Dernière mise-à-jour : 2020/01/30 03:28

SO216 - Gestion de la sécurité

Surveillance Sécuritaire

La commande who

La commande **who** indique qui est connecté au système :

```
# who
root       console      mars 19 11:43   (:0)
root       pts/3        mars 19 13:18   (:0.0)
```

La commande whodo

La commande **whodo** indique qui fait quoi sur le système à l'instant **t**. L'information provient des fichiers **/var/adm/utmpx** et **/proc/<pid>** :

```
# whodo
jeudi 19 mars 2009 17 h 20 CET
unknown

console      root     11:43
      ?           800    0:00 Xsession
    pts/2         875    0:00 sdt_shell
    pts/2         893    0:00 sh
    pts/2         905    0:00 Xsession2.jds
    pts/2         907    0:04 gnome-session
    pts/2         930    0:22 xscreensaver
```

```
    pts/2          928    0:00 gnome-keyring-d
    pts/2          925    1:43 gconfd-2
      ?            876    0:04 dsdm
      ?           1022   17:54 java

pts/3        root     13:18
      ?           1162    1:25 gnome-terminal
    pts/3         1165    0:00 sh
    pts/3         2689    0:00 whodo
      ?           1163    0:00 gnome-pty-helpe
      ?           1117    0:00 run-mozilla.sh
      ?           1123   11:39 firefox-bin
      ?           1102    0:00 firefox
```

La commande last

Cette commande indique les dates et heures des dernières connexions des utilisateurs lues à partir du fichier binaire **/var/adm/wtmpx** :

```
# last
root      pts/3        :0.0            Thu Mar 19 13:18   encore connecté
root      pts/3        :0.0            Thu Mar 19 11:44 - 11:47  (00:02)
root      console      :0              Thu Mar 19 11:43   encore connecté
reboot    system boot                  Thu Mar 19 11:41
reboot    system down                  Wed Mar 18 00:17
root      pts/3        :0.0            Tue Mar 17 18:57 - arrêté  (1+16:44
root      pts/4        :0.0            Tue Mar 17 17:47 - arrêté  (1+17:54
root      pts/3        :0.0            Tue Mar 17 15:23 - 17:50  (02:26)
root      console      :0              Tue Mar 17 09:25 - arrêté  (2+02:16
reboot    system boot                  Tue Mar 17 09:23
reboot    system down                  Fri Mar  6 16:06
root      console      :0              Fri Mar  6 15:54 - arrêté  (10+17:2
reboot    system boot                  Fri Mar  6 15:51
reboot    system down                  Sat Feb 28 13:49
```

```
root     pts/3        :0.0             Sat Feb 28 13:29 - 13:49  (00:19)
root     pts/3        :0.0             Sat Feb 28 13:13 - 13:29  (00:15)
root     console      :0               Sat Feb 28 13:05 - arrêté  (6+02:46
reboot   system boot                   Sat Feb 28 13:03
reboot   system down                   Sat Feb 28 13:01
reboot   system boot                   Sat Feb 28 12:05
reboot   system down                   Sat Feb 28 11:58
root     console      :0               Sat Feb 28 11:51 - arrêté   (00:13)
reboot   system boot                   Sat Feb 28 11:36
```

Consultez les manuels de ces trois commandes afin de vous familiariser avec les options disponibles.

Types de Sécurité

Les différentes approches à la sécurité sont les suivantes :

Type de Sécurité	**Nom**	**Description**
DAC	*Discretional Access Control*	L'accès aux objets est en fonction de l'identité (utilisateur,groupe). Un utilisateur peut rendre accessible aux autres ses propres objets.
MAC	*Mandatory Access Control*	L'accès aux objets est en fonction de la classification de l'objet (Très secret, Secret, Confidentiel, Public). L'administrateur définit la politique de sécurité et les utilisateurs s'y conforment.
RBAC	*Role Based Access Control*	Un utilisateur a un ou plusieurs rôles. Les droits sont attribués aux rôles.
TE	*Type enforcement*	Chaque objet a une étiquette appelé *type* pour un fichier et *domaine* pour un processus. La politique de sécurité définit l'interaction entre les types et les domaines.
MLS	*Multi-Level Security*	Les politiques de sécurité imposent que qu'un sujet doit dominer un objet pour pouvoir le lire tandis que l'objet doit dominer le sujet pour que ce dernier puisse y écrire.

Dans sa conception de base, Unix utilise une approche sécurité de type **DAC**. Cette approche est maintenue dans Solaris, complimentée par la mise en

place et l'utilisation du **RBAC**.

PAM

pam.conf

PAM (*Pluggable Authentification Modules* ou Modules d'Authentification Enfichables) est une architecture modulaire permettant à l'administrateur système de définir une politique d'authentification pour les logiciels prenant en charge PAM.

Le fichier de configuration est **/etc/pam.conf** :

```
# cat /etc/pam.conf
#
#ident  "@(#)pam.conf   1.31    07/12/07 SMI"
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# PAM configuration
#
# Unless explicitly defined, all services use the modules
# defined in the "other" section.
#
# Modules are defined with relative pathnames, i.e., they are
# relative to /usr/lib/security/$ISA. Absolute path names, as
# present in this file in previous releases are still acceptable.
#
# Authentication management
#
# login service (explicit because of pam_dial_auth)
#
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
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient         pam_rhosts_auth.so.1
rlogin  auth requisite          pam_authtok_get.so.1
rlogin  auth required           pam_dhkeys.so.1
rlogin  auth required           pam_unix_cred.so.1
rlogin  auth required           pam_unix_auth.so.1
#
# Kerberized rlogin service
#
krlogin auth required           pam_unix_cred.so.1
krlogin auth required           pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient         pam_rhosts_auth.so.1
rsh     auth required           pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh    auth required           pam_unix_cred.so.1
krsh    auth required           pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet auth required           pam_unix_cred.so.1
ktelnet auth required           pam_krb5.so.1
#
```

```
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite          pam_authtok_get.so.1
ppp     auth required           pam_dhkeys.so.1
ppp     auth required           pam_unix_cred.so.1
ppp     auth required           pam_unix_auth.so.1
ppp     auth required           pam_dial_auth.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite          pam_authtok_get.so.1
other   auth required           pam_dhkeys.so.1
other   auth required           pam_unix_cred.so.1
other   auth required           pam_unix_auth.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd  auth required           pam_passwd_auth.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron    account required        pam_unix_account.so.1
#
# 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_unix_account.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session management
#
other   session required        pam_unix_session.so.1
```

```
#
# 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 required       pam_authtok_store.so.1
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
#
```

Le contenu de ce fichier fait appel à des modules qui se trouvent dans le répertoire **/usr/lib/security** :

```
# ls /usr/lib/security
64                          pam_deny.so                 pam_sample.so.1
amd64                       pam_deny.so.1               pam_smartcard.so
audit_binfile.so            pam_dhkeys.so               pam_smartcard.so.1
audit_binfile.so.1          pam_dhkeys.so.1             pam_tsol_account.so
audit_syslog.so             pam_dial_auth.so            pam_tsol_account.so.1
audit_syslog.so.1           pam_dial_auth.so.1          pam_unix_account.so
crypt_bsdbf.so              pam_krb5_migrate.so         pam_unix_account.so.1
crypt_bsdbf.so.1            pam_krb5_migrate.so.1       pam_unix_auth.so
crypt_bsdmd5.so             pam_krb5.so                 pam_unix_auth.so.1
crypt_bsdmd5.so.1           pam_krb5.so.1               pam_unix_cred.so
crypt_sunmd5.so             pam_ldap.so                 pam_unix_cred.so.1
crypt_sunmd5.so.1           pam_ldap.so.1               pam_unix_session.so
kmf_nss.so.1                pam_passwd_auth.so          pam_unix_session.so.1
kmf_openssl.so.1            pam_passwd_auth.so.1        pam_winbind.so
kmf_pkcs11.so.1             pam_projects.so             pam_winbind.so.1
pam_authtok_check.so        pam_projects.so.1           pkcs11_kernel.so
pam_authtok_check.so.1      pam_rhosts_auth.so          pkcs11_kernel.so.1
pam_authtok_get.so          pam_rhosts_auth.so.1        pkcs11_softtoken_extra.so
```

```
pam_authtok_get.so.1         pam_roles.so                pkcs11_softtoken_extra.so.1
pam_authtok_store.so         pam_roles.so.1              pkcs11_softtoken.so
pam_authtok_store.so.1       pam_sample.so               pkcs11_softtoken.so.1
```

Chaque section dans /etc/pam.conf contient les règles PAM utilisées pour le service indiqué. Par exemple :

```
#
# PPP service (explicit because of pam_dial_auth)
#
ppp     auth requisite          pam_authtok_get.so.1
ppp     auth required           pam_dhkeys.so.1
ppp     auth required           pam_unix_cred.so.1
ppp     auth required           pam_unix_auth.so.1
ppp     auth required           pam_dial_auth.so.1
```

Tout autre service non-indiqué utilise la section **other** :

```
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other   auth requisite          pam_authtok_get.so.1
other   auth required           pam_dhkeys.so.1
other   auth required           pam_unix_cred.so.1
other   auth required           pam_unix_auth.so.1
```

Chaque ligne comporte cinq champs séparés par un espace dont les quatre premiers champs sont obligatoires.

Le **premier champs** est le nom du service.

Le **deuxième champs** est le **type de règle**. Il en existe quatre :

Type	**Description**
auth	Utilisé pour authentifier un utilisateur ou les pré-requis système

Type	Description
account	Utilisé pour vérifier si l'utilisateur peut s'authentifier
password	Utilisé pour vérifier si l'utilisateur dispose des droits pour mettre le mécanisme d'authentification à jour
session	Utilisé pour gérer la session après l'authentification

Le **troisème champs** est le ***Control-flag***. Il en existe quatre :

Control-flag	Description
required	La réussite de ce module est indispensable. L'échec d'un module *required* n'est communiqué à l'application qu'après la vérification de tous les modules ayant un *control-flag* de **required**
requisite	La réussite de ce module est indispensable. L'échec d'un module *requisite* est immédiatement communiqué à l'application
sufficient	La réussite de ce module est suffisant pour authoriser l'authentification. Si aucun test *required* précédent est en échec, la vérification s'arrête. Si un test *required* précédent était en échec, le test *sufficient* est ignoré. L'échec d'un test *sufficient* n'a pas de conséquence si tous les tests *required* réussissent.
optional	La réussite ou l'échec de ce module est sans importance, **sauf** s'il s'agit du seul module à exécuter

Le **quatrième champs** stipule le **module** associé à la règle. Sans chemin absolu, le fichier est supposé être dans le répertoire **/usr/lib/security**. Pour inclure un module en dehors de ce répertoire il convient donc de stipuler son chemin absolu.

Le **cinquième champs** contient des options éventuelles.

Par exemple, considérez la section **rlogin** :

```
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin  auth sufficient         pam_rhosts_auth.so.1
rlogin  auth requisite          pam_authtok_get.so.1
rlogin  auth required           pam_dhkeys.so.1
rlogin  auth required           pam_unix_cred.so.1
rlogin  auth required           pam_unix_auth.so.1
```

Dans cette section, si la règle **sufficient** réussit, les modules suivants ne sont pas invoqués.

Modules

Certains modules de PAM peuvent être configurés grâce aux options. Le format de l'appel du module est :

/usr/lib/security/pam_<nom du service>_<nom du module>.so.x <options>

Les options sont détaillées dans le manuel de chaque module. Par exemple pour pam_rhosts_auth.so.1 :

```
# man pam_rhosts_auth
Mise en page en cours.  Veuillez patienter... terminé

Standards, Environments, and Macros            pam_rhosts_auth(5)

NAME
     pam_rhosts_auth - authentication management PAM module using
     ruserok()

SYNOPSIS
     /usr/lib/security/pam_rhosts_auth.so.1

DESCRIPTION
     The             rhosts             PAM             module,
     /usr/lib/security/pam_rhosts_auth.so.1, authenticates a user
     via    the    rlogin    authentication    protocol.     Only
     pam_sm_authenticate()  is  implemented  within  this module.
     pam_sm_authenticate()  uses  the  ruserok(3SOCKET)   library
     function   to   authenticate   the   rlogin   or  rsh  user.
     pam_sm_setcred() is a null function.

     /usr/lib/security/pam_rhosts_auth.so.1  is  designed  to  be
     stacked   on   top   of   the  /usr/lib/security/pam_unix.so.1
     module for both the rlogin and rsh services. This module  is
     normally configured as sufficient so that subsequent authen-
     tication    is    performed    only    on     failure     of
```

```
     pam_sm_authenticate(). The following option may be passed in
     to this service module:

     debug           syslog(3C)    debugging    information    at
                     LOG_DEBUG level.

ATTRIBUTES
     See attributes(5) for descriptions of the  following  attri-
     butes:


    _____________________________________________________________
    |       ATTRIBUTE TYPE        |       ATTRIBUTE VALUE       |
    | MT Level                    | MT-Safe with exceptions      |
    |_____________________________|______________________________|

SEE ALSO
     pam(3PAM),     pam_authenticate(3PAM),     ruserok(3SOCKET),
     syslog(3C), libpam(3LIB), pam.conf(4), attributes(5)

NOTES
     The interfaces in  libpam() are MT-Safe only if each  thread
     within the multi-threaded application uses its own  PAM han-
     dle.

SunOS 5.10          Last change: 28 Oct 1996                  1
```

Ce manuel indique l'utilisation de l'option **debug**.

Passez en revue les manuels des autres modules PAM appelés par le fichier pam.conf.

RBAC

Si ce n'est pas déjà fait, créez deux utilisateurs **user1** et **user2**.

Le service **RBAC** (**R**ole **B**ased **A**ccess **C**ontrol) permet à un utilisateur autorisé à exécuter une commande en tant que **root**.

L'implémentation est basée sur des **autorisations** ou ***authorisations***.

Des autorisations et des commandes sont regroupés dans des **profils** ou ***rights***.

Un **rôle** est un pseudo-compte que l'utilisateur peut atteindre via la commande su.

Les autorisations sont définies dans le fichier **/etc/security/auth_attr** :

```
# cat /etc/security/auth_attr
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/security/auth_attr
#
# execution attributes for profiles. see auth_attr(4)
#
#ident  "@(#)auth_attr  1.1     07/01/31 SMI"
#
#
:::::
solaris.:::All Solaris Authorizations::help=AllSolAuthsHeader.html
solaris.admin.dcmgr.:::OS Server Manager::help=AuthDcmgrHeader.html
solaris.admin.dcmgr.admin:::Manage OS Services and Patches::help=AuthDcmgrAdmin.html
solaris.admin.dcmgr.clients:::Manage Diskless Clients::help=AuthDcmgrClients.html
solaris.admin.dcmgr.read:::View OS Services, Patches and Diskless Clients::help=AuthDcmgrRead.html
```

```
solaris.admin.diskmgr.:::Disk Manager::help=AuthDiskmgrHeader.html
solaris.admin.diskmgr.read:::View Disks::help=AuthDiskmgrRead.html
solaris.admin.diskmgr.write:::Manage Disks::help=AuthDiskmgrWrite.html
solaris.admin.fsmgr.:::Mounts and Shares::help=AuthFsmgrHeader.html
solaris.admin.fsmgr.read:::View Mounts and Shares::help=AuthFsmgrRead.html
solaris.admin.fsmgr.write:::Mount and Share Files::help=AuthFsmgrWrite.html
solaris.admin.logsvc.:::Log Viewer::help=AuthLogsvcHeader.html
solaris.admin.logsvc.purge:::Remove Log Files::help=AuthLogsvcPurge.html
solaris.admin.logsvc.read:::View Log Files::help=AuthLogsvcRead.html
solaris.admin.logsvc.write:::Manage Log Settings::help=AuthLogsvcWrite.html
solaris.admin.patchmgr.:::Patch Manager::
solaris.admin.patchmgr.read:::View Patches::help=AuthPatchmgrRead.html
solaris.admin.patchmgr.write:::Add and Remove Patches::help=AuthPatchmgrWrite.html
solaris.admin.printer.:::Printer Information::help=AuthPrinterHeader.html
solaris.admin.printer.delete:::Delete Printer Information::help=AuthPrinterDelete.html
solaris.admin.printer.modify:::Update Printer Information::help=AuthPrinterModify.html
solaris.admin.printer.read:::View Printer Information::help=AuthPrinterRead.html
solaris.admin.privilege.:::Privileges::help=AuthPrivilegeHeader.html
solaris.admin.privilege.write:::Manage Privileges::help=AuthPrivilegeWrite.html
solaris.admin.procmgr.:::Process Manager::help=AuthProcmgrHeader.html
solaris.admin.procmgr.admin:::Manage All Processes::help=AuthProcmgrAdmin.html
solaris.admin.procmgr.user:::Manage Owned Processes::help=AuthProcmgrUser.html
solaris.admin.serialmgr.:::Serial Port Manager::help=AuthSerialmgrHeader.html
solaris.admin.serialmgr.delete:::Delete Serial Ports::help=AuthSerialmgrDelete.html
solaris.admin.serialmgr.modify:::Manage Serial Ports::help=AuthSerialmgrModify.html
solaris.admin.serialmgr.read:::View Serial Ports::help=AuthSerialmgrRead.html
solaris.admin.usermgr.:::User Accounts::help=AuthUsermgrHeader.html
solaris.admin.usermgr.audit:::Audit Controls::help=AuthUserMgrAudit.html
solaris.admin.usermgr.labels:::Label and Clearance Range::help=AuthUserMgrLabels.html
solaris.admin.usermgr.pswd:::Change Password::help=AuthUserMgrPswd.html
solaris.admin.usermgr.read:::View Users and Roles::help=AuthUsermgrRead.html
solaris.admin.usermgr.write:::Manage Users::help=AuthUsermgrWrite.html
solaris.admin.volmgr.:::Logical Volume Manager::
solaris.admin.volmgr.read:::View Logical Volumes::help=AuthVolmgrRead.html
```

```
solaris.admin.volmgr.write:::Manage Logical Volumes::help=AuthVolmgrWrite.html
solaris.audit.:::Audit Management::help=AuditHeader.html
solaris.audit.config:::Configure Auditing::help=AuditConfig.html
solaris.audit.read:::Read Audit Trail::help=AuditRead.html
solaris.compsys.:::Computer System Information::help=AuthCompSysHeader.html
solaris.compsys.read:::View Computer System Information::help=AuthCompSysRead.html
solaris.compsys.write:::Manage Computer System Information::help=AuthCompSysWrite.html
solaris.device.:::Device Allocation::help=DevAllocHeader.html
solaris.device.allocate:::Allocate Device::help=DevAllocate.html
solaris.device.cdrw:::CD-R/RW Recording Authorizations::help=DevCDRW.html
solaris.device.config:::Configure Device Attributes::help=DevConfig.html
solaris.device.grant:::Delegate Device Administration::help=DevGrant.html
solaris.device.revoke:::Revoke or Reclaim Device::help=DevRevoke.html
solaris.dhcpmgr.:::DHCP Service Management::help=DhcpmgrHeader.html
solaris.dhcpmgr.write:::Modify DHCP Service Configuration::help=DhcpmgrWrite.html
solaris.file.:::File Operations::help=FileHeader.html
solaris.file.chown:::Change File Owner::help=FileChown.html
solaris.file.owner:::Act as File Owner::help=FileOwner.html
solaris.grant:::Grant All Solaris Authorizations::help=PriAdmin.html
solaris.jobs.:::Job Scheduler::help=JobHeader.html
solaris.jobs.admin:::Manage All Jobs::help=AuthJobsAdmin.html
solaris.jobs.grant:::Delegate Cron & At Administration::help=JobsGrant.html
solaris.jobs.user:::Manage Owned Jobs::help=AuthJobsUser.html
solaris.label.:::Label Management::help=LabelHeader.html
solaris.label.file.downgrade:::Downgrade File Label::help=LabelFileDowngrade.html
solaris.label.file.upgrade:::Upgrade File Label::help=LabelFileUpgrade.html
solaris.label.print:::View Printer Queue at All Labels::help=LabelPrint.html
solaris.label.range:::Set Label Outside User Accred Range::help=LabelRange.html
solaris.label.win.downgrade:::Downgrade DragNDrop or CutPaste Info::help=LabelWinDowngrade.html
solaris.label.win.noview:::DragNDrop or CutPaste without viewing contents::help=LabelWinNoView.html
solaris.label.win.upgrade:::Upgrade DragNDrop or CutPaste Info::help=LabelWinUpgrade.html
solaris.login.:::Login Control::help=LoginHeader.html
solaris.login.enable:::Enable Logins::help=LoginEnable.html
solaris.login.remote:::Remote Login::help=LoginRemote.html
```

```
solaris.mail.:::Mail::help=MailHeader.html
solaris.mail.mailq:::Mail Queue::help=MailQueue.html
solaris.network.hosts.:::Computers and Networks::help=NetworkHostsHeader.html
solaris.network.hosts.read:::View Computers and Networks::help=NetworkHostsRead.html
solaris.network.hosts.write:::Manage Computers and Networks::help=NetworkHostsWrite.html
solaris.print.:::Printer Management::help=PrintHeader.html
solaris.print.admin:::Administer Printer::help=PrintAdmin.html
solaris.print.cancel:::Cancel Print Job::help=PrintCancel.html
solaris.print.list:::List Jobs in Printer Queue::help=PrintList.html
solaris.print.nobanner:::Print without Banner::help=PrintNoBanner.html
solaris.print.ps:::Print Postscript::help=PrintPs.html
solaris.print.unlabeled:::Print without Label::help=PrintUnlabeled.html
solaris.profmgr.:::Rights::help=ProfmgrHeader.html
solaris.profmgr.assign:::Assign All Rights::help=AuthProfmgrAssign.html
solaris.profmgr.delegate:::Assign Owned Rights::help=AuthProfmgrDelegate.html
solaris.profmgr.execattr.write:::Manage Commands::help=AuthProfmgrExecattrWrite.html
solaris.profmgr.read:::View Rights::help=AuthProfmgrRead.html
solaris.profmgr.write:::Manage Rights::help=AuthProfmgrWrite.html
solaris.project.:::Solaris Projects::
solaris.project.read:::View Projects::help=AuthProjmgrRead.html
solaris.project.write:::Manage Projects::help=AuthProjmgrWrite.html
solaris.role.:::Roles::help=RoleHeader.html
solaris.role.assign:::Assign All Roles::help=AuthRoleAssign.html
solaris.role.delegate:::Assign Owned Roles::help=AuthRoleDelegate.html
solaris.role.write:::Manage Roles::help=AuthRoleWrite.html
solaris.smf.:::SMF Management::help=SmfHeader.html
solaris.smf.manage.:::Manage All SMF Service States::help=SmfManageHeader.html
solaris.smf.manage.autofs:::Manage Automount Service States::help=SmfAutofsStates.html
solaris.smf.manage.bind:::Manage DNS Service States::help=BindStates.html
solaris.smf.manage.cde.:::Manage CDE Service States::help=ManageCDEHeader.html
solaris.smf.manage.cde.calendar:::Manage Calendar Service States::help=ManageCDECalendar.html
solaris.smf.manage.cde.printinfo:::Manage Printinfo Service States::help=ManageCDEPrintinfo.html
solaris.smf.manage.cde.spc:::Manage Spc Service States::help=ManageCDESpc.html
solaris.smf.manage.cde.tooltalk:::Manage Tooltalk Service States::help=ManageCDETooltalk.html
```

```
solaris.smf.manage.cron:::Manage Cron Service States::help=SmfCronStates.html
solaris.smf.manage.dt.:::Manage Desktop Service States::help=ManageDtHeader.html
solaris.smf.manage.dt.login:::Manage Desktop Login Service States::help=ManageDtLogin.html
solaris.smf.manage.font:::Manage Font Service States::
solaris.smf.manage.inetd:::Manage inetd and inetd managed services States::help=SmfIntedStates.html
solaris.smf.manage.labels:::Manage label server::help=LabelServer.html
solaris.smf.manage.name-service-cache:::Manage Name Service Cache Daemon Service States::help=SmfNscdStates.html
solaris.smf.manage.postgres:::Manage Postgres service states::
solaris.smf.manage.power:::Manage Power Management Service States::help=SmfPowerStates.html
solaris.smf.manage.routing:::Manage Routing Service States::help=SmfRoutingStates.html
solaris.smf.manage.rpc.bind:::Manage RPC Program number mapper::help=SmfRPCBind.html
solaris.smf.manage.sendmail:::Manage Sendmail Service States::help=SmfSendmailStates.html
solaris.smf.manage.servicetags:::Manage Service Tags Service States::help=StStates.html
solaris.smf.manage.ssh:::Manage Secure Shell Service States::help=SmfSshStates.html
solaris.smf.manage.system-log:::Manage Syslog Service States::help=SmfSyslogStates.html
solaris.smf.manage.tnctl:::Manage Refresh of Trusted Network Parameters::help=TNctl.html
solaris.smf.manage.tnd:::Manage Trusted Network Daemon::help=TNDaemon.html
solaris.smf.manage.x11:::Manage X11 Service States::
solaris.smf.modify.:::Modify All SMF Service Properties::help=SmfModifyHeader.html
solaris.smf.modify.application:::Modify Application Type Properties::help=SmfModifyAppl.html
solaris.smf.modify.dependency:::Modify Service Dependencies::help=SmfModifyDepend.html
solaris.smf.modify.framework:::Modify Framework Type Properties::help=SmfModifyFramework.html
solaris.smf.modify.method:::Modify Service Methods::help=SmfModifyMethod.html
solaris.smf.value.:::Change Values of SMF Service Properties::help=SmfValueHeader.html
solaris.smf.value.cde.:::Change CDE Service Property Values::help=ValueCDEHeader.html
solaris.smf.value.cde.calendar:::Change Calendar Service Property Values::help=ValueCDECalendar.html
solaris.smf.value.cde.login:::Change dtlogin Service Property Values::help=ValueCDELogin.html
solaris.smf.value.cde.printinfo:::Change Printinfo Service Property Values::help=ValueCDEPrintinfo.html
solaris.smf.value.cde.spc:::Change Spc Service Property Values::help=ValueCDESpc.html
solaris.smf.value.cde.tooltalk:::Change Tooltalk Service Property Values::help=ValueCDETooltalk.html
solaris.smf.value.inetd:::Change values of SMF Inetd configuration paramaters::help=SmfValueInted.html
solaris.smf.value.postgres:::Change Postgres value properties::
solaris.smf.value.routing:::Change Values of SMF Routing Properties::help=SmfValueRouting.html
solaris.smf.value.servicetags:::Change Service Tag Service Property Values::help=StValue.html
```

```
solaris.smf.value.tnd:::Change Trusted Network Daemon Service Property Values::help=ValueTND.html
solaris.snmp.:::SNMP Management::help=AuthSnmpHeader.html
solaris.snmp.read:::Get SNMP Information::help=AuthSnmpRead.html
solaris.snmp.write:::Set SNMP Information::help=AuthSnmpWrite.html
solaris.system.:::Machine Administration::help=SysHeader.html
solaris.system.date:::Set Date & Time::help=SysDate.html
solaris.system.shutdown:::Shutdown the System::help=SysShutdown.html
```

Chaque ligne est divisée en 7 champs. Seuls le premier, le quatrième et le dernier sont utilisées :

Champs	**Description**
1	Nome de l'attribut
4	Bref description
7	Fichier d'aide

Les fichiers d'aide se trouve dans le répertoire **/usr/lib/help/auths/locale/C** :

```
# ls /usr/lib/help/auths/locale/C
AllSolAuthsHeader.html         AuthProfmgrDelegate.html       JobHeader.html                 RoleHeader.html
AuditConfig.html               AuthProfmgrExecattrWrite.html  JobsGrant.html                 SmfAutofsStates.html
AuditHeader.html               AuthProfmgrRead.html           LabelFileDowngrade.html        SmfCronStates.html
AuditRead.html                 AuthProfmgrWrite.html          LabelFileUpgrade.html          SmfHeader.html
AuthCompSysHeader.html         AuthProjmgrRead.html           LabelHeader.html               SmfInetdStates.html
AuthCompSysRead.html           AuthProjmgrWrite.html          LabelPrint.html                SmfManageHeader.html
AuthCompSysWrite.html          AuthRoleAssign.html            LabelRange.html                SmfModifyAppl.html
AuthDcmgrAdmin.html            AuthRoleDelegate.html          LabelServer.html               SmfModifyDepend.html
AuthDcmgrClients.html          AuthRoleWrite.html             LabelWinDowngrade.html
SmfModifyFramework.html
AuthDcmgrHeader.html           AuthSerialmgrDelete.html       LabelWinNoView.html            SmfModifyHeader.html
AuthDcmgrRead.html             AuthSerialmgrHeader.html       LabelWinUpgrade.html           SmfModifyMethod.html
AuthDiskmgrHeader.html         AuthSerialmgrModify.html       LoginEnable.html               SmfNscdStates.html
AuthDiskmgrRead.html           AuthSerialmgrRead.html         LoginHeader.html               SmfPowerStates.html
AuthDiskmgrWrite.html          AuthSnmpHeader.html            LoginRemote.html
SmfRoutingStates.html
```

```
AuthFsmgrHeader.html          AuthSnmpRead.html             MailHeader.html
SmfSendmailStates.html
AuthFsmgrRead.html            AuthSnmpWrite.html            MailQueue.html                SmfSshStates.html
AuthFsmgrWrite.html           AuthUsermgrHeader.html        ManageCDECalendar.html        SmfSyslogStates.html
AuthJobsAdmin.html            AuthUserMgrPswd.html          ManageCDEHeader.html          SmfValueHeader.html
AuthJobsUser.html             AuthUsermgrRead.html          ManageCDEPrintinfo.html       SmfValueInetd.html
AuthLogsvcHeader.html         AuthUsermgrWrite.html         ManageCDESpc.html             SmfValueRouting.html
AuthLogsvcPurge.html          AuthVolmgrRead.html           ManageCDETooltalk.html        SysDate.html
AuthLogsvcRead.html           AuthVolmgrWrite.html          ManageDtHeader.html           SysHeader.html
AuthLogsvcWrite.html          BindStates.html               ManageDtLogin.html            SysShutdown.html
AuthPatchmgrRead.html         DevAllocate.html              NetworkHostsHeader.html       TNctl.html
AuthPatchmgrWrite.html        DevAllocHeader.html           NetworkHostsRead.html         TNDaemon.html
AuthPrinterDelete.html        DevCDRW.html                  NetworkHostsWrite.html
ValueCDECalendar.html
AuthPrinterHeader.html        DevConfig.html                PriAdmin.html                 ValueCDEHeader.html
AuthPrinterModify.html        DevGrant.html                 PrintAdmin.html               ValueCDELogin.html
AuthPrinterRead.html          DevRevoke.html                PrintCancel.html
ValueCDEPrintinfo.html
AuthPrivilegeHeader.html      DhcpmgrHeader.html            PrintHeader.html              ValueCDESpc.html
AuthPrivilegeWrite.html       DhcpmgrWrite.html             PrintList.html
ValueCDETooltalk.html
AuthProcmgrAdmin.html         FileChown.html                PrintNoBanner.html            ValueTND.html
AuthProcmgrHeader.html        FileHeader.html               PrintPs.html                  X11States.html
AuthProcmgrUser.html          FileOwner.html                PrintUnlabeled.html
AuthProfmgrAssign.html        FontStates.html               ProfmgrHeader.html
```

Les profils prédéfinis sont stockés dans le fichier **/etc/security/prof_attr** :

```
# cat /etc/security/prof_attr
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/security/prof_attr
```

```
#
# execution attributes for profiles. see prof_attr(4)
#
#ident  "@(#)prof_attr  1.1     07/01/31 SMI"
#
#
::::
........
User Management:::Manage users, groups, home
directory:auths=solaris.profmgr.read,solaris.admin.usermgr.write,solaris.admin.usermgr.read;help=RtUserMngmnt.htm
l
........
```

Cette ligne, toute comme les autres, contient 5 champs :

Champs	**Description**
1	Nom du profil
2	Inutilisé
3	Inutilisé
4	Brève description
5	Attributs séparés par des points-virgules

Dans notre ligne d'exemple, l'attribut est **auths=...**. Ce qui suit est une liste d'autorisations, telles que celles-ci se trouvent dans le fichier **/etc/security/auth_attr**, séparées par des virgules.

Les profiles majeurs sont :

```
Primary Administrator:::Can perform all administrative tasks:auths=solaris.*,solaris.grant;help=RtPriAdmin.html
```

```
System Administrator:::Can perform most non-security administrative tasks:profiles=Audit Review,Printer
Management,Cron Management,Device Management,File System Management,Mail Management,Maintenance and Repair,Media
Backup,Media Restore,Name Service Management,Network Management,Object Access Management,Process
Management,Software Installation,User Management,Project Management,All;help=RtSysAdmin.html
```

```
Operator:::Can perform simple administrative tasks:profiles=Printer Management,Media
Backup,All;help=RtOperator.html
```

```
Basic Solaris User:::Automatically assigned
rights:auths=solaris.profmgr.read,solaris.jobs.users,solaris.mail.mailq,solaris.admin.usermgr.read,solaris.admin.
logsvc.read,solaris.admin.fsmgr.read,solaris.admin.serialmgr.read,solaris.admin.diskmgr.read,solaris.admin.procmg
r.user,solaris.compsys.read,solaris.admin.printer.read,solaris.admin.prodreg.read,solaris.admin.dcmgr.read,solari
s.snmp.read,solaris.project.read,solaris.admin.patchmgr.read,,solaris.network.hosts.read,solaris.admin.volmgr.rea
d;profiles=All;help=RtDefault.html
```

Le associations de commandes avec les profils sont stockées dans le fichier **/etc/security/exec_attr** :

```
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/security/exec_attr
#
# execution attributes for profiles. see exec_attr(4)
#
#ident  "@(#)exec_attr  1.2     07/03/30 SMI"
#
#
..........
User Management:solaris:cmd:::/usr/sbin/groupadd:uid=0
User Management:solaris:cmd:::/usr/sbin/groupdel:uid=0
User Management:solaris:cmd:::/usr/sbin/groupmod:uid=0
User Management:solaris:cmd:::/usr/sbin/roleadd:euid=0
User Management:solaris:cmd:::/usr/sbin/roledel:euid=0
User Management:solaris:cmd:::/usr/sbin/rolemod:euid=0
User Management:solaris:cmd:::/usr/sbin/useradd:euid=0
User Management:solaris:cmd:::/usr/sbin/userdel:euid=0
User Management:solaris:cmd:::/usr/sbin/usermod:euid=0
User Management:suser:cmd:::/usr/sbin/grpck:euid=0
```

```
User Management:suser:cmd:::/usr/sbin/pwck:euid=0
User Security:solaris:act:::SDTscgui;*;*;*;0:uid=0
User Security:solaris:cmd:::/usr/sbin/passmgmt:uid=0
User Security:suser:cmd:::/usr/bin/passwd:uid=0
User Security:suser:cmd:::/usr/sbin/pwck:euid=0
User Security:suser:cmd:::/usr/sbin/pwconv:euid=0
..........
```

Les attributions des rôles et/ou des autorisations à des utilisateurs se trouvent dans le fichier **/etc/user_attr** :

```
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/user_attr
#
# execution attributes for profiles. see user_attr(4)
#
#ident  "@(#)user_attr  1.1     07/01/31 SMI"
#
#
adm::::profiles=Log Management
lp::::profiles=Printer Management
postgres::::type=role;profiles=Postgres Administration,All
root::::auths=solaris.*,solaris.grant;profiles=Web Console
Management,All;lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

Le fichier **/etc/security/policy.conf** définit les profiles et autorisations attribués à tous les utilisateurs :

```
#
# Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/security/policy.conf
```

```
#
# security policy configuration for user attributes. see policy.conf(4)
#
#ident  "@(#)policy.conf        1.11    04/09/27 SMI"
#
AUTHS_GRANTED=solaris.device.cdrw
PROFS_GRANTED=Basic Solaris User

# 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

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

# The Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
#
# These settings determine the default privileges users have.  If not set,
# the default privileges are taken from the inherited set.
# There are two different settings; PRIV_DEFAULT determines the default
# set on login; PRIV_LIMIT defines the Limit set on login.
# Individual users can have privileges assigned or taken away through
# user_attr.  Privileges can also be assigned to profiles in which case
# the users with those profiles can use those privileges through pfexec(1m).
```

```
# For maximum future compatibility, the specifications should
# always include "basic" or "all"; privileges should then be removed using
# the negation.  E.g., PRIV_LIMIT=all,!sys_linkdir takes away only the
# sys_linkdir privilege, regardless of future additional privileges.
# Similarly, PRIV_DEFAULT=basic,!file_link_any takes away only the
# file_link_any privilege from the basic privilege set; only that notation
# is immune from a future addition of currently unprivileged operations to
# the basic privilege set.
# NOTE: removing privileges from the the Limit set requires EXTREME care
# as any set-uid root program may suddenly fail because it lacks certain
# privilege(s).
#
#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
#
# LOCK_AFTER_RETRIES specifies the default account locking policy for local
# user accounts (passwd(4)/shadow(4)).  The default may be overridden by
# a user's user_attr(4) "lock_after_retries" value.
# YES enables local account locking, NO disables local account locking.
# The default value is NO.
#
#LOCK_AFTER_RETRIES=NO
```

Pour visualiser les roles, profiles et auths attribués à un utilisateur,il convient d'utiliser les commandes **roles**, **profiles** et **auths** :

```
# roles
Pas de rôles
# profiles
Web Console Management
All
Basic Solaris User
# auths
solaris.*
# roles user1
```

```
Pas de rôles
# profiles user1
Basic Solaris User
All
# auths user1
solaris.device.cdrw,solaris.profmgr.read,solaris.jobs.users,solaris.mail.mailq,solaris.admin.usermgr.read,solaris
.admin.logsvc.read,solaris.admin.fsmgr.read,solaris.admin.serialmgr.read,solaris.admin.diskmgr.read,solaris.admin
.procmgr.user,solaris.compsys.read,solaris.admin.printer.read,solaris.admin.prodreg.read,solaris.admin.dcmgr.read
,solaris.snmp.read,solaris.project.read,solaris.admin.patchmgr.read,solaris.network.hosts.read,solaris.admin.volm
gr.read
```

LAB#1 - Créer un rôle

Trois principales commandes sont utilisées pour la gestion de RBAC :

- **roleadd**
  - ajoute un compte rôle sur le système,
- **rolemod**
  - modifie l'information de la connexion d'un rôle,
- **useradd**
  - ajoute un compte utilisateur sur le système

roleadd

La commande roleadd ajoute une entrée aux fichiers **/etc/passwd**, **/etc/shadow** et **/etc/user_attr**. Elle utilise fréquemment les options suivantes :

Option	Description
-c comment	brève description du rôle
-d dir	répertoire local du rôle
-m	créer le répertoire local si c'est nécessaire
-A authorization	affecter des autorisations au rôle

Option	Description
-P profile	affecter des profils au rôle

Vous allez maintenant créer un compte de rôle pour un gestionnaire de sauvegardes. Saisissez donc la commande suivante :

```
#roleadd -m -d /export/home/tarback -c "Gestionnaire de sauvegardes" -P "Media Backup,Media Restore" tarback
[Entrée]
```

Vous obtiendrez un résultat similaire à celui-ci :

```
# roleadd -m -d /export/home/tarback -c "Gestionnaire de sauvegardes" -P "Media Backup,Media Restore" tarback
64 blocs
```

Consultez maintenant les fichiers **/etc/user_attr**, **/etc/passwd** et **/etc/shadow** :

```
# cat /etc/user_attr | grep tarback
tarback::::type=role;profiles=Media Backup,Media Restore
# cat /etc/passwd | grep tarback
tarback:x:103:1:Gestionnaire de sauvegardes:/export/home/tarback:/bin/pfsh
# cat /etc/shadow | grep tarback
tarback:*LK*:::::::
```

Veuillez noter qu'un compte de rôle utilise un shell de profil. **Bash** ne peut **pas** être utilisé en tant que shell pour un compte de rôle.

Les shells des profils sont **pfsh**, **pfcsh**, **pfksh** pour respectivement le Bourne, le C, et le Korn shell.

Un shell de profil est un type de shell spécial qui donne accès aux applications privilégiées qui sont affectées au profil.

La commande ou application privilégiée est exécutée avec les attributs spécifiés dans la base de données par la commande **pfexec**.

Consultez le manuel de la commande pfexec.

Dernièrement, créez un mot de passe pour tarback :

```
# passwd tarback
Nouveau mot de passe :
Entrez de nouveau le mot de passe :
passwd: mot de passe correctement modifié pour tarback
```

rolemod

Les options les plus fréquentes sont :

Option	Description
-e expire	date d'expiration pour un rôle
-l new_logname	nouveau nom de connexion
-s	shell
-A authorization	une ou plusieurs autorisations séparées par une virgule
-P profile	un ou plusieurs profils séparés par une virgule

Par exemple :

```
# rolemod –A auth1,auth2 –P profile1,profile2
```

Cette ligne de commande ajoute les autorisations **auth1** et **auth2** aux profils **profile1** et **profile2**.

useradd

La commande useradd peut être utilisée pour ajouter un nouvel utilisateur avec des autorisations et des profils aux fichiers /etc/passwd, /etc/shadow et /etc/user_attr.

Voici quelques options intéressantes :

Option	Description
-R role	spécifie un ou plusieurs profils d'exécution séparés par une virgule définis dans user_attr
-A authorization	une ou plusieurs autorisations séparées par une virgule
-P profile	un ou plusieurs profils séparés par une virgule

Saisissez la commande suivante pour ajouter l'utilisateur **admin** qui a le droit d'assumer le rôle du de gestionnaire de sauvegardes :

```
# useradd -d /export/home/admin -m -s /bin/ksh -c "Admin" -R tarback admin [Entrée]
```

Vous obtiendrez un résultat similaire à celui-ci :

```
# useradd -d /export/home/admin -m -s /bin/ksh -c "Admin" -R tarback admin
64 blocs
```

Consultez maintenant les fichiers **/etc/user_attr**, **/etc/passwd** et **/etc/shadow** :

```
# cat /etc/user_attr | grep tarback
tarback::::type=role;profiles=Media Backup,Media Restore
admin::::type=normal;roles=tarback
# cat /etc/passwd | grep admin
admin:x:104:1:Admin:/export/home/admin:/bin/ksh
# cat /etc/shadow | grep admin
admin:*LK*:::::::
```

Créez maintenant le mot de passe pour **admin**. Indiquez un mot de passe identique au nom du compte :

```
# passwd admin [Entrée]
```

Devenez maintenant l'utilisateur **admin** :

```
# su - admin [Entrée]
```

Pour visualiser les roles, profiles et auths attribués à admin, il convient d'utiliser les commandes **roles**, **profiles** et **auths** :

```
$ roles
tarback
$ profiles
Basic Solaris User
All
$ auths
solaris.device.cdrw,solaris.profmgr.read,solaris.jobs.users,solaris.mail.mailq,solaris.admin.usermgr.read,solaris
.admin.logsvc.read,solaris.admin.fsmgr.read,solaris.admin.serialmgr.read,solaris.admin.diskmgr.read,solaris.admin
.procmgr.user,solaris.compsys.read,solaris.admin.printer.read,solaris.admin.prodreg.read,solaris.admin.dcmgr.read
,solaris.snmp.read,solaris.project.read,solaris.admin.patchmgr.read,solaris.network.hosts.read,solaris.admin.volm
gr.read
```

En tant qu'admin, assumez le rôle de tarback

```
$ su - tarback [Entrée]
```

Les commandes maintenant utilisables par **admin** *via* le rôle **tarback** peuvent être visualisées dans le fichier **/etc/security/exec_attr** :

```
$ cat /etc/security/exec_attr | grep Backup
Media Backup:solaris:act:::Tar;*;*;*;*:privs=all
Media Backup:solaris:act:::Tar;*;TAR,MAGTAPE;*;>0:privs=all
Media Backup:solaris:act:::TarList;*;*;*;*:
Media Backup:suser:cmd:::/usr/bin/mt:euid=0
Media Backup:suser:cmd:::/usr/lib/fs/ufs/ufsdump:euid=0;gid=sys
Media Backup:suser:cmd:::/usr/sbin/tar:euid=0
$ cat /etc/security/exec_attr | grep Restore
Media Restore:solaris:act:::TarList;*;*;*;*:
Media Restore:solaris:act:::TarUnpack;*;*;*;2:privs=all
Media Restore:solaris:act:::TarUnpack;*;*;*;<2:privs=all
Media Restore:suser:cmd:::/usr/bin/cpio:euid=0
Media Restore:suser:cmd:::/usr/bin/mt:euid=0
Media Restore:suser:cmd:::/usr/lib/fs/ufs/ufsrestore:euid=0
Media Restore:suser:cmd:::/usr/sbin/tar:euid=0
```

Notez que les commandes sont exécutées avec un UID effectif de O.

Quittez le rôle **tarback** ainsi que le compte **admin** :

```
$ exit
$ exit
#
```

LAB#2 - Rôles et Profils

Dans ce LAB vous allez permettre à l'utilisateur **user1** de redémarrer le système. Un utilisateur normal n'a pas de rôles lors de sa création.

Vous allez :

- Créer un rôle,
- Créer le mot de passe pour le rôle,
- Ajouter le rôle aux rôles utilisables par un utilisateur,
- Créer un profil,
- Ajouter le profil au rôle,
- Ajouter une commande au profil,
- Tester votre configuration.

Pour commencer, utilisez la commande **roles** :

```
#roles user1 [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# roles user1
Pas de rôles
```

Assumez l'identité de **user1** et essayez de redémarrer le système :

```
#su - user1 [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# su - user1
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ /usr/sbin/reboot
reboot : autorisation refusée
```

Notez que dans l'état actuel des choses, user1 ne peut pas redémarrer le système. Redevenez root et créer un rôle dénommé **reboot** :

```
# roleadd -m -d /export/home/reboot reboot [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# roleadd -m -d /export/home/reboot reboot
64 blocs
```

Créez maintenant un mot de passe pour reboot. Utilisez un mot de passe identique au nom du rôle :

```
# passwd reboot [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# passwd reboot
Nouveau mot de passe :
Entrez de nouveau le mot de passe :
passwd: mot de passe correctement modifié pour reboot
```

Vérifiez maintenant que le rôle a bien été créé :

```
# grep reboot /etc/passwd [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# grep reboot /etc/passwd
reboot:x:105:1::/export/home/reboot:/bin/pfsh
```

Ajoutez maintenant le rôle **reboot** aux rôles utilisables par **user1** :

```
# usermod -R reboot user1 [Entrée]
```

Vérifiez maintenant que le rôle a bien été ajouté :

```
# grep "user1" /etc/user_attr [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# usermod -R reboot user1
# grep "user1" /etc/user_attr
user1::::type=normal;roles=reboot
```

Actuellement ce rôle ne possède aucun profil. Pour créer un profil, il convient d'éditer le fichier **/etc/security/prof_attr** :

```
# echo "REBOOT:::profile pour reboot:help=reboot.html" >> /etc/security/prof_attr [Entrée]
```

Il est maintenant nécessaire d'ajouter le profil **REBOOT** au rôle reboot :

```
# rolemod -P REBOOT reboot [Entrée]
```

Vérifiez maintenant que le profil a bien été ajouté au rôle :

```
# grep reboot /etc/user_attr [Entrée]
```

Vous obtiendrez les résultat suivant :

```
# grep reboot /etc/user_attr
reboot::::type=role;profiles=REBOOT
user1::::type=normal;roles=reboot
```

Le profil REBOOT est actuellement vide. Il est nécessaire d'ajouter la commande /usr/sbin/reboot au profil. Il convient donc d'éditer le fichier **/etc/security/exec_attr** :

```
# echo "REBOOT:suser:cmd:::/usr/sbin/reboot:euid=0" >> /etc/security/exec_attr [Entrée]
```

Le rôle ainsi que le profil ayant été configurés, assumez l'identité d'user1 et essayez de redémarrer le système :

```
# su - user1
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ /usr/sbin/reboot
reboot : autorisation refusée
```

Vous noterez que vous n'avez pas l'autorisation nécessaire ! Ceci est parce que vous n'avez pas utiliser le rôle créé pour redémarrer le système. Tapez donc la commande suivante :

```
$ su reboot [Entrée]
```

Fermez toutes vos fenêtres et essayez ensuite de redémarrer le système :

```
$ /usr/sbin/reboot
```

Quand votre système a redémarré, essayez d'utiliser le rôle reboot en tant que l'utilisateur **user2** :

```
# su - user2
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ su reboot
Mot de passe :
Les rôles ne peuvent être assumés que par des utilisateurs autorisés
su: Désolé
```

Notez que ceci n'est pas possible.

Quittez le compte **user2** :

```
$ exit
#
```

LAB#3 - Autorisations

Dans ce LAB vous allez associer une autorisation à un service. Chaque utilisateur ou rôle ayant cette autorisation pourras travailler avec le service.

Vous allez :

- Créer une autorisation pour gérer le service d'Apache2,
- Informer Apache2 de la création de l'autorisation,
- Associer l'autorisation à un utilisateur,
- Tester votre configuration.

Tout d'abord, établissez le fait que l'utilisateur user1 n'est pas en mesure de travailler avec le service **apache2** :

```
$ /usr/sbin/svcadm -v disable -s apache2 [Entrée]
```

Vous obtiendrez le résultat suivant :

```
# su - user1
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ /usr/sbin/svcadm -v disable -s apache2
svcadm: svc:/network/http:apache2: Impossible de modifier le groupe de propriétés "general" (autorisation
refusée).
$ exit
#
```

Créez maintenant une autorisation pour gérer le service d'Apache2 dans le fichier **/etc/security/auth_attr**

```
# echo "solaris.smf.manage.apache/server:::Apache Server management::" >> /etc/security/auth_attr [Entrée]
```

Actuellement Apache n'est pas au courant de cette autorisation. Pour vérifier ce point,il convient d'utiliser la commande **svcprop** :

```
# svcprop -p general apache2 [Entrée]
```

Vous obtiendrez le résultat suivant :

```
# svcprop -p general apache2
general/enabled boolean false
general/entity_stability astring Evolving
```

Notez que l'autorisation **solaris.smf.manage.apache/server** est inconnue au service apache2. Il est donc maintenant nécessaire de dire à Apache de vérifier cette autorisation quand un utilisateur essaie de travailler avec le service d'Apache :

```
# svccfg -s apache2 setprop general/action_authorization=astring: 'solaris.smf.manage.apache/server' [Entrée]
```

A l'aide du manuel, expliquez-vous cette ligne de commande.

Vérifiez maintenant le résultat de votre commande :

```
# svcadm refresh apache2; svcprop -p general apache2 [Entrée]
```

```
# svcadm refresh apache2; svcprop -p general apache2
general/enabled boolean true
general/action_authorization astring solaris.smf.manage.apache/server
general/entity_stability astring Evolving
```

Notez que l'**action_authorization** a bien été associée avec le service.

Vous pouvez maintenant associer cette autorisation à l'utilisateur user1 :

```
# usermod -A solaris.smf.manage.apache/server user1 [Entrée]
```

Devenez user1 et visualiser le statut du service apache2 grâce à la commande **svcs** :

```
# su - user1
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ svcs apache2
STATE          STIME    FMRI
online         21:03:13 svc:/network/http:apache2
```

L'autorisation du type **action_authorization** vous permet de visualiser le statut du service. Essayez maintenant d'arrêter le service :

```
# /usr/sbin/svcadm disable apache2 [Entrée]
```

Vous obtiendrez le résultat suivant :

```
$ /usr/sbin/svcadm disable apache2
svcadm: svc:/network/http:apache2: Autorisation refusée.
```

Notez que l'autorisation du type **action_authorization** ne vous permet **que** de visualiser le statut du service. Pour pouvoir arrêter le service il faut une autorisation du type **value_authorization**.

```
# svccfg -s apache2 setprop general/value_authorization=astring: 'solaris.smf.manage.apache/server' [Entrée]
```

```
$ exit
# svccfg -s apache2 setprop general/value_authorization=astring: 'solaris.smf.manage.apache/server'
```

A l'aide du manuel, expliquez-vous cette ligne de commande.

Essayez de nouveau à démarrer le service apache2 en tant que l'utilisateur user1. Vous obtiendrez le résultat suivant :

```
# su - user1
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$ /usr/sbin/svcadm disable apache2
$ svcs apache2
STATE          STIME    FMRI
disabled       21:16:46 svc:/network/http:apache2
```

Activez de nouveau le service apache :

```
$ /usr/sbin/svcadm enable apache2
$ svcs apache2
STATE          STIME    FMRI
online         21:17:25 svc:/network/http:apache2
```

L'utilisateur user1 peut maintenant travailler avec le service apache2.

LAB#4 - RBAC et les Privilèges

Dans ce LAB vous allez associer un privilège à un utilisateur et à un rôle.

Vous allez :

- Attribuer directement des privilèges à un utilisateur,
- Attribuer, indirectement via un rôle, des privilèges à un utilisateur.

Les **Privilèges** permettent à un utilisateur de faire quelque chose avec le noyau. Il existe 70 privilèges :

```
contract_event contract_observer cpc_cpu dtrace_kernel dtrace_proc dtrace_user file_chown file_chown_self
file_dac_execute file_dac_read file_dac_search file_dac_write file_downgrade_sl file_flag_set file_link_any
file_owner file_setid file_upgrade_sl graphics_access graphics_map ipc_dac_read ipc_dac_write ipc_owner
net_bindmlp net_icmpaccess net_mac_aware net_privaddr net_rawaccess proc_audit proc_chroot proc_clock_highres
proc_exec proc_fork proc_info proc_lock_memory proc_owner proc_priocntl proc_session proc_setid proc_taskid
proc_zone sys_acct sys_admin sys_audit sys_config sys_devices sys_ip_config sys_ipc_config sys_linkdir sys_mount
```

```
sys_net_config sys_nfs sys_res_config sys_resource sys_smb sys_suser_compat sys_time sys_trans_label win_colormap
win_config win_dac_read win_dac_write win_devices win_dga win_downgrade_sl win_fontpath win_mac_read
win_mac_write win_selection win_upgrade_sl
```

Chaque processus dans le système possède 4 jeux de privilèges. Pour consulter les privilèges du processus courant, c'est-à-dire votre terminal, saisissez la commande suivante :

```
# ppriv -v $$ [Entrée]
```

Vous obtiendrez le résultat suivant :

```
$ exit
# ppriv -v $$
1137:   sh
flags = <none>
        E:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
        I: file_link_any,proc_exec,proc_fork,proc_info,proc_session
        P:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
```

```
        L:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
```

Les quatre jeux sont identifiés par une lettre :

Lettre	**Description**
E	Privilèges effectifs
I	Privilèges par héritage
P	Privilèges autorisés
L	Privilèges Limités

Pour faciliter la gestion des privilèges, les jeux sont organisés en **alias** :

```
# ppriv $$
1137:   sh
flags = <none>
        E: all
        I: basic
        P: all
        L: all
# su user2
$ ppriv $$
1193:   sh
flags = <none>
        E: basic
        I: basic
        P: basic
```

```
        L: all
```

L'utilisation de l'option **-v** permet de contrôler le contenu des alias :

```
$ exit
# ppriv -v $$
1137:   sh
flags = <none>
        E:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
        I: file_link_any,proc_exec,proc_fork,proc_info,proc_session
        P:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
        L:
contract_event,contract_observer,cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,file_chown,file_chown_self,file_da
c_execute,file_dac_read,file_dac_search,file_dac_write,file_downgrade_sl,file_link_any,file_owner,file_setid,file
_upgrade_sl,graphics_access,graphics_map,ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,net_icmpaccess,net_mac_
aware,net_privaddr,net_rawaccess,proc_audit,proc_chroot,proc_clock_highres,proc_exec,proc_fork,proc_info,proc_loc
k_memory,proc_owner,proc_priocntl,proc_session,proc_setid,proc_taskid,proc_zone,sys_acct,sys_admin,sys_audit,sys_
config,sys_devices,sys_ip_config,sys_ipc_config,sys_linkdir,sys_mount,sys_net_config,sys_nfs,sys_res_config,sys_r
```

```
esource,sys_suser_compat,sys_time,sys_trans_label,win_colormap,win_config,win_dac_read,win_dac_write,win_devices,
win_dga,win_downgrade_sl,win_fontpath,win_mac_read,win_mac_write,win_selection,win_upgrade_sl
```

Dans notre cas, nous souhaitons donner les privilèges de l'utilisation de **dtrace** à **user2**. Pour utiliser dtrace, user2 aura besoin de trois privilèges :

- dtrace_kernel
- dtrace_proc
- dtrace_user

Afin d'attribuer ces privilèges à user2, saisissez la commande suivante en tant que **root** :

```
# usermod -K defaultpriv=basic,dtrace_kernel,dtrace_proc,dtrace_user user2 [Entrée]
```

Devenez maintenant user2 et contrôlez ses privilèges :

```
# su user2
$ ppriv $$
1228:   sh
flags = <none>
        E: basic,dtrace_kernel,dtrace_proc,dtrace_user
        I: basic,dtrace_kernel,dtrace_proc,dtrace_user
        P: basic,dtrace_kernel,dtrace_proc,dtrace_user
        L: all
```

Vous noterez que les privilèges ont été ajoutés.

Dans l'exemple ci-dessus, nous avons attribué les privilèges directement à user2. Solaris nous permet aussi d'attribuer des privilèges à un rôle.

Dans le cas de ce LAB, nous allons d'abord créer un rôle appelé **chbogues** en utilisant le profil **Process Management**:

```
# roleadd -m -d /export/home/chbogues -P "Process Management" chbogues [Entrée]
```

Saisissez donc la commande. Vous obtiendrez le résultat suivant :

```
$ exit
# roleadd -m -d /export/home/chbogues -P "Process Management" chbogues
64 blocs
```

Attribuez maintenant le mot de passe **chbogues** au rôle chbogue :

```
# passwd chbogues
Nouveau mot de passe :
Entrez de nouveau le mot de passe :
passwd: mot de passe correctement modifié pour chbogues
```

Il est maintenant nécessaire d'attribuer les privilèges dtrace_kernel,dtrace_proc et dtrace_user à notre rôle chbogues :

```
# rolemod -K defaultpriv=basic,dtrace_kernel,dtrace_proc,dtrace_user chbogues [Entrée]
```

et ensuite d'attribuer le droit d'utilisation du rôle à l'utilisateur user1 :

```
# usermod -R chbogues user1 [Entrée]
```

Devenez maintenant user1 et contrôlez ses privilèges :

```
# su user1
$ ppriv $$
1254:   sh
flags = <none>
        E: basic
        I: basic
        P: basic
        L: all
```

Vous noterez que l'utilisateur user1 ne possède pas de privilèges dtrace_kernel,dtrace_proc et dtrace_user.

En tant qu'user1, assumez le rôle chbogues et contrôlez les privilèges :

```
$ su chbogues
Mot de passe :
$ ppriv $$
1263:   pfsh
flags = <none>
        E: basic,dtrace_kernel,dtrace_proc,dtrace_user
        I: basic,dtrace_kernel,dtrace_proc,dtrace_user
        P: basic,dtrace_kernel,dtrace_proc,dtrace_user
        L: all
```

Grâce au rôle, user1 peut maintenant utiliser les privilèges dtrace_kernel,dtrace_proc et dtrace_user.

L'utilisation des privilèges n'est évidemment pas restreinte à des utilisateurs. Dans le cas de Solaris, il existe des processus appelés **privileged aware process**, par exemple, le processus *kfcd* :

```
$ exit
$ exit
# ps -ef | grep "kcfd"
  daemon   120     1   0 20:51:48 ?           0:09 /usr/lib/crypto/kcfd
    root  1265  1261   1 21:34:56 pts/3       0:00 grep kcfd
# ppriv -v 120
120:    /usr/lib/crypto/kcfd
flags = PRIV_AWARE
        E: file_owner,proc_priocntl,sys_devices
        I: none
        P: file_owner,proc_priocntl,sys_devices
        L: none
```

Notez ici que le démon ne possède que les privilèges minimums pour pouvoir exécuter correctement.

Références

- **The Oracle Technology Network**
