- Transmission de données, 335
- Utilisation du transfert de port, 328–329
- Utilisation sans mot de passe, 327–328
- Variable d'environnement, 341–342
- Versions du protocole, 313

**Sécurisation**

- Liste des tâches liées aux connexions, 60–61
- Liste des tâches liées aux mots de passe, 60–61
- Réseau à l'installation, 49

**Sécurité**

- Allocation de périphériques, 81–102
- Audit, 551–566
- Authentification DH, 289–292
- BART, 103–122
- Calcul de synthèses de fichiers, 247–248
- Calcul du code MAC de fichiers, 248–250
- Chiffrement de fichier, 250–253
- Chiffrement de mot de passe, 40
- Empêcher la connexion à distance, 70–71
- Matériel système, 71–73
- `net services limited`, option d'installation, 49
- NFS client-serveur, 289–292
- Option d'installation, 49
- Périphériques, 43–46
- Présentation des stratégies, 33–34
- Protection contre le déni de service, 49
- Protection contre les chevaux de Troie, 47

**Sécurité (Suite)**

- Protection de la PROM, 71–73
- Protection des périphériques, 101–102
- Protection du matériel, 71–73
- Réseau non sécurisé, 330
- Script, 188
- Secure by Default, 49
- Secure Shell, 313–332
- Structure cryptographique, 231–237
- Structure de gestion des clés, 269–284
- Système, 37

**Sécurité des machines, Voir Sécurité système****Sécurité du système**

- Accès, 37
- Accès aux machines, 38
- Chiffrement de mot de passe, 40
- Comptes spéciaux, 42
- Contrôle d'accès basé sur les rôles (RBAC, role-based access control), 145–149
- Modification
  - Mot de passe root, 61
- Mot de passe, 39
- Présentation, 37
- Protection du matériel, 38
- Restriction d'accès par connexion, 38
- Restrictions d'accès par connexion, 38
  - root, restrictions d'accès, 52
- Shell restreint, 47, 48
- Surveillance de la commande su, 46

**Sécurité informatique, Voir Sécurité système****Sécurité physique, Description, 38****Sécurité réseau**

- Authentification, 53–55
- Autorisation, 53–55
- Contrôle d'accès, 52–56
- Génération de rapports sur les problèmes, 57
- Présentation, 53
- Système pare-feu
  - Eclatement de paquets, 56
  - Hôte de confiance, 56
  - Nécessité, 55

**Sécurité système**

- Affichage
  - Etat de connexion d'un utilisateur, 61–62

**Sécurité système, Affichage (Suite)**

- Utilisateur sans mot de passe, 62
- Contrôle de la commande su, 69–70
- Enregistrement des tentatives de connexion ayant échoué, 63–64
- Privileges, 158–167
- Protection du matériel, 71–73
- RBCA (role-based access control, contrôle de l'accès basé sur le rôle), 46
- Restriction de l'accès root, 70–71
- Restriction de l'accès root à distance, 70–71
- Système pare-feu, 55–56

**Sélection**

- Classes d'audit, 585–586
  - Enregistrement d'audit, 619–621
  - Événement de piste d'audit, 619–621
- sendmail, commande, Autorisation requise, 225

**seq, stratégie d'audit**

- Description, 576
- sequence, jeton, 576, 662

**sequence, jeton d'audit**

- Format, 662
- seq, stratégie d'audit, 662

**ServerAliveCountMax, mot-clé, ssh\_config, fichier, 340****ServerAliveInterval, mot-clé, ssh\_config, fichier, 340****ServerKeyBits, mot-clé, sshd\_config, fichier, 340****Serveur**

- AUTH\_DH, session client-serveur, 289–292
- Configuration pour Secure Shell, 336
- Définition dans Kerberos, 535
- Obtention d'accès à l'aide de Kerberos, 541–544

**Serveur d'application, Configuration, 400–403****Serveur de clés**

- Démarrage, 293
- Description, 289

**Serveurs**

- Domaines, 356
- Obtention d'informations d'identification, 542–543

**Serveurs NFS, Configuration de Kerberos, 404–405****Service**

- Définition dans Kerberos, 535
- Désactivation sur un hôte, 512–514

- Service (*Suite*)
  - Obtention d'accès à un service spécifique, 543–544
- Service d'audit
  - Voir aussi* Audit
  - Activation, 614
  - Actualisation du noyau, 611
  - Configuration de la stratégie, 590–592
  - Configuration des contrôles de file d'attente, 592–594
  - Création de la piste d'audit, 652
  - Dépannage, 627–629
  - Désactivation, 613–614
  - Stratégie, 573
  - Valeurs par défaut, 643–644
- Service d'octroi de tickets, *Voir* TGS
- Service de noms
  - Voir* Service de noms individuel
  - Champ d'application et RBAC, 157
- Service de noms LDAP
  - Mot de passe, 40
  - Spécification d'un algorithme de mot de passe, 68–69
- Service de noms NIS
  - Authentification, 287
  - Mot de passe, 39
  - Spécification de l'algorithme de mot de passe, 67–68
- Service de sécurité, Kerberos, 357
- Services cryptographiques, *Voir* Structure cryptographique
- setflags, option, auditconfig, commande, 585–586
- setgid, autorisation
  - Description, 126–127
  - Mode absolu, 130, 139
  - Mode symbolique, 129
  - Risque de sécurité, 127
- setnaflags, option, auditconfig, commande, 585–586
- setpin, sous-commande, pktool, commande, 277–278
- setplugin, option
  - auditconfig, commande, 604–605, 605–606
- setpolicy, option, auditconfig, commande, 590–592
- setuid, autorisation
  - Description, 126
  - Mode absolu, 130, 139
  - Mode symbolique, 129
  - Risque de sécurité, 48, 126
- setuid, autorisations, Recherche de fichiers avec jeu d'autorisations, 139
- sftp, commande
  - Audit du transfert de fichiers, 640–641
  - Copie de fichiers, 330
  - Description, 345
- sh, commande, Version privilégiée, 156–157
- SHA1, fournisseur de noyau, 255
- SHA2, fournisseur de noyau, 255
- Shell, Version privilégiée, 156–157
- Shell Bourne, Version privilégiée, 156–157
- Shell de profil, Description, 156–157
- Shell Korn, Version privilégiée, 156–157
- Shell restreint (rsh), 47
- Shells de profil
  - Limitation des droits, 199–201
  - Limitation des utilisateurs aux applications de bureau, 198–199
  - Ouverture, 175–177
- .shosts, fichier, Description, 343
- shosts.equiv, fichier, Description, 343
- Signature
  - CSR PKCS #10, 282–283
  - Utilisation de la commande pktool, 282–283
- Signature des fournisseurs, Structure cryptographique, 237
- Signe arobase (@), device\_allocate, fichier, 100
- Signe dièse (#)
  - device\_allocate, fichier, 100
  - device\_maps, fichier, 99
- Signe égal (=), Symbole d'autorisations de fichier, 129
- Signe moins (-)
  - Entrée dans le fichier sulog, 69
  - Préfixe de classe d'audit, 648
  - Symbole d'autorisations de fichier, 129
  - Symbole de type de fichier, 124
- Signe plus (+)
  - Entrée dans le fichier sulog, 69
  - Préfixe de classe d'audit, 648



Signe plus (+) (*Suite*)

- Symbole d'autorisations de fichier, 129

- Signe plus (+) dans les préfixes de classe d'audit, 605

- slave\_datatrans, fichier

- Description, 532

- Propagation KDC, 433–434

- slave\_datatrans\_slave, fichier, Description, 532

## SMF

- Activation du serveur de clés, 293

- auditd, service, 643–644

- Gestion de la configuration Secure by Default, 49

- kcfd, service, 235

- Redémarrage Secure Shell, 321

- Service d'allocation de périphériques, 96

- Service de structure cryptographique, 235

- ssh, service, 321

- socket, jeton d'audit, 662

- Softtoken PKCS #11, Gestion de keystore, 271

- solaris.device.revoke, autorisation, 98

- Sommaire de l'aide, Outil SEAM, 478

- sp, modificateur d'événement d'audit, 659

- Spécifique à Kerberos, Terminologie, 534–535

- sr\_clean script, Description, 102

- ssh, commande

- Description, 345

- Option du transfert de port, 328–329

- Options de substitution des mots-clés, 345

- Utilisation, 325–326

- Utilisation d'une commande proxy, 332

- ssh-add, commande

- Description, 345

- Exemple, 327–328

- Stockage de clés privées, 327–328

- ssh-agent, commande

- Description, 345

- Ligne de commande, 327–328

- .ssh/config, fichier

- Description, 344

- Remplacement, 344

- ssh\_config, fichier

- Configuration de Secure Shell, 336

- Mot-clé, 336–342

- Voir Mot-clé spécifique

- Paramètre spécifique à l'hôte, 341

- ssh\_config, fichier (*Suite*)

- Remplacement, 344

- ssh\_host\_dsa\_key, fichier, Description, 342

- ssh\_host\_dsa\_key.pub, fichier, Description, 343

- ssh\_host\_key, fichier, Remplacement, 344

- ssh\_host\_key.pub, fichier, Description, 343

- ssh\_host\_rsa\_key, fichier, Description, 342

- ssh\_host\_rsa\_key.pub, fichier, Description, 343

- .ssh/id\_dsa, fichier, 344

- .ssh/id\_rsa, fichier, 344

- .ssh/identity, fichier, 344

- ssh-keygen, commande

- Description, 345

- Protection par phrase de passe, 316

- Utilisation, 323–325

- ssh-keyscan, commande, Description, 345

- ssh-keysign, commande, Description, 345

- .ssh/known\_hosts, fichier

- Description, 343

- Remplacement, 344

- ssh\_known\_hosts, fichier, 343

- .ssh/rc, fichier, Description, 344

- sshd, commande, Description, 345

- sshd\_config, fichier

- Description, 342

- Mot-clé, 336–342

- Voir Mot-clé spécifique

- Remplacement des entrées

- /etc/default/login, 341–342

- sshd.pid, fichier, Description, 343

- sshr, fichier, Description, 344

- st\_clean, script

- Description, 101

- Lecteur de bande, 101

- stash, fichier

- Création, 396, 443

- Définition, 535

- Sticky bit, autorisation

- Description, 127

- Mode absolu, 130, 139

- Mode symbolique, 129

- Stockage

- Fichier d'audit, 569–570

- Fichiers d'audit, 598–601



- Stockage (*Suite*)
  - Phrase de passe, 252
- Stop (arrêt), RBAC, Profil de droits, 216
- Stratégie
  - Administration, 475–514
  - Audit, 573–576
  - Définition dans la structure cryptographique, 234
  - Définition dans Oracle Solaris, 33–34
  - Périphériques, 82–83
  - Présentation, 33–34
- Stratégie d'audit
  - Affichage des paramètres par défaut, 583–585
  - Définition, 590–592
  - Définition dans la zone globale, 647
  - Définition de ahl, 591
  - Définition de la stratégie arge, 633
  - Définition de la stratégie argv, 633
  - Définition de perzone, 592
  - Description, 553
  - Effet, 573–576
  - Jeton ajouté, 649
  - Jeton d'audit, 649
  - Par défaut, 573–576
  - Paramètre de zone globale, 564–565
  - public, 575
  - Sans impact sur les jetons, 649
- Stratégie d'audit active, Stratégie d'audit temporaire, 590–592
- Stratégie d'audit configurée, Stratégie d'audit permanente, 590–592
- Stratégie d'audit permanente, Stratégie d'audit configurée, 590–592
- Stratégie d'audit temporaire
  - Définition, 591–592
  - Stratégie d'audit active, 590–592
- Stratégie de périphériques
  - add\_drv, commande, 95
  - Affichage, 82–83
  - Audit des modifications, 84
  - Commande, 95
  - Configuration, 82–85
  - Gestion des périphériques, 82
  - Liste des tâches, 82
  - Modification, 83–84
- Stratégie de périphériques (*Suite*)
  - Présentation, 43–46
  - Protection du noyau, 94–102
  - Suppression de périphériques, 84
  - update\_drv, commande, 83–84, 95
- Stratégie de sécurité, Valeur par défaut (RBAC), 220
- Stratégies
  - Affichage de liste, 495–497
  - Affichage des attributs, 497–499
  - Création (Kerberos), 486, 499–500
  - Liste des tâches d'administration, 494–495
  - Modification, 501–502
  - Mots de passe, 520
  - Outil SEAM, panneau pour, 503–506
  - Spécification de l'algorithme de mots de passe, 66–69
  - Suppression, 502–503
- StrictHostKeyChecking, mot-clé, Fichier ssh\_config, 340
- StrictModes, mot-clé, Fichier sshd\_config, 340
- Structure cryptographique
  - Actualisation, 267–268
  - Administration avec rôle, 184
  - Bibliothèque PKCS #11, 233
  - Commande au niveau de l'utilisateur, 236
  - Connexion de fournisseurs, 237
  - Consommateurs, 233
  - cryptoadm, commande, 235
  - Définition des termes, 233
  - Description, 231–233
  - elfsign, commande, 236
  - Enregistrement des fournisseurs, 237
  - Fournisseur, 233
  - Fournisseurs, 233
  - Interaction, 235
  - Liste des fournisseurs, 255–258
  - Liste des tâches, 239
  - Messages d'erreur, 253
  - Plug-ins matériels, 233
  - Redémarrage, 267–268
  - Signature des fournisseurs, 237
  - Zones, 237, 267–268
- Structure de gestion des clés (KMF), Voir KMF

**su, commande**

- Affichage des tentatives d'accès sur la console, 70–71

- Contrôle de l'utilisation, 69–70

- Endossement d'un rôle, 174–175

- su, fichier, Contrôle de la commande su, 69–70

- subject, jeton d'audit, Format, 662–663

- Subsystem, mot-clé, Fichier sshd\_config, 340

- su log, fichier, 69–70

- Contrôle du contenu, 69

- SUPATH dans Secure Shell, 342

**Superutilisateur**

- Comparé au modèle de privilège, 158–167

- Comparé au modèle RBAC, 145–149

- Contrôle des tentatives d'accès, 70–71

- Contrôle et restriction, 69–71

- Dépannage de l'accès à distance, 71

- Dépannage de l'endossement de root en tant que rôle, 204

- Différences avec le modèle de privilège, 161

- Suppression dans RBAC, 156

**Suppression**

- Archivage des fichiers d'audit, 625

- Audit spécifique à l'utilisateur, 589

- Événements d'audit du fichier

- audit\_event, 636–637

- Fichier d'audit, 617

- Fichier d'audit not\_terminated, 623–624

- Fournisseur cryptographique, 261

- Fournisseur de logiciels

- Définitivement, 263, 264

- Temporairement, 263

- Fournisseurs cryptographiques, 262

- Plug-ins de la KMF, 283–284

- Principal (Kerberos), 491

- Principal avec la commande kt remove, 511

- Principal de service de fichier keytab, 511

- Privilège du jeu limite, 197

- Privilèges du jeu de base, 187

- Privilèges du jeu limite, 187

- Service d'hôte, 513

- Stratégie de périphériques, 84

- Stratégies (Kerberos), 502–503

**Surveillance**

- Piste d'audit en temps réel, 578

- su, tentatives de commande, 46

- Utilisation des commandes privilégiées, 184–185

- Utilisation du système, 50

- svc:/system/device/allocate, Service d'allocation de périphériques, 96

**svcadm, commande**

- Activation de la structure

- cryptographique, 267–268

- Activation du démon keyserver, 293

- Actualisation de la structure

- cryptographique, 258–260

- Administration de la structure

- cryptographique, 235

- Redémarrage

- Secure Shell, 321

- syslog, daemon, 65

- Redémarrage du démon

- syslog, 605

**svcs, commande**

- Liste des services cryptographiques, 267–268

- Liste des services du serveur de clés, 293

- Symbole double dollar (\$\$), Numéro du processus de shell parent, 210

**Symbolique, mode**

- Description, 128

- Modification des autorisations de fichier, 136

**Synchronisation d'horloge**

- KDC esclave, 396, 443

- KDC esclave Kerberos, 396

- KDC maître, 384, 391

- KDC maître Kerberos, 384, 391

- Planification Kerberos, 369

- Présentation, 427–428

- Serveur esclave Kerberos, 443

- Syntaxe de citation dans BART, 120

**Synthèse**

- Calcul pour un fichier, 247–248

- Fichier, 247–248, 248

- SYS, privilège, 160

- syslog.conf, fichier

- Audit, 646

- audit.notice, niveau, 605

- syslog.conf, fichier (*Suite*)
    - Débogage de privilège, 226
    - Enregistrement des tentatives de connexion ayant échoué, 64–66
    - Message de pile exécutable, 132
    - Niveau kern.notice, 132
    - priv.debug, entrée, 226
  - SYSLOG\_FAILED\_LOGINS
    - Secure Shell, 341
    - Variable système, 64
  - syslogFacility, mot-clé, Fichier sshd\_config, 340
  - System Administrator (administrateur système), RBAC,
    - Profil de droits, 216
  - System Administrator (administrateur système) (RBAC), Protection du matériel, 71
  - /system/volatile/sshd.pid, fichier,
    - Description, 343
  - Système, Protection contre les programmes dangereux, 139
  - Système, sécurité
    - ACL UFS, 130–131
    - Liste des tâches, 139
    - Protection contre les programmes dangereux, 139
  - Système, variable
    - noexec\_user\_stack\_log, 141
    - rstchown, 135
  - Système à connexion unique, 524–530
    - Kerberos, 349
  - Système de fichiers
    - NFS, 287
    - Partage de fichiers, 51
    - Sécurité
      - Authentification et NFS, 287
  - Système de fichiers d'audit, Description, 552
  - Système de fichiers NFS
    - Authentification, 287
    - Sécurité client-serveur, 289–292
  - Système pare-feu
    - Connexion depuis l'extérieur, 332
    - Connexion extérieure avec Secure Shell
      - Fichier de configuration, 330–332
      - Ligne de commande, 332
    - Connexion sécurisée à l'hôte, 330
    - Eclatement de paquets, 56
  - Système pare-feu (*Suite*)
    - Hôte de confiance, 56
    - Sécurité, 55–56
    - Transfert des paquets, 56
  - Systèmes de fichiers
    - Activation de l'analyse de virus, 78
    - Ajout d'un moteur d'analyse de virus, 78
    - Analyse de virus, 77–78
    - Exclusion de fichiers des analyses antivirus, 80
  - Systèmes de fichiers NFS, Accès sécurisé AUTH\_DH, 295
  - Systèmes de fichiers ZFS, Création pour les fichiers d'audit binaires, 598–601
- ## T
- T option
    - encrypt, commande, 251
    - mac, commande, 249
  - t, option, audit, commande, 613–614
  - Table, gsscred, 546
  - Table d'informations d'identification, Ajout d'entrée unique, 406–407
  - tail, commande, Exemple d'utilisation, 579
  - Taille des fichiers d'audit
    - Réduction, 617–619
    - Réduction de l'espace de stockage requis, 578
  - TCP
    - Adresses, 659
    - Secure Shell, 321, 335
  - Technologie à clé publique, Voir PKI
  - telnet, commande
    - Kerberos, 524–527, 533
  - telnetd, démon, Kerberos, 534
  - Temps universel (UTC)
    - Horodatage utilisé en audit, 652
    - Utilisation de l'horodatage dans l'audit, 617
  - Tentative de connexion ayant échoué
    - loginlog, fichier, 63–64
    - syslog.conf, fichier, 64–66
  - Terminologie
    - Kerberos, 534–540
    - Spécifique à Kerberos, 534–535
    - Spécifique à l'authentification, 535–536
  - text, audit jeton, Format, 663

## TGS, Obtention d'informations

d'identification, 541–542

## TGT, Kerberos, 351–353

## Ticket

Affichage, 517–518

Avertissement d'expiration, 421

Création, 515–516

Création avec kinit, 516

Définition, 350

Destruction, 518

Durée de vie, 538–539

Durée de vie renouvelable maximale, 539

## Fichier

*Voir* Cache d'informations d'identification

Initial, 536

klist, commande, 517–518

Non valide, 537

Obtention, 515–516

Option -F ou -f, 526

Option -k, 526

Postdatable, 537

Proxy, 537

Renouvelable, 537

Requis pour un domaine spécifique, 526

Transmissible, 516, 527–528, 536

Utilisable avec proxy, 537

Ticket d'octroi de ticket, *Voir* TGT

## Ticket initial, Définition, 536

## Ticket non valide, Définition, 537

## Ticket postdaté

Définition, 537

Description, 351

## Ticket proxy, Définition, 537

## Ticket renouvelable, Définition, 537

## Ticket transmissible

Exemple, 516

Option -F, 526, 527–528

Option -f, 525, 527–528

## Ticket utilisable avec proxy, Définition, 537

## Tickets

Définition dans Kerberos, 535

Informations d'identification, 351

Postdatés, 351

Transmissibles, 351

Tickets (*Suite*)

Types, 536–540

## Tickets transmissibles

Définition, 536

Description, 351

TIMEOUT dans Secure Shell, 341

/tmp/krb5cc\_uid, fichier, Description cache

d'informations d'identification, 532

/tmp/ovsec\_admin.xxxxx, fichier, Description, 532

TMPFS, système de fichiers, Sécurité, 127

trail, stratégie d'audit

Description, 576

et trailer, jeton, 576

trailer, jeton d'audit

Format, 663

Ordre d'un enregistrement d'audit, 663

praudit, affichage, 663

Transaction rediffusée, 291

Transfert de fichiers, Audit, 640–641

## Transfert de paquets

Eclatement de paquets, 56

Sécurité du pare-feu, 55

## Transfert de port

Configuration dans Secure Shell, 321

Secure Shell, 329

## Transfert X11, Configuration dans le fichier

ssh\_config, 338

Transmission de données, Secure Shell, 335

Transmission des connexions X11, Configuration dans

le fichier ssh\_config, 338

Transmission X11, Secure Shell, 335

Transparence, Définition dans Kerberos, 350

truss, commande, Débogage de privilèges, 211

Types de tickets, 536–540

TZ dans Secure Shell, 341

**U**

-u, option, allocate, commande, 98

## UDP

Adresses, 659

Secure Shell, 321

Transfert de port, 321

Utilisation pour les journaux d'audit à distance, 558

- umask, valeur
  - Création de fichier, 127–128
  - Valeurs typiques, 127
- umount, commande, Attribut de sécurité, 87
- Unité de CD-ROM
  - Allocation, 93
  - Sécurité, 102
- Unité de disquette, Script de nettoyage de périphériques, 102
- UNIX, autorisation de fichiers, *Voir* Fichier, autorisation
- update\_drv, commande
  - Description, 95
  - Utilisation, 83–84
- URL d'aide en ligne, Outil graphique Kerberos, 373
- use\_authid, option, SASL, 311
- use of authorization, jeton d'audit, 663
- use of privilege, jeton d'audit, 664
- UseOpenSSLEngine, mot-clé, Secure Shell, 340
- UsePrivilegedPort, mot-clé, Secure Shell, 340
- user, jeton d'audit, 664
- User, mot-clé, Fichier ssh\_config, 340
- user\_attr, base de données
  - Description, 220
  - Liste des exceptions utilisateur à la présélection d'audit, 586–590
- user\_attr, fichier, Exceptions aux classes d'audit à l'échelle du système, 556
- useradd, commande, Description, 224
- userattr, commande
  - Affichage des exceptions à l'audit à l'échelle du système, 583–585
  - Description, 224
- userdel, commande, Description, 224
- UserKnownHostsFile, mot-clé, Fichier ssh\_config, 340
- UserKnownHostsFile2, mot-clé, *Voir* UserKnownHostsFile, mot-clé
- usermod, commande
  - audit\_flags, mot-clé, 586–590
- usermod, commande
  - Description, 224
  - Exceptions à l'audit à l'échelle du système, 556
- usermod, commande (*Suite*)
  - Limitation de l'utilisateur aux icônes de bureau uniquement, 199
  - Modification des propriétés RBAC de l'utilisateur, 196
- usermod, commande
  - Spécification des exceptions utilisateur à la présélection d'audit, 586–590
  - Utilisation du préfixe de caret (^) pour l'exception audit\_flags, 588
- usermod, commande
  - Utilisation pour l'attribution du rôle, 183–184
- UseRsh, mot-clé, ssh\_config, fichier, 340
- /usr/bin/ftp, commande, Kerberos, 533
- /usr/bin/kdestroy, commande, Kerberos, 533
- /usr/bin/kinit, commande, Kerberos, 533
- /usr/bin/klist, commande, Kerberos, 533
- /usr/bin/kpasswd, commande, Kerberos, 533
- /usr/bin/ktutil, commande, Kerberos, 533
- /usr/bin/kvno, commande, Kerberos, 533
- /usr/bin/rcp, commande, Kerberos, 533
- /usr/bin/rlogin, commande, Kerberos, 533
- /usr/bin/rsh, commande, Kerberos, 533
- /usr/bin/telnet, commande, Kerberos, 533
- /usr/lib/kprop, commande, Description, 533
- /usr/lib/krb5/kadmind, démon, Kerberos, 534
- /usr/lib/krb5/kpropd, démon, Kerberos, 534
- /usr/lib/krb5/krb5kdc, démon, Kerberos, 534
- /usr/lib/krb5/ktkt\_warnd, démon, Kerberos, 534
- /usr/lib/libsas1.so, bibliothèque,
  - Présentation, 309
- /usr/sbin/gkadmin, commande, Description, 533
- /usr/sbin/gsscred, commande, Description, 533
- /usr/sbin/in.ftpd, démon, Kerberos, 534
- /usr/sbin/in.rlogind, démon, Kerberos, 534
- /usr/sbin/in.rshd, démon, Kerberos, 534
- /usr/sbin/in.telnetd, démon, Kerberos, 534
- /usr/sbin/kadmin, commande, Description, 533
- /usr/sbin/kadmin.local, commande,
  - Description, 533
- /usr/sbin/kclient, commande, Description, 533
- /usr/sbin/kdb5\_ldap\_util, commande,
  - Description, 533
- /usr/sbin/kdb5\_util, commande, Description, 533

/usr/sbin/kgcmgr, commande, Description, 534  
/usr/sbin/kproplog, commande, Description, 534

## Utilisateur

- Affichage de l'état de connexion, 61–62
- Allocation de périphériques, 91–92
- Attribution d'autorisation d'allocation, 87
- Attribution des valeurs par défaut RBAC, 222–223
- Audit de toutes ses commandes, 631–633
- Calcul de synthèse de fichiers, 247–248
- Calcul du code MAC de fichiers, 248–250
- Démontage de périphériques alloués, 94
- Dépannage de l'exécution des commandes privilégiées, 207–208
- Désactivation de la connexion, 63
- Détermination des commandes privilégiées détenues, 207–208
- Détermination des privilèges attribués directement, 206–207
- Génération d'une clé symétrique, 243–247
- Jeu de privilèges de base, 163
- Libération de périphériques, 93–94
- Montage de périphériques alloués, 92–93
- Privilège héritable initial, 163

Utilisateur, procédure, Protection de fichier, 132–133

Utilisateur root, Transformation en rôle root, 203

## Utilisateurs

- Affectation de privilèges, 197
- Affectation de profils de droits, 197
- Attribution de plusieurs rôles, 196
- Audit de chaque utilisateur, 588–589
- Authentification pour le profil de droits, 201
- Authentification pour un rôle, 201–202
- Chiffrement de fichiers, 250–253
- Création
  - root, utilisateur, 202–204
- Création d'un profil de droits pour un groupe, 589–590
- Exceptions aux valeurs par défaut Secure Shell, 321–322
- Modification des propriétés (RBAC), 196–197
- Modification du masque de présélection d'audit, 586–590
- Restriction des privilèges de base, 187
- Sans mot de passe, 62

## Utilisateurs (*Suite*)

- Suppression des indicateurs d'audit, 589

- Utilisation du profil de droits, 201

## Utilisation

- allocate, commande, 91–92
- Allocation de périphériques, 91–92
- Autorisation de fichier, 132–141
- BART, 106
- cryptoadm, commande, 254
- dd, commande, 240–242
- deallocate, commande, 94
- digest, commande, 247–248
- encrypt, commande, 250–253
- Liste des tâches de la configuration RBAC par défaut, 170
- Liste des tâches de Secure Shell, 322–323
- Liste des tâches des privilèges, 204
- Liste des tâches RBAC, 169–170
- mac, commande, 248–250
- Nouvel algorithme de mot de passe, 67
- pktool, commande, 243–247
- ppriv, commande, 210
- rolemod, commande, 195
- ssh-add, commande, 327–328
- ssh-agent, démon, 327–328
- Structure cryptographique, liste des tâches, 239
- truss, commande, 211
- umount, commande, 94
- usermod, commande, 197
- Valeurs par défaut du RBAC, 170–177
- Utilisation de la commande, pktool, 278–282
- Utilisation de la structure de gestion des clés (liste des tâches), 272–273
- Utilitaire de gestion des services
  - Actualisation de la structure cryptographique, 259
  - Redémarrage de la structure cryptographique, 267–268
- Utilitaire de gestion des services (SMF), Voir SMF

## V

- v1, protocole, Secure Shell, 313
- v, option
  - digest, commande, 247



- v, option (*Suite*)
    - mac, commande, 249
    - ppriv, commande, 210
  - v2, protocole, Secure Shell, 313
  - Valeur de champ ipc (jeton ipc), 659–660
  - Valeur par défaut, A l'échelle du système dans le fichier
    - policy.conf, 40
  - Valeurs par défaut
    - Paramètres de privilèges dans le fichier
      - policy.conf, 226
    - Service d'audit, 643–644
  - /var/adm/auditlog, fichier, Enregistrements d'audit
    - au format texte, 605
  - /var/adm/loginlog, fichier, Enregistrement des
    - tentatives de connexion ayant échoué, 63–64
  - /var/adm/messages, fichier
    - Dépannage de l'audit, 629
    - Message de pile exécutable, 132
  - /var/adm/sulog, fichier, Contrôle du contenu, 69
  - /var/krb5/.k5.REALM, fichier, Description, 532
  - /var/krb5/kadmin.log, fichier, Description, 532
  - /var/krb5/kdc.log, fichier, Description, 532
  - /var/krb5/principal, fichier, Description, 532
  - /var/krb5/principal.kadm5, fichier,
    - Description, 532
  - /var/krb5/principal.kadm5.lock, fichier,
    - Description, 532
  - /var/krb5/principal.ok, fichier, Description, 532
  - /var/krb5/principal.ulong, fichier, Description, 532
  - /var/krb5/slave\_datatrans, fichier,
    - Description, 532
  - /var/krb5/slave\_datatrans\_slave, fichier,
    - Description, 532
  - /var/log/authlog, fichier, Connexion ayant
    - échoué, 64–66
  - /var/log/syslog, fichier, Dépannage de l'audit, 629
  - Variable
    - Ajout à l'enregistrement d'audit, 574, 657–658
    - Audit des variables associées à une commande, 657
    - Définition dans Secure Shell, 341
    - KEYBOARD\_ABORT, 72–73
    - login et Secure Shell, 341–342
    - noexec\_user\_stack\_log, 132
    - rstchown, 135
  - Variable (*Suite*)
    - Serveur et port proxy, 331
  - Variable d'environnement
    - Voir aussi* Variable
    - Jeton d'audit, 657–658
    - PATH, 47
    - Présence dans les enregistrements d'audit, 574, 654
    - Redéfinition des serveurs et des ports proxy, 331
    - Secure Shell, 341–342
    - Utilisation avec la commande ssh-agent, 345
  - Variable d'environnement PATH, Définition, 47
  - Variable système
    - Voir aussi* Variable
    - CRYPT\_DEFAULT, 66
    - KEYBOARD\_ABORT, 72–73
    - SYSLOG\_FAILED\_LOGINS, 64
  - Variables, noexec\_user\_stack, 131
  - Variables système, noexec\_user\_stack, 141
  - Vérificateur
    - Description, 290
    - Fenêtre, 290
    - Renvoi au client NFS, 291
  - Vérificateur de fenêtre, 290
  - Vérification, Exécution de l'audit, 627–629
  - Vérification de privilège, Dans les applications, 154
  - VerifyReverseMapping, mot-clé, Fichier
    - ssh\_config, 340
  - Virus
    - Attaque par déni de service, 49
    - Cheval de Troie, 47
  - vnode, jeton d'audit, Format, 656
- W**
- warn.conf, fichier, Description, 532
  - wr, modificateur d'événement d'audit, 659
- X**
- X, option, Commandes utilisant Kerberos, 526
  - X Window System, Et outil SEAM, 477
  - X11DisplayOffset, mot-clé, Fichier sshd\_config, 340
  - X11Forwarding, mot-clé, Fichier sshd\_config, 340

X11UseLocalHost, mot-clé, Fichier sshd\_config, 340  
-x, option, Commandes utilisant Kerberos, 526  
xauth, commande, Transmission X11, 340  
XAuthLocation, mot-clé, Transmission de port Secure  
Shell, 340  
xcclient, jeton d'audit, 664

## **Z**

### Zone

- Audit, 564–565
- Périphérique, 44
- perzone, stratégie d'audit, 564–565
- Planification de l'audit, 568–569
- Services cryptographiques, 267–268
- zonename, stratégie d'audit, 569
- zone.max-locked-memory, contrôle de ressources, 162
- zonename, jeton d'audit, 664
- zonename, stratégie d'audit
  - Description, 576
  - Utilisation, 569, 647

### Zones

- Audit, 647
- Configuration de l'audit dans la zone globale, 591
- perzone, stratégie d'audit, 569, 647
- Structure cryptographique, 237
- zonename, stratégie d'audit, 647