Version : **2021.01**

Dernière mise-à-jour : 2023/02/14 09:17

A faire : Afin de mettre en pratique les exemples dans ce cours, vous devez vous connecter à votre système en tant que root grâce à la commande **su -** et le mot de passe **fenestros**.

LCF201 - Gestion des Utilisateurs

Contenu du Module

Présentation

La bonne gestion des utilisateurs passe par une bonne stratégie de groupes. En effet, chaque utilisateur est affecté à un groupe **principal** mais il peut aussi être membre d'un ou de plusieurs groupes secondaires.

Comme dans d'autres systèmes d'exploitation, sous Linux il est préférable de donner les droits d'accès aux groupes et non aux utilisateurs individuels.

Les bases de données utilisées pour stocker les informations des utilisateurs et des groupes sont stipulées dans le fichier **/etc/nsswitch.conf**. Dans notre cas les entrées passwd, shadow et group indique le mot clef **files**. Ceci indique l'utilisation des fichiers suivants en tant que base de données :

- **/etc/passwd**,
- **/etc/shadow**,
- **/etc/group**.

/etc/nsswitch.conf sous RHEL 5

```
[root@centos5 ~]# cat /etc/nsswitch.conf
```

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       nisplus or nis+         Use NIS+ (NIS version 3)
#       nis or yp               Use NIS (NIS version 2), also called YP
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the local database (.db) files
#       compat                  Use NIS on compat mode
#       hesiod                  Use Hesiod for user lookups
#       [NOTFOUND=return]       Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files
shadow:     files
```

```
group:      files
...
```

/etc/nsswitch.conf sous RHEL 6

```
[root@centos6 ~]# cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Valid entries include:
#
#   nisplus            Use NIS+ (NIS version 3)
#   nis             Use NIS (NIS version 2), also called YP
#   dns             Use DNS (Domain Name Service)
#   files             Use the local files
#   db             Use the local database (.db) files
#   compat             Use NIS on compat mode
#   hesiod             Use Hesiod for user lookups
#   [NOTFOUND=return]    Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
```

```
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files
shadow:     files
group:      files
...
```

/etc/nsswitch.conf sous RHEL 7

```
[root@centos7 ~]# cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Valid entries include:
#
#   nisplus            Use NIS+ (NIS version 3)
#   nis             Use NIS (NIS version 2), also called YP
#   dns             Use DNS (Domain Name Service)
#   files             Use the local files
#   db             Use the local database (.db) files
#   compat             Use NIS on compat mode
```

```
#   hesiod            Use Hesiod for user lookups
#   [NOTFOUND=return]    Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files sss
shadow:     files sss
group:      files sss
...
```

Interrogation des Bases de Données

La commande **getent** est utilisée pour interroger les bases de données. Elle prend la forme suivante :

```
getent base-de-données clef
```

Par exemple pour rechercher l'utilisateur dans la base de données des utilisateurs, il convient d'utiliser la commande suivante :

```
[root@centos5 ~]# getent passwd trainee
trainee:x:500:500:trainee:/home/trainee:/bin/bash
```

```
[root@centos6 ~]# getent passwd trainee
trainee:x:500:500:trainee:/home/trainee:/bin/bash
```

```
[root@centos7 ~]# getent passwd trainee
```

```
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
```

Pour rechercher quels utilisateurs appartiennent à quels groupes, il convient d'utiliser la commande suivante :

```
[root@centos5 ~]# getent group mail
mail:x:12:mail
```

```
[root@centos6 ~]# getent group mail
mail:x:12:mail,postfix
```

```
[root@centos7 ~]# getent group mail
mail:x:12:postfix
```

L'utilisation de la commande getent sans spécifier une clef imprime à l'écran le contenu de la base de données :

```
[root@centos5 ~]# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
```

```
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:101:1::/var/run/vboxadd:/bin/false
```

```
[root@centos6 ~]# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

```
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:498:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
pulse:x:497:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:496:1::/var/run/vboxadd:/bin/false
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
lighttpd:x:495:492:lighttpd web server:/var/www/lighttpd:/sbin/nologin
```

```
[root@centos7 ~]# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
```

```
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
unbound:x:998:997:Unbound DNS resolver:/etc/unbound:/sbin/nologin
colord:x:997:996:User for colord:/var/lib/colord:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
saslauth:x:996:76:"Saslauthd user":/run/saslauthd:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
libstoragemgmt:x:995:994:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:994:993::/var/lib/chrony:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
vboxadd:x:992:1::/var/run/vboxadd:/bin/false
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
crypt:x:1001:1001::/home/crypt:/bin/bash
```

Les Fichiers /etc/group et /etc/gshadow

Pour lister les groupes existants sur le système, saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
nscd:x:28:
floppy:x:19:
vcsa:x:69:
pcap:x:77:
```

```
slocate:x:21:
ntp:x:38:
dbus:x:81:
audio:x:63:gdm
avahi:x:70:
rpc:x:32:
mailnull:x:47:
smmsp:x:51:
apache:x:48:
hsqldb:x:96:
sshd:x:74:
rpcuser:x:29:
nfsnobody:x:65534:
xfs:x:43:
haldaemon:x:68:
avahi-autoipd:x:101:
gdm:x:42:
trainee:x:500:
vboxsf:x:102:
```

```
[root@centos6 ~]# cat /etc/group
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
lp:x:7:daemon
mem:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:mail,postfix
uucp:x:14:
```

```
man:x:15:
games:x:20:
gopher:x:30:
video:x:39:
dip:x:40:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
dbus:x:81:
utmp:x:22:
utempter:x:35:
desktop_admin_r:x:499:
desktop_user_r:x:498:
avahi-autoipd:x:170:
floppy:x:19:
vcsa:x:69:
rpc:x:32:
rtkit:x:497:
cdrom:x:11:
tape:x:33:
dialout:x:18:
ntp:x:38:
saslauth:x:76:
postdrop:x:90:
postfix:x:89:
avahi:x:70:
haldaemon:x:68:haldaemon
pulse:x:496:
pulse-access:x:495:
fuse:x:494:
gdm:x:42:
rpcuser:x:29:
```

```
nfsnobody:x:65534:
abrt:x:173:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
sshd:x:74:
tcpdump:x:72:
slocate:x:21:
trainee:x:500:
wbpriv:x:88:
vboxsf:x:501:
tss:x:59:
ecryptfs:x:493:
mysql:x:27:
lighttpd:x:492:
```

```
[root@centos7 ~]# cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
```

```
tape:x:30:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
utmp:x:22:
utempter:x:35:
ssh_keys:x:999:
systemd-journal:x:190:
dbus:x:81:
polkitd:x:998:
unbound:x:997:
colord:x:996:
usbmuxd:x:113:
cgred:x:995:
dip:x:40:
avahi:x:70:
avahi-autoipd:x:170:
saslauth:x:76:
kvm:x:36:qemu
qemu:x:107:
libstoragemgmt:x:994:
rpc:x:32:
rpcuser:x:29:
nfsnobody:x:65534:
rtkit:x:172:
radvd:x:75:
ntp:x:38:
chrony:x:993:
abrt:x:173:
pulse-access:x:992:
pulse:x:171:
```

```
gdm:x:42:
gnome-initial-setup:x:991:
stapusr:x:156:
stapsys:x:157:
stapdev:x:158:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
sshd:x:74:
tcpdump:x:72:
trainee:x:1000:trainee
vboxsf:x:990:
tss:x:59:
crypt:x:1001:
```

> **Important** : Notez que la valeur du GID du groupe root est toujours de 0. Notez cependant que sous RHEL 5 et 6 les GID des utilisateurs normaux commencent à **500** et les GID des comptes système sont inclus entre 1 et 99 par convention. Sous RHEL 7, les GID des utilisateurs normaux commencent à **1000** et les GID des comptes système sont inclus entre 201 et 999.

Dans ce fichier, chaque ligne est constituée de 4 champs :

- Le nom **unique** du groupe,
- Le mot de passe du groupe. Une valeur de **x** dans ce champs indique que le système utilise le fichier **/etc/gshadow** pour stocker les mots de passe. Une valeur de **!** indique que le groupe n'a pas de mot passe et que l'accès au groupe via la commande **newgrp** n'est pas possible,
- Le GID. Une valeur unique utilisée pour déterminée les droits d'accès aux fichiers et aux répertoires,
- La liste des membres ayant le groupe comme groupe **secondaire**.

Pour consulter le fichier **/etc/gshadow**, saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/gshadow
root:::root
bin:::root,bin,daemon
```

```
daemon:::root,bin,daemon
sys:::root,bin,adm
adm:::root,adm,daemon
tty:::
disk:::root
lp:::daemon,lp
mem:::
kmem:::
wheel:::root
mail:::mail
news:::news
uucp:::uucp
man:::
games:::
gopher:::
dip:::
ftp:::
lock:::
nobody:::
users:::
utmp:x::
utempter:x::
nscd:x::
floppy:x::
vcsa:x::
pcap:x::
slocate:x::
ntp:x::
dbus:x::
audio:x::gdm
avahi:x::
rpc:x::
mailnull:x::
smmsp:x::
```

```
apache:x::
hsqldb:x::
sshd:x::
rpcuser:x::
nfsnobody:x::
xfs:x::
haldaemon:x::
avahi-autoipd:x::
gdm:x::
trainee:!!::
vboxsf:!::
```

```
[root@centos6 ~]# cat /etc/gshadow
root:::
bin:::bin,daemon
daemon:::bin,daemon
sys:::bin,adm
adm:::adm,daemon
tty:::
disk:::
lp:::daemon
mem:::
kmem:::
wheel:::
mail:::mail,postfix
uucp:::
man:::
games:::
gopher:::
video:::
dip:::
ftp:::
lock:::
audio:::
```

```
nobody:::
users:::
dbus:!::
utmp:!::
utempter:!::
desktop_admin_r:!::
desktop_user_r:!::
avahi-autoipd:!::
floppy:!::
vcsa:!::
rpc:!::
rtkit:!::
cdrom:!::
tape:!::
dialout:!::
ntp:!::
saslauth:!::
postdrop:!::
postfix:!::
avahi:!::
haldaemon:!::haldaemon
pulse:!::
pulse-access:!::
fuse:!::
gdm:!::
rpcuser:!::
nfsnobody:!::
abrt:!::
stapusr:!::
stapsys:!::
stapdev:!::
sshd:!::
tcpdump:!::
slocate:!::
```

```
trainee:!!::
wbpriv:!::
vboxsf:!::
tss:!::
ecryptfs:!::
mysql:!::
lighttpd:!::
```

```
[root@centos7 ~]# cat /etc/gshadow
root:::
bin:::
daemon:::
sys:::
adm:::
tty:::
disk:::
lp:::
mem:::
kmem:::
wheel:::
cdrom:::
mail:::postfix
man:::
dialout:::
floppy:::
games:::
tape:::
video:::
ftp:::
lock:::
audio:::
nobody:::
users:::
utmp:!::
```

```
utempter:!::
ssh_keys:!::
systemd-journal:!::
dbus:!::
polkitd:!::
unbound:!::
colord:!::
usbmuxd:!::
cgred:!::
dip:!::
avahi:!::
avahi-autoipd:!::
saslauth:!::
kvm:!::qemu
qemu:!::
libstoragemgmt:!::
rpc:!::
rpcuser:!::
nfsnobody:!::
rtkit:!::
radvd:!::
ntp:!::
chrony:!::
abrt:!::
pulse-access:!::
pulse:!::
gdm:!::
gnome-initial-setup:!::
stapusr:!::
stapsys:!::
stapdev:!::
slocate:!::
postdrop:!::
postfix:!::
```

```
sshd:!::
tcpdump:!::
trainee:!!::trainee
vboxsf:!::
tss:!::
crypt:!::
```

Chaque ligne est constituée de 4 champs :

- Le nom du groupe. Ce champs est utilisé pour faire le lien avec le fichier **/etc/group**,
- Le mot de passe **crypté** du groupe s'il en existe un. Une valeur **vide** dans ce champs indique que seuls les membres du groupe peuvent exécuter la commande **newgrp**. Une valeur de **!**, de **x** ou de * indique que personne ne peut exécuter la commande **newgrp** pour le groupe,
- L'administrateur du groupe s'il en existe un,
- La liste des membres ayant le groupe comme groupe **secondaire**.

Afin de vérifier les fichiers **/etc/group** et **/etc/gshadow** pour des erreurs éventuelles, saisissez la commande suivante :

```
[root@centos5 ~]# grpck -r
```

```
[root@centos6 ~]# grpck -r
```

```
[root@centos7 ~]# grpck -r
```

Dans le cas où vos fichiers ne comportent pas d'erreurs, vous vous retrouverez retourné au prompt.

> **Important** : L'option **-r** permet la vérification des erreurs sans le modifier.

Dans le cas où il est nécessaire de régénérer un des deux fichiers, il convient d'utiliser une des deux commandes suivantes :

- **grpconv**
  - permet de régénérer le fichier **/etc/gshadow** à partir du fichier **/etc/group** et éventuellement du fichier **/etc/gshadow** existant

- **grpunconv**
  - permet de régénérer le fichier **/etc/group** à partir du fichier **/etc/gshadow** et éventuellement du fichier **/etc/group** existant puis supprime le fichier **/etc/gshadow**

Les Fichiers /etc/passwd et /etc/shadow

> **Important** : Notez que la règle la plus libérale concernant les noms d'utilisateurs sous Linux limite la longueur à 32 caractères et permet l'utilisation de majuscules, de minuscules, de nombres (sauf au début du nom) ainsi que la plupart des caractères de ponctuation. Ceci dit, certains utilitaires, tel **useradd** interdisent l'utilisation de majuscules et de caractères de ponctuation mais permettent l'utilisation des caractères **_**, **.** ainsi que le caractère **$** à la fin du nom (**ATTENTION** : dans le cas de samba, un nom d'utilisateur se terminant par **$** est considéré comme un compte **machine**). Qui plus est, certains utilitaires limitent la longueur du nom à **8** caractères.

Pour lister les comptes utilisateur existants sur le système, saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
```

```
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi:x:70:70:Avahi daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:101:1::/var/run/vboxadd:/bin/false
```

```
[root@centos6 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

```
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:498:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
pulse:x:497:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:496:1::/var/run/vboxadd:/bin/false
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
lighttpd:x:495:492:lighttpd web server:/var/www/lighttpd:/sbin/nologin
```

```
[root@centos7 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
```

```
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
unbound:x:998:997:Unbound DNS resolver:/etc/unbound:/sbin/nologin
colord:x:997:996:User for colord:/var/lib/colord:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
saslauth:x:996:76:"Saslauthd user":/run/saslauthd:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
libstoragemgmt:x:995:994:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:994:993::/var/lib/chrony:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
vboxadd:x:992:1::/var/run/vboxadd:/bin/false
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
crypt:x:1001:1001::/home/crypt:/bin/bash
```

Important : Notez que la valeur de l'UID de root est toujours de 0. Notez cependant que sous RHEL 5 et 6 les UID des utilisateurs normaux commencent à **500** et les UID des comptes système sont inclus entre 1 et 99 par convention. Sous RHEL 7, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 201 et 999.

Chaque ligne est constituée de 7 champs :

- Le nom d'utilisateur
- Le mot de passe. Une valeur de **x** dans ce champs indique que le système utilise le fichier **/etc/shadow** pour stocker les mots de passe.
- L'UID. Une valeur unique qui est utilisée pour déterminée les droits aux fichiers et aux répertoires.
- Le GID. Une valeur indiquant le groupe **principal** de l'utilisateur
- Le nom complet. Ce champs optionnel est aussi appelé **GECOS**
- Le répertoire personnel de l'utilisateur
- Le shell de l'utilisateur.

Pour consulter le fichier **/etc/shadow**, saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/shadow
root:$1$e2VuK3.8$cy7P6EdqfaSpIBGxalr2M0:16672:0:99999:7:::
bin:*:16672:0:99999:7:::
daemon:*:16672:0:99999:7:::
adm:*:16672:0:99999:7:::
lp:*:16672:0:99999:7:::
sync:*:16672:0:99999:7:::
shutdown:*:16672:0:99999:7:::
halt:*:16672:0:99999:7:::
mail:*:16672:0:99999:7:::
news:*:16672:0:99999:7:::
uucp:*:16672:0:99999:7:::
operator:*:16672:0:99999:7:::
games:*:16672:0:99999:7:::
gopher:*:16672:0:99999:7:::
```

```
ftp:*:16672:0:99999:7:::
nobody:*:16672:0:99999:7:::
nscd:!!:16672:0:99999:7:::
vcsa:!!:16672:0:99999:7:::
pcap:!!:16672:0:99999:7:::
ntp:!!:16672:0:99999:7:::
dbus:!!:16672:0:99999:7:::
avahi:!!:16672:0:99999:7:::
rpc:!!:16672:0:99999:7:::
mailnull:!!:16672:0:99999:7:::
smmsp:!!:16672:0:99999:7:::
apache:!!:16672:0:99999:7:::
hsqldb:!!:16672:0:99999:7:::
sshd:!!:16672:0:99999:7:::
rpcuser:!!:16672:0:99999:7:::
nfsnobody:!!:16672:0:99999:7:::
xfs:!!:16672:0:99999:7:::
haldaemon:!!:16672:0:99999:7:::
avahi-autoipd:!!:16672:0:99999:7:::
gdm:!!:16672:0:99999:7:::
trainee:$1$wwULknA7$k9AoozIcTYDbLk9Ts5f5S1:16672:0:99999:7:::
vboxadd:!!:16672::::::
```

```
[root@centos6 ~]# cat /etc/shadow
root:$6$iRkW7flDRC7d5.6A$Lw/4Lm1hiSSmy1iX09YUpcNPh1lYGDCwja5ZcCgXQS4ZGIsl1A2ITK7Ts7k68JVHOvO0paMiEbD2iPN7FudRZ/:1
5828:0:99999:7:::
bin:*:15513:0:99999:7:::
daemon:*:15513:0:99999:7:::
adm:*:15513:0:99999:7:::
lp:*:15513:0:99999:7:::
sync:*:15513:0:99999:7:::
shutdown:*:15513:0:99999:7:::
halt:*:15513:0:99999:7:::
mail:*:15513:0:99999:7:::
```

```
uucp:*:15513:0:99999:7:::
operator:*:15513:0:99999:7:::
games:*:15513:0:99999:7:::
gopher:*:15513:0:99999:7:::
ftp:*:15513:0:99999:7:::
nobody:*:15513:0:99999:7:::
dbus:!!:15828::::::
avahi-autoipd:!!:15828::::::
vcsa:!!:15828::::::
rpc:!!:15828:0:99999:7:::
rtkit:!!:15828::::::
ntp:!!:15828::::::
saslauth:!!:15828::::::
postfix:!!:15828::::::
avahi:!!:15828::::::
haldaemon:!!:15828::::::
pulse:!!:15828::::::
gdm:!!:15828::::::
rpcuser:!!:15828::::::
nfsnobody:!!:15828::::::
abrt:!!:15828::::::
sshd:!!:15828::::::
tcpdump:!!:15828::::::
trainee:$6$N8zTnmNWvcB769EI$s3dXmCsh5JZhImxkR2RKI18lBf7FtqDFljN8oTgPZV8uM2QFtgCz7I.PdISxurNVS4oKgv61kVWIgSX7gP4DN
/:15828:0:99999:7:::
vboxadd:!!:15828::::::
tss:!!:16620::::::
mysql:!!:16656::::::
lighttpd:!!:16656::::::
```

```
[root@centos7 ~]# cat /etc/shadow
root:$6$r4px/s9L2uwGSFnI$NkK5mzNF.CMAFFqMcO.i.tnrMZQDkriDLYwICsimsPaDWKFwUHS3NhDwZY5e7P3glIu.gTBtaOE.SOOW/D.AU/:1
6502:0:99999:7:::
bin:*:16231:0:99999:7:::
```

```
daemon:*:16231:0:99999:7:::
adm:*:16231:0:99999:7:::
lp:*:16231:0:99999:7:::
sync:*:16231:0:99999:7:::
shutdown:*:16231:0:99999:7:::
halt:*:16231:0:99999:7:::
mail:*:16231:0:99999:7:::
operator:*:16231:0:99999:7:::
games:*:16231:0:99999:7:::
ftp:*:16231:0:99999:7:::
nobody:*:16231:0:99999:7:::
dbus:!!:16502::::::
polkitd:!!:16502::::::
unbound:!!:16502::::::
colord:!!:16502::::::
usbmuxd:!!:16502::::::
avahi:!!:16502::::::
avahi-autoipd:!!:16502::::::
saslauth:!!:16502::::::
qemu:!!:16502::::::
libstoragemgmt:!!:16502::::::
rpc:!!:16502:0:99999:7:::
rpcuser:!!:16502::::::
nfsnobody:!!:16502::::::
rtkit:!!:16502::::::
radvd:!!:16502::::::
ntp:!!:16502::::::
chrony:!!:16502::::::
abrt:!!:16502::::::
pulse:!!:16502::::::
gdm:!!:16502::::::
gnome-initial-setup:!!:16502::::::
postfix:!!:16502::::::
sshd:!!:16502::::::
```

```
tcpdump:!!:16502::::::
trainee:$6$tMd44tmmFiitAS7.$sJSua3jhyKm2k0mIifYuTpUO0d6q6/gS3PDyuxbHadHVYLsoVslZ3Pn8m5X93rr64oj.KK8OL6J.gvhxbQBrZ
1:16502:0:99999:7:::
vboxadd:!!:16590::::::
tss:!!:16590::::::
crypt:!!:16621:0:99999:7:::
```

Chaque ligne est constituée de 8 champs :

- Le nom de l'utilisateur. Ce champs est utilisé pour faire le lien avec le fichier **/etc/passwd**,
- Le mot de passe **crypté** de l'utilisateur. Le cryptage est à sens **unique**. Ce champ peut aussi contenir une des trois valeurs suivantes :
  - **!!** - Le mot de passe n'a pas encore été défini et l'utilisateur ne peut pas se connecter,
  - * - L'utilisateur ne peut pas se connecter,
  - **vide** - aucun mot de passe sera demandé pour l'utilisateur concerné,
- Le nombre de jours entre le **01/01/1970** et le dernier changement du mot de passe,
- Le nombre de jours que le mot de passe est encore valide. Une valeur de **0** dans ce champs indique sue le mot de passe n'expire jamais,
- Le nombre de jours après lequel le mot de passe doit être changé,
- Le nombre de jours avant la date de modification forcée que l'utilisateur recevra un avertissement,
- Le nombre de jours après l'expiration du mot de passe que le compte sera désactivé,
- Le **numéro** du jour après le **01/01/1970** que le compte a été désactivé.

Afin de vérifier les fichiers **/etc/passwd** et **/etc/shadow** pour des erreurs éventuelles, saisissez la commande suivante :

```
[root@centos5 ~]# pwck -r
utilisateur adm : le répertoire /var/adm n'existe pas
utilisateur news : le répertoire /etc/news n'existe pas
utilisateur uucp : le répertoire /var/spool/uucp n'existe pas
utilisateur gopher : le répertoire /var/gopher n'existe pas
utilisateur ftp : le répertoire /var/ftp n'existe pas
utilisateur pcap : le répertoire /var/arpwatch n'existe pas
utilisateur avahi-autoipd : le répertoire /var/lib/avahi-autoipd n'existe pas
utilisateur vboxadd : le répertoire /var/run/vboxadd n'existe pas
pwck : aucun changement
```

```
[root@centos6 ~]# pwck -r
utilisateur adm : le répertoire « /var/adm » n'existe pas
utilisateur uucp : le répertoire « /var/spool/uucp » n'existe pas
utilisateur gopher : le répertoire « /var/gopher » n'existe pas
utilisateur ftp : le répertoire « /var/ftp » n'existe pas
utilisateur avahi-autoipd : le répertoire « /var/lib/avahi-autoipd » n'existe pas
utilisateur saslauth : le répertoire « /var/empty/saslauth » n'existe pas
utilisateur pulse : le répertoire « /var/run/pulse » n'existe pas
utilisateur vboxadd : le répertoire « /var/run/vboxadd » n'existe pas
pwck : aucun changement
```

```
[root@centos7 ~]# pwck -r
user 'ftp': directory '/var/ftp' does not exist
user 'avahi-autoipd': directory '/var/lib/avahi-autoipd' does not exist
user 'pulse': directory '/var/run/pulse' does not exist
user 'gnome-initial-setup': directory '/run/gnome-initial-setup/' does not exist
user 'vboxadd': directory '/var/run/vboxadd' does not exist
pwck: no changes
```

> **Important** : Les erreurs ci-dessus ne sont pas importantes. Elles sont dues au fait que les répertoires de connexion de certains comptes systèmes ne sont pas créés par le système lors de la création des comptes et ceci justement pour éviter la possibilité qu'un pirate ou un hacker puisse se connecter au système en utilisant le compte concerné. Encore une fois, l'option **-r** permet la vérification des erreurs dans sans le modifier.

Dans le cas où il est nécessaire de régénérer un des deux fichiers, il convient d'utiliser une des deux commandes suivantes :

- **pwconv**
  - permet de régénérer le fichier **/etc/shadow** à partir du fichier **/etc/passwd** et éventuellement du fichier **/etc/shadow** existant
- **pwunconv**
  - permet de régénérer le fichier **/etc/passwd** à partir du fichier **/etc/shadow** et éventuellement du fichier **/etc/passwd** existant puis supprime le fichier **/etc/shadow**

Commandes

Groupes

groupadd

Cette commande est utilisée pour créer un groupe.

Options de la commande

```
[root@centos7 ~]# groupadd --help
Usage: groupadd [options] GROUP

Options:
  -f, --force                   exit successfully if the group already exists,
                                and cancel -g if the GID is already used
  -g, --gid GID                 use GID for the new group
  -h, --help                    display this help message and exit
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -o, --non-unique              allow to create groups with duplicate
                                (non-unique) GID
  -p, --password PASSWORD       use this encrypted password for the new group
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
```

Important : Il est possible de créer plusieurs groupes ayant le même GID.

Important : Notez l'option **-r** qui permet la création d'un groupe système.

groupdel

Cette commande est utilisée pour supprimer un groupe.

Options de la commande

```
[root@centos7 ~]# groupdel --help
Usage: groupdel [options] GROUP

Options:
  -h, --help                    display this help message and exit
  -R, --root CHROOT_DIR         directory to chroot into
```

groupmod

Cette commande est utilisée pour modifier un groupe existant.

Options de la commande

```
[root@centos7 ~]# groupmod --help
Usage: groupmod [options] GROUP

Options:
```

```
  -g, --gid GID                 change the group ID to GID
  -h, --help                    display this help message and exit
  -n, --new-name NEW_GROUP      change the name to NEW_GROUP
  -o, --non-unique              allow to use a duplicate (non-unique) GID
  -p, --password PASSWORD       change the password to this (encrypted)
                                PASSWORD
  -R, --root CHROOT_DIR         directory to chroot into
```

newgrp

Cette commande est utilisée pour modifier le groupe de l'utilisateur qui l'invoque.

Options de la commande

```
[root@centos7 ~]# newgrp --help
Usage: newgrp [-] [group]
```

gpasswd

Cette commande est utilisée pour modifier administrer le fichier **/etc/group**.

Options de la commande

```
[root@centos7 ~]# gpasswd --help
Usage: gpasswd [option] GROUP

Options:
  -a, --add USER                add USER to GROUP
```

```
  -d, --delete USER             remove USER from GROUP
  -h, --help                    display this help message and exit
  -Q, --root CHROOT_DIR         directory to chroot into
  -r, --remove-password         remove the GROUP's password
  -R, --restrict                restrict access to GROUP to its members
  -M, --members USER,...        set the list of members of GROUP
  -A, --administrators ADMIN,...
                                set the list of administrators for GROUP
Except for the -A and -M options, the options cannot be combined.
```

Utilisateurs

useradd

Cette commande est utilisée pour ajouter un utilisateur.

Les codes retour de la commande useradd sont :

Code Retour	Description
1	Impossible de mettre à jour le fichier /etc/passwd
2	Syntaxe invalide
3	Option invalide
4	L'UID demandé est déjà utilisé
6	Le groupe spécifié n'existe pas
9	Le nom d'utilisateur indiqué existe déjà
10	Impossible de mettre à jour le fichier /etc/group
12	Impossible de créer le répertoire personnel de l'utilisateur
13	Impossible de créer le spool mail de l'utilisateur

Options de la commande

```
[root@centos7 ~]# useradd --help
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]

Options:
  -b, --base-dir BASE_DIR       base directory for the home directory of the
                                new account
  -c, --comment COMMENT         GECOS field of the new account
  -d, --home-dir HOME_DIR       home directory of the new account
  -D, --defaults                print or change default useradd configuration
  -e, --expiredate EXPIRE_DATE  expiration date of the new account
  -f, --inactive INACTIVE       password inactivity period of the new account
  -g, --gid GROUP               name or ID of the primary group of the new
                                account
  -G, --groups GROUPS           list of supplementary groups of the new
                                account
  -h, --help                    display this help message and exit
  -k, --skel SKEL_DIR           use this alternative skeleton directory
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -l, --no-log-init             do not add the user to the lastlog and
                                faillog databases
  -m, --create-home             create the user's home directory
  -M, --no-create-home          do not create the user's home directory
  -N, --no-user-group           do not create a group with the same name as
                                the user
  -o, --non-unique              allow to create users with duplicate
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             login shell of the new account
  -u, --uid UID                 user ID of the new account
  -U, --user-group              create a group with the same name as the user
```

```
  -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mapping
```

Important : Il est possible de créer plusieurs utilisateurs ayant le même UID.

Important : Notez l'option **-r** qui permet la création d'un compte système. Dans ce cas la commande useradd ne crée pas de répertoire personnel.

userdel

Cette commande est utilisée pour supprimer un utilisateur.

Options de la commande

```
[root@centos7 ~]# userdel --help
Usage: userdel [options] LOGIN

Options:
  -f, --force                   force some actions that would fail otherwise
                                e.g. removal of user still logged in
                                or files, even if not owned by the user
  -h, --help                    display this help message and exit
  -r, --remove                  remove home directory and mail spool
  -R, --root CHROOT_DIR         directory to chroot into
  -Z, --selinux-user            remove any SELinux user mapping for the user
```

Important : Notez que lors de la suppression d'un utilisateur, l'UID associé avec ce compte peut être réutilisé. Le nombre maximum de comptes était de **65 536** avec le noyau **2.2.x**. Avec les noyaux récents, cette limite passe à plus de 4,2 Milliards.

usermod

Cette commande est utilisée pour modifier un utilisateur existant.

Options de la commande

```
[root@centos7 ~]# usermod --help
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
```

```
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

Important : Notez l'option **-L** qui permet de verrouiller un compte.

passwd

Cette commande est utilisée pour créer ou modifier le mot de passe d'un utilisateur.

Options de la commande

```
[root@centos7 ~]# passwd --help
Usage: passwd [OPTION...] <accountName>
  -k, --keep-tokens       keep non-expired authentication tokens
  -d, --delete            delete the password for the named account (root only)
  -l, --lock              lock the password for the named account (root only)
  -u, --unlock            unlock the password for the named account (root only)
  -e, --expire            expire the password for the named account (root only)
  -f, --force             force operation
  -x, --maximum=DAYS      maximum password lifetime (root only)
  -n, --minimum=DAYS      minimum password lifetime (root only)
  -w, --warning=DAYS      number of days warning users receives before
                          password expiration (root only)
```

```
  -i, --inactive=DAYS     number of days after password expiration when an
                          account becomes disabled (root only)
  -S, --status            report password status on the named account (root
                          only)
  --stdin                 read new tokens from stdin (root only)

Help options:
  -?, --help              Show this help message
  --usage                 Display brief usage message
```

Important : Notez l'option **-l** qui permet de verrouiller un compte en plaçant le caractère **!** devant le mot de passe crypté.

chage

La commande chage modifie le nombre de jours entre les changements de mot de passe et la date du dernier changement. Ces informations sont utilisées par le système pour déterminer si un utilisateur doit changer son mot de passe.

Options de la commande

```
[root@centos7 ~]# chage --help
Usage: chage [options] LOGIN

Options:
  -d, --lastday LAST_DAY        set date of last password change to LAST_DAY
  -E, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -h, --help                    display this help message and exit
  -I, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
```

```
  -l, --list                    show account aging information
  -m, --mindays MIN_DAYS        set minimum number of days before password
                                change to MIN_DAYS
  -M, --maxdays MAX_DAYS        set maximim number of days before password
                                change to MAX_DAYS
  -R, --root CHROOT_DIR         directory to chroot into
  -W, --warndays WARN_DAYS      set expiration warning days to WARN_DAYS
```

Configuration

La commande **useradd** est configurée par le fichier **/etc/default/useradd**. Pour consulter ce fichier, saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

```
[root@centos6 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

```
[root@centos7 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Dans ce fichier, nous trouvons les directives suivantes :

- **GROUP** - identifie le groupe principal par défaut de l'utilisateur quand l'option **-N** est utilisée avec la commande **useradd**. Dans le cas contraire le groupe principal est soit le groupe spécifié par l'option **-g** de la commande, soit un nouveau groupe au même nom que l'utilisateur,
- **HOME** - indique que le répertoire personnel de l'utilisateur sera créé dans le répertoire **home** lors de la création du compte si cette option a été activée dans le fichier **/etc/login.defs**,
- **INACTIVE** - indique le nombre de jours d'inactivité après l'expiration d'un mot de passe avant que le compte soit verrouillé. La valeur de -1 désactive cette directive,
- **EXPIRE** - sans valeur, cette directive indique que le mot de passe de l'utilisateur n'expire jamais,
- **SHELL** - renseigne le shell de l'utilisateur,
- **SKEL** - indique le répertoire contenant les fichiers qui seront copiés vers le répertoire personnel de l'utilisateur, si ce répertoire est créé lors de la création de l'utilisateur,
- **CREATE_MAIL_SPOOL** - indique si oui ou non une boite mail interne au système sera créée pour l'utilisateur.

Cette même information peut être visualisée en exécutant la commande **useradd** avec l'option **-D** :

```
[root@centos5 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

```
[root@centos6 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

```
[root@centos7 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Pour consulter la liste des fichiers dans **/etc/skel**, saisissez la commande suivante :

```
[root@centos5 ~]# ls -la /etc/skel
total 64
drwxr-xr-x   3 root root  4096 août 25 13:30 .
drwxr-xr-x 102 root root 12288 août 25 14:06 ..
-rw-r--r--   1 root root    33 juil. 10  2013 .bash_logout
-rw-r--r--   1 root root   176 juil. 10  2013 .bash_profile
-rw-r--r--   1 root root   124 juil. 10  2013 .bashrc
-rw-r--r--   1 root root   515 avril 28  2011 .emacs
drwxr-xr-x   4 root root  4096 août 25 13:30 .mozilla
```

```
[root@centos6 ~]# ls -la /etc/skel
total 36
drwxr-xr-x.   4 root root  4096 28 juil. 14:27 .
drwxr-xr-x. 113 root root 12288 13 déc.  06:48 ..
```

```
-rw-r--r--.   1 root root    18 30 mai    2011 .bash_logout
-rw-r--r--.   1 root root   176 30 mai    2011 .bash_profile
-rw-r--r--.   1 root root   124 30 mai    2011 .bashrc
drwxr-xr-x.   2 root root  4096 12 nov.   2010 .gnome2
drwxr-xr-x.   4 root root  4096 28 juil. 14:19 .mozilla
```

```
[root@centos7 ~]# ls -la /etc/skel
total 24
drwxr-xr-x.   3 root root   74 Jun  4 09:50 .
drwxr-xr-x. 131 root root 8192 Sep  4 12:18 ..
-rw-r--r--.   1 root root   18 Mar  5 23:06 .bash_logout
-rw-r--r--.   1 root root  193 Mar  5 23:06 .bash_profile
-rw-r--r--.   1 root root  231 Mar  5 23:06 .bashrc
drwxr-xr-x.   4 root root   37 Mar  8 13:41 .mozilla
```

Important : Notez que sous RHEL le fichier **.bash_profile** remplace le fichier **.profile**.

Pour connaître l'UID, le GID et l'appartenance aux groupes d'un utilisateur, il convient d'utiliser la commande **id**. Saisissez la commande suivante :

```
[root@centos5 ~]# id trainee
uid=500(trainee) gid=500(trainee) groupes=500(trainee) context=user_u:system_r:unconfined_t
```

```
[root@centos6 ~]# id trainee
uid=500(trainee) gid=500(trainee) groupes=500(trainee)
```

```
[root@centos7 ~]# id trainee
uid=1000(trainee) gid=1000(trainee) groups=1000(trainee)
```

Pour seulement connaître les groupes d'un utilisateur, il convient d'utiliser la commande **groups**. Saisissez la commande suivante :

```
[root@centos5 ~]# groups trainee
```

```
trainee : trainee
```

```
[root@centos6 ~]# groups trainee
trainee : trainee
```

```
[root@centos7 ~]# groups trainee
trainee : trainee
```

Les valeurs minimales de l'UID et du GID utilisés par défaut lors de la création d'un utilisateur sont stipulées dans le fichier **/etc/login.defs** :

```
...
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  500
UID_MAX                60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  500
GID_MAX                60000
...
```

```
...
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN           500
UID_MAX         60000

#
# Min/max values for automatic gid selection in groupadd
#
```

```
GID_MIN           500
GID_MAX         60000
...
```

```
...
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
SYS_UID_MIN               201
SYS_UID_MAX               999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
SYS_GID_MIN               201
SYS_GID_MAX               999
...
```

LAB #1 - Gérer les Utilisateurs et les Groupes

Créez maintenant trois groupes **groupe1**, **groupe2** et **groupe3**. La valeur du GID du groupe **groupe3** doit être de **1807** :

```
[root@centos7 ~]# groupadd groupe1; groupadd groupe2; groupadd -g 1807 groupe3
```

Créez maintenant trois utilisateurs **fenestros1**, **fenestros2** et **fenestros3**. Les trois utilisateurs ont pour groupe principal **groupe1**, **groupe2** et **groupe3** respectivement. **fenestros2** est aussi membre des groupes **groupe1** et **groupe3**. **fenestros1** à un GECOS de **tux1** :

```
[root@centos7 ~]# useradd -g groupe2 fenestros2; useradd -g 1807 fenestros3; useradd -g groupe1 fenestros1
[root@centos7 ~]# usermod -G groupe1,groupe3 fenestros2
[root@centos7 ~]# usermod -c "tux1" fenestros1
```

En consultant votre fichier **/etc/passwd**, vous obtiendrez un résultat similaire à celui-ci:

```
[root@centos7 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
...
fenestros2:x:1001:1002::/home/fenestros2:/bin/bash
fenestros3:x:1002:1807::/home/fenestros3:/bin/bash
fenestros1:x:1003:1001:tux1:/home/fenestros1:/bin/bash
```

En regardant votre fichier **/etc/group**, vous obtiendrez un résultat similaire à celui-ci:

```
[root@centos7 ~]# cat /etc/group
root:x:0:
...
groupe1:x:1001:fenestros2
groupe2:x:1002:
groupe3:x:1807:fenestros2
```

Créez le mot de passe **fenestros** pour le **groupe3** :

```
[root@centos7 ~]# gpasswd groupe3
Changing the password for group groupe3
New Password: fenestros
Re-enter new password: fenestros
```

Important : Notez que les mots de passe saisis ne seront **pas** visibles.

Consultez le fichier **/etc/gshadow** :

```
[root@centos7 ~]# cat /etc/gshadow
root:::
...
groupe1:!::fenestros2
groupe2:!::
groupe3:$6$hBRhs6HH9izNw2h$t751fnVXMstGtzTX.gwhgtdxewlSdfXTmWY.ZuePu6yoKkPfsSSciKku.4H7SSQvLERlixsCCsjcUHoYh96Pj1
::fenestros2
```

Important : Notez la présence du mot de passe crypté pour le **groupe3**.

Nommez maintenant **fenestros1** administrateur du **groupe3** :

```
[root@centos7 ~]# gpasswd -A fenestros1 groupe3
```

Consultez le fichier **/etc/gshadow** de nouveau :

```
[root@centos7 ~]# cat /etc/gshadow
root:::
...
groupe1:!::fenestros2
groupe2:!::
groupe3:$6$hBRhs6HH9izNw2h$t751fnVXMstGtzTX.gwhgtdxewlSdfXTmWY.ZuePu6yoKkPfsSSciKku.4H7SSQvLERlixsCCsjcUHoYh96Pj1
:fenestros1:fenestros2
```

Important : L'utilisateur **fenestros1** peut maintenant administrer le groupe **groupe3** en y ajoutant ou en y supprimant des utilisateurs à condition de connaître le mot de passe du groupe.

Essayez maintenant de supprimer le groupe **groupe3** :

```
[root@centos7 ~]# groupdel groupe3
groupdel: cannot remove the primary group of user 'fenestros3'
```

Important : En effet, vous ne pouvez pas supprimer un groupe tant qu'un utilisateur le possède comme son groupe principal.

Supprimez donc l'utilisateur **fenestros3** :

```
[root@centos7 ~]# userdel fenestros3
```

Ensuite essayez de supprimer le groupe **groupe3** :

```
[root@centos7 ~]# groupdel groupe3
```

Important : Notez que cette fois-ci la commande est exécutée sans erreur.

Le fait de supprimer un utilisateur **sans** l'option **-r** implique que le répertoire personnel de l'utilisateur demeure sur la machine.

Saisissez la commande suivante sous RHEL 7 pour vérifier :

```
[root@centos7 ~]# ls -ld /home/fenestros3
drwx------. 3 1002 1807 74 Oct 15 18:15 /home/fenestros3
```

Pour supprimer les fichiers de cet utilisateur, il convient de saisir la commande suivante :

```
[root@centos7 ~]# find /home -user 1002 -exec rm -rf {} \;
find: ‘/home/fenestros3’: No such file or directory
```

```
[root@centos7 ~]# ls -ld /home/fenestros3
ls: cannot access /home/fenestros3: No such file or directory
```

> **Important** : La commande **find** est lancée d'une manière itérative. L'erreur est normale car quand la commande **find** ne trouve plus de fichiers à supprimer, elle s'arrête avec un code retour de 2.

Créez maintenant les mots de passe pour **fenestros1** et **fenestros2**. Indiquez un mot de passe identique au nom du compte :

```
[root@centos7 ~]# passwd fenestros1
Changing password for user fenestros1.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos7 ~]# passwd fenestros2
Changing password for user fenestros2.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
```

> **Important** : Notez que les règles gouvernant l'utilisation des mots de passe ne sont pas appliqués aux utilisateurs créés par root. Notez aussi que les mots de passe saisis ne seront **PAS** visibles.

LAB #2 - Forcer l'utilisation des mots de passe complexe avec PAM sous RHEL/CentOS 6

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.

Les fichiers de configuration se trouvent dans le répertoire **/etc/pam.d** :

```
[root@centos6 ~]# ls /etc/pam.d
atd                   halt              smartcard-auth-ac
authconfig            ksu               smtp
authconfig-gtk        login             smtp.postfix
authconfig-tui        newrole           sshd
chfn                  other             su
chsh                  passwd            sudo
config-util           password-auth     sudo-i
crond                 password-auth-ac  su-l
cups                  polkit-1          system-auth
cvs                   poweroff          system-auth-ac
eject                 ppp               system-config-authentication
fingerprint-auth      reboot            system-config-date
fingerprint-auth-ac   remote            system-config-kdump
gdm                   run_init          system-config-keyboard
gdm-autologin         runuser           system-config-network
gdm-fingerprint       runuser-l         system-config-network-cmd
gdm-password          setup             system-config-users
gnome-screensaver     smartcard-auth    xserver
```

Ces fichiers ont une structure spécifique et sont nommés d'après le service ou l'application qu'ils contrôlent. Leur contenu fait appel à des modules qui se trouvent dans le répertoire **/lib/security** :

```
[root@centos6 ~]# ls /lib/security
pam_access.so          pam_krb5.so             pam_sepermit.so
pam_cap.so             pam_lastlog.so          pam_shells.so
pam_chroot.so          pam_ldap.so             pam_smbpass.so
pam_ck_connector.so    pam_limits.so           pam_sss.so
pam_console.so         pam_listfile.so         pam_stress.so
```

```
pam_cracklib.so       pam_localuser.so         pam_succeed_if.so
pam_debug.so          pam_loginuid.so          pam_tally2.so
pam_deny.so           pam_mail.so              pam_time.so
pam_echo.so           pam_mkhomedir.so         pam_timestamp.so
pam_env.so            pam_motd.so              pam_tty_audit.so
pam_exec.so           pam_namespace.so         pam_umask.so
pam_faildelay.so      pam_nologin.so           pam_unix_acct.so
pam_filter            pam_oddjob_mkhomedir.so  pam_unix_auth.so
pam_filter.so         pam_passwdqc.so          pam_unix_passwd.so
pam_fprintd.so        pam_permit.so            pam_unix_session.so
pam_ftp.so            pam_postgresok.so        pam_unix.so
pam_gnome_keyring.so  pam_pwhistory.so         pam_userdb.so
pam_group.so          pam_rhosts.so            pam_warn.so
pam_issue.so          pam_rootok.so            pam_wheel.so
pam_keyinit.so        pam_securetty.so         pam_winbind.so
pam_krb5              pam_selinux_permit.so    pam_xauth.so
pam_krb5afs.so        pam_selinux.so
```

Les modules les plus importants sont :

Module	**Description**
pam_listfile.so	Ce module est utilisé pour consulter un fichier spécifique pour vérifier les authiorisations. Par exemple, le service ftp utilise ce module pour consulter le fichier **/etc/ftpusers** qui contient une liste d'utilisateurs qui ne sont **pas** autorisés à se connecter au serveur ftp.
pam_access.so	Ce module est utilisé pour interdire l'accès aux services sécurisés par des hôtes non-autorisés.
pam_nologin.so	Ce module interdit les connexions d'utilisteurs, autre que root, dans le cas où le fichier **/etc/nologin** est présent.
pam_securetty.so	Ce module interdit des connexions de root à partir des périphériques tty qui ne sont pas listés dans le fichier **/etc/securetty**.
pam_cracklib.so	Ce module est utilisé pour vérifier le mot de passe d'un utilisateur
pam_unix.so	Ce module est utilisé pour vérifier les informations suivantes ; expire, last_change, max_change, min_change, warn_change.
pam_limits.so	Ce module implémente les limites des ressources détaillées dans le fichier **/etc/security/limits.conf** et dans les fichiers ***.conf** trouvés dans le répertoire **/etc/security/limits.d/**.
pam_echo.so	Ce module présente le contenu du fichier passé en argument à tout utilisateur lors de sa connexion.

Chaque fichier dans /etc/pam.d contient les règles PAM utilisées pendant l'authentification. Ouvrez le fichier **login** :

```
[root@centos6 ~]# cat /etc/pam.d/login
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth       include      system-auth
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
session    optional     pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
-session   optional     pam_ck_connector.so
```

La première ligne de ce fichier est un commentaire qui spécifie que le fichier est conforme à la spécification PAM 1.0.

Ce fichier, tout comme les autres, est ensuite structuré de la façon suivante :

- Une module par ligne,
- Quatre champs séparés par un espace dans chaque règle dont les trois premières sont obligatoires.

Le **premier champs** est le ***type de module***. Il en existe quatre :

Type	**Description**
auth	Utilisé pour authentifier un utilisateur ou les pré-requis système (par exemple /etc/nologin)
account	Utilisé pour vérifier si l'utilisateur peut s'authentifier (par exemple la validité du compte)
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 (par exemple monter un répertoire)

Le **deuxième 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
include	Ce control-flag permet d'inclure toutes les lignes du même *type de module* se trouvant dans le fichier spécifié en argument

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

Le **quatrième champs** contient éventuellement les **arguments**.

Ouvrez maintenant le fichier **system-auth** :

```
[root@centos6 ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
```

```
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

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

Utiliser des Mots de Passe Complexe

La complexité des mots de passe est gérée par le module **pam_cracklib.so**. Afin de mettre en place une politique de mots de passe complexe, il convient de modifier la ligne :

```
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
```

en

```
password    requisite     pam_cracklib.so try_first_pass retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-2
ocredit=-1
```

Dans ce cas, le mot de passe doit être long de 8 caractères et doit contenir au moins un caractère minuscule, un caractère majuscule, deux chiffres et un caractère spécial.

Configuration

Certains modules de PAM peuvent être configurés grâce aux fichiers présents dans le répertoire **/etc/security** :

```
[root@centos6 ~]# ls /etc/security
access.conf       console.perms    limits.d        opasswd
chroot.conf       console.perms.d  namespace.conf  pam_env.conf
```

```
console.apps      group.conf       namespace.d     sepermit.conf
console.handlers  limits.conf      namespace.init  time.conf
```

Parmi les fichiers cités on note ceux qui peuvent être utilisés pour configurer les modules suivants :

Fichier/*Répertoire*	**Description**
access.conf	Utilisé par le module pam_access.so
console.apps	Utilisés par le module pam_console.so
console.perms	Utilisé par le module pam_console.so
console.perms.d	Utilisé par le module pam_console.so
group.conf	Utilisés par le module pam_group.so
limits.conf	Utilisé par le module pam_limits.so
pam_env.conf	Utilisé par le module pam_env.so
time.conf	Utilisé par le module pam_time.so

A faire : Passez en revue chacun de ces fichiers.

Dernièrement, PAM propose une solution pour toutes les applications ne disposant pas de leurs propres fichiers de configuration PAM. Cette solution prend la forme du fichier **/etc/pam.d/other** :

```
[root@centos6 ~]# cat /etc/pam.d/other
#%PAM-1.0
auth     required       pam_deny.so
account  required       pam_deny.so
password required       pam_deny.so
session  required       pam_deny.so
```

LAB #3 - Forcer l'utilisation des mots de passe complexe avec PAM sous RHEL/CentOS 7

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.

Les fichiers de configuration se trouvent dans le répertoire **/etc/pam.d** :

```
[root@centos7 ~]# ls /etc/pam.d
atd                     login              smtp
chfn                    other              smtp.postfix
chsh                    passwd             sshd
config-util             password-auth      su
crond                   password-auth-ac   sudo
cups                    pluto              sudo-i
fingerprint-auth        polkit-1           su-l
fingerprint-auth-ac     postlogin          system-auth
gdm-autologin           postlogin-ac       system-auth-ac
gdm-fingerprint         ppp                system-config-language
gdm-launch-environment  remote             systemd-user
gdm-password            runuser            vlock
gdm-pin                 runuser-l          vmtoolsd
gdm-smartcard           setup              xserver
ksu                     smartcard-auth
liveinst                smartcard-auth-ac
```

Ces fichiers ont une structure spécifique et sont nommés d'après le service ou l'application qu'ils contrôlent. Leur contenu fait appel à des modules qui se trouvent dans le répertoire **/lib64/security** :

```
[root@centos7 ~]# ls /lib64/security
pam_access.so         pam_krb5afs.so          pam_selinux.so
pam_cap.so            pam_krb5.so             pam_sepermit.so
pam_chroot.so         pam_lastlog.so          pam_shells.so
pam_console.so        pam_limits.so           pam_sss.so
pam_cracklib.so       pam_listfile.so         pam_stress.so
pam_debug.so          pam_localuser.so        pam_succeed_if.so
pam_deny.so           pam_loginuid.so         pam_systemd.so
```

```
pam_echo.so            pam_mail.so              pam_tally2.so
pam_env.so             pam_mkhomedir.so         pam_time.so
pam_exec.so            pam_motd.so              pam_timestamp.so
pam_faildelay.so       pam_namespace.so         pam_tty_audit.so
pam_faillock.so        pam_nologin.so           pam_umask.so
pam_filter             pam_oddjob_mkhomedir.so  pam_unix_acct.so
pam_filter.so          pam_permit.so            pam_unix_auth.so
pam_fprintd.so         pam_postgresok.so        pam_unix_passwd.so
pam_ftp.so             pam_pwhistory.so         pam_unix_session.so
pam_gnome_keyring.so   pam_pwquality.so         pam_unix.so
pam_group.so           pam_rhosts.so            pam_userdb.so
pam_issue.so           pam_rootok.so            pam_warn.so
pam_keyinit.so         pam_securetty.so         pam_wheel.so
pam_krb5               pam_selinux_permit.so    pam_xauth.so
```

Les modules les plus importants sont :

Module	**Description**
pam_access.so	Ce module est utilisé pour interdire l'accès aux services sécurisés par des hôtes non-autorisés.
pam_echo.so	Ce module présente le contenu du fichier passé en argument à tout utilisateur lors de sa connexion.
pam_limits.so	Ce module implémente les limites des ressources détaillées dans le fichier **/etc/security/limits.conf** et dans les fichiers ***.conf** trouvés dans le répertoire **/etc/security/limits.d/**.
pam_listfile.so	Ce module est utilisé pour consulter un fichier spécifique pour vérifier les authiorisations. Par exemple, le service ftp utilise ce module pour consulter le fichier **/etc/ftpusers** qui contient une liste d'utilisateurs qui ne sont **pas** autorisés à se connecter au serveur ftp.
pam_nologin.so	Ce module interdit les connexions d'utilisteurs, autre que root, dans le cas où le fichier **/etc/nologin** est présent.
pam_pwquality.so	Ce module est utilisé pour vérifier la qualité du mot de passe d'un utilisateur
pam_securetty.so	Ce module interdit des connexions de root à partir des périphériques tty qui ne sont pas listés dans le fichier **/etc/securetty**.
pam_unix.so	Ce module est utilisé pour vérifier les informations suivantes ; expire, last_change, max_change, min_change, warn_change.

Chaque fichier dans /etc/pam.d contient les règles PAM utilisées pendant l'authentification. Ouvrez le fichier **login** :

```
[root@centos7 ~]# cat /etc/pam.d/login
#%PAM-1.0
```

```
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth       substack     system-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
session    optional     pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    include      postlogin
-session   optional     pam_ck_connector.so
```

La première ligne de ce fichier est un commentaire qui spécifie que le fichier est conforme à la spécification PAM 1.0.

Ce fichier, tout comme les autres, est ensuite structuré de la façon suivante :

- Une module par ligne,
- Quatre champs séparés par un espace dans chaque règle dont les trois premières sont obligatoires.

Le **premier champs** est le ***type de module***. Il en existe quatre :

Type	**Description**
auth	Utilisé pour authentifier un utilisateur ou les pré-requis système (par exemple /etc/nologin)
account	Utilisé pour vérifier si l'utilisateur peut s'authentifier (par exemple la validité du compte)
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 (par exemple monter un répertoire)

Le **deuxième 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
include	Ce control-flag permet d'inclure toutes les lignes du même *type de module* se trouvant dans le fichier spécifié en argument

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

Le **quatrième champs** contient éventuellement les **arguments**.

Ouvrez maintenant le fichier **password-auth-ac** :

```
[root@centos7 ~]# cat /etc/pam.d/password-auth-ac
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so
```

```
session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

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

Utiliser des Mots de Passe Complexe

La complexité des mots de passe est gérée par le module **pam_pwquality.so**. Afin de mettre en place une politique de mots de passe complexe, il convient de modifier la ligne :

```
password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
```

en

```
password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 minlen=8 lcredit=-1 ucredit=-1
dcredit=-2 ocredit=-1
```

Dans ce cas, le mot de passe doit être long de 8 caractères et doit contenir au moins un caractère minuscule, un caractère majuscule, deux chiffres et un caractère spécial.

Configuration

Certains modules de PAM peuvent être configurés grâce aux fichiers présents dans le répertoire **/etc/security** :

```
[root@centos7 ~]# ls /etc/security
access.conf       console.perms    limits.d        opasswd         time.conf
chroot.conf       console.perms.d  namespace.conf  pam_env.conf
console.apps      group.conf       namespace.d     pwquality.conf
```

```
console.handlers  limits.conf      namespace.init  sepermit.conf
```

Parmi les fichiers cités on note ceux qui peuvent être utilisés pour configurer les modules suivants :

Fichier/*Répertoire*	**Description**
access.conf	Utilisé par le module pam_access.so
console.apps	Utilisés par le module pam_console.so
console.perms	Utilisé par le module pam_console.so
console.perms.d	Utilisé par le module pam_console.so
group.conf	Utilisés par le module pam_group.so
limits.conf	Utilisé par le module pam_limits.so
pam_env.conf	Utilisé par le module pam_env.so
pwquality.conf	Utilisé par le module pam_cracklib.so
time.conf	Utilisé par le module pam_time.so

A faire : Passez en revue chacun de ces fichiers.

Dernièrement, PAM propose une solution pour toutes les applications ne disposant pas de leurs propres fichiers de configuration PAM. Cette solution prend la forme du fichier **/etc/pam.d/other** :

```
[root@centos7 ~]# cat /etc/pam.d/other
#%PAM-1.0
auth     required       pam_deny.so
account  required       pam_deny.so
password required       pam_deny.so
session  required       pam_deny.so
```

su et su -

Vous allez maintenant devenir **fenestros2**, d'abord sans l'environnement de **fenestros2** puis avec l'environnement de **fenestros2**.

Contrôlez votre répertoire courant de travail :

```
[root@centos7 ~]# pwd
/root
```

Pour devenir **fenestros2 sans** son environnement, saisissez la commande suivante :

```
[root@centos7 ~]# su fenestros2
```

Contrôlez votre répertoire courant de travail :

```
[fenestros2@centos7 root]$ pwd
/root
```

Vous noterez que vous êtes toujours dans le répertoire **/root**. Ceci indique que vous avez gardé l'environnement de **root**.

> **Important** : L'environnement d'un utilisateur inclut donc, entre autre, le répertoire personnel de l'utilisateur ainsi que la valeur de la variable système **PATH**.

Saisissez la commande suivante pour redevenir **root** :

```
[fenestros2@centos7 root]$ exit
exit
```

Saisissez la commande suivante pour redevenir **fenestros2** :

```
[root@centos7 ~]# su - fenestros2
Last login: Thu Oct 15 18:30:54 CEST 2015 on pts/0
```

Contrôlez votre répertoire courant de travail :

```
[fenestros2@centos7 ~]$ pwd
/home/fenestros2
```

Vous noterez que vous êtes maintenant dans le répertoire **/home/fenestros2**. Ceci indique que vous avez l'environnement de **fenestros2**.

> **Important** : Notez que **root** peut devenir n'importe quel utilisateur **sans** avoir besoin de connaître son mot de passe.

sudo

> **Important** : Afin de mettre en pratique les exemples qui suivent, vous devez être connecté à votre système en tant que root. Tapez donc la commande **exit** pour sortir de l'environnement de **fenestros2**.

La commande **sudo** permet à un utilisateur autorisé d'exécuter une commande en tant que **root** ou en tant qu'un autre utilisateur. Lors de l'exécution de la commande, l'UID et le GID éffectifs et réels sont ceux de l'identité de l'utilisateur cible. L'utilisation de la commande **sudo** est une façon simple de déléguer des tâches administratives à d'autres utilisateurs sans communiquer le mot de passe de **root** et sans placer un SUID bit sur l'exécutable. La commande **sudo** est configurée grâce au fichier **/etc/sudoers**.

Saisissez la commande suivante :

```
[root@centos5 ~]# cat /etc/sudoers
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

```
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhap using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
## These are groups of related commands...

## Networking
#Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables,
/usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
#Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
#Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
```

```
#Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
#Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
#Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
#Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
#Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

#
# Disable "ssh hostname sudo <cmd>", because it will show the password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

#
# Refuse to run if unable to disable echo on the tty. This setting should also be
# changed in order to be able to use sudo without a tty. See requiretty above.
#
Defaults   !visiblepw

Defaults    env_reset
Defaults    env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR \
                        LS_COLORS MAIL PS1 PS2 QTDIR USERNAME \
                        LANG LC_ADDRESS LC_CTYPE LC_COLLATE LC_IDENTIFICATION \
                        LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC \
                        LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS \
```

```
                        _XKB_CHARSET XAUTHORITY"

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now
```

```
[root@centos6 ~]# cat /etc/sudoers
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

```
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
## These are groups of related commands...

## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables,
/usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
```

```
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

#
# Disable "ssh hostname sudo <cmd>", because it will show the password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

#
# Preserving HOME has security implications since many programs
# use it when searching for configuration files.
#
Defaults    always_set_home

Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"
```

```
#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##  user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)     ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel    ALL=(ALL)    ALL

## Same thing without a password
# %wheel    ALL=(ALL)    NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom
```

```
## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now
```

```
[root@centos7 ~]# cat /etc/sudoers
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
## These are groups of related commands...

## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables,
/usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
```

```
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

#
# Disable "ssh hostname sudo <cmd>", because it will show the password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

#
# Refuse to run if unable to disable echo on the tty. This setting should also be
# changed in order to be able to use sudo without a tty. See requiretty above.
#
Defaults   !visiblepw
```

```
#
# Preserving HOME has security implications since many programs
# use it when searching for configuration files. Note that HOME
# is already set when the the env_reset option is enabled, so
# this option is only effective for configurations where either
# env_reset is disabled or HOME is present in the env_keep list.
#
Defaults    always_set_home

Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##  user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
```

```
root    ALL=(ALL)     ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)    ALL

## Same thing without a password
# %wheel    ALL=(ALL)    NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
```

> **Important** : Notez la présence de la ligne en commentaire **# %wheel ALL=(ALL) ALL**. Cette ligne possède le format **Qui Où = (En tant que qui) Quoi**. La ligne implique donc que les membres du groupe **wheel** peuvent exécuter à partir de n'importe quel hôte et en tant que n'importe quel utilisateur, toutes les commandes du système. Dans ce fichier donc, un groupe est référencé par un **%**. Un nom sans ce caractère est forcément un utilisateur. Pour éditer le fichier **/etc/sudoers**, il est **nécessaire** d'utiliser la commande **visudo**.
