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

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**.

LSF106 - Gestion des Utilisateurs

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

```
SLES12SP1:~ # 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:
#
#       compat                  Use compatibility setup
#       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
#       [NOTFOUND=return]       Stop searching if not found so far
#
# For more information, please read the nsswitch.conf.5 manual page.
#

# passwd: files nis
# shadow: files nis
# group:  files nis

passwd: compat
group:  compat

hosts:      files dns
networks:   files dns

services:   files
protocols:  files
rpc:        files
ethers:     files
netmasks:   files
netgroup:   files nis
```

```
publickey:  files

bootparams: files
automount:  files nis
aliases:    files
```

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 :

```
SLES12SP1:~ # getent passwd trainee
trainee:x:1000:100:trainee:/home/trainee:/bin/bash
```

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

```
SLES12SP1:~ # 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 :

```
SLES12SP1:~ # getent passwd
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
ftpsecure:x:488:65534:Secure FTP User:/var/lib/empty:/bin/false
games:x:12:100:Games account:/var/games:/bin/bash
gdm:x:486:485:Gnome Display Manager daemon:/var/lib/gdm:/bin/false
```

```
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:499:499:User for D-Bus:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
nscd:x:496:495:User for nscd:/run/nscd:/sbin/nologin
ntp:x:74:492:NTP daemon:/var/lib/ntp:/bin/false
openslp:x:494:2:openslp daemon:/var/lib/empty:/sbin/nologin
polkitd:x:497:496:User for polkitd:/var/lib/polkit:/sbin/nologin
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
pulse:x:490:489:PulseAudio daemon:/var/lib/pulseaudio:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
rpc:x:495:65534:user for rpcbind:/var/lib/empty:/sbin/nologin
rtkit:x:491:490:RealtimeKit:/proc:/bin/false
scard:x:487:487:Smart Card Reader:/var/run/pcscd:/usr/sbin/nologin
sshd:x:498:498:SSH daemon:/var/lib/sshd:/bin/false
statd:x:489:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
usbmux:x:493:65534:usbmuxd daemon:/var/lib/usbmuxd:/sbin/nologin
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
vnc:x:492:491:user for VNC:/var/lib/empty:/sbin/nologin
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
trainee:x:1000:100:trainee:/home/trainee:/bin/bash
```

Les Fichiers /etc/group et /etc/gshadow

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

```
SLES12SP1:~ # cat /etc/group
at:x:25:
audio:x:17:
bin:x:1:daemon
```

```
brlapi:x:494:
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:
disk:x:6:
floppy:x:19:
ftp:x:49:
games:x:40:
gdm:x:485:
kmem:x:9:
lock:x:54:
lp:x:7:
mail:x:12:postfix
maildrop:x:59:postfix
man:x:62:
messagebus:x:499:
modem:x:43:
news:x:13:
nobody:x:65533:
nogroup:x:65534:nobody
nscd:x:495:
ntadmin:x:71:
ntp:x:492:
polkitd:x:496:
postfix:x:51:
public:x:32:
pulse:x:489:
pulse-access:x:488:
root:x:0:
rtkit:x:490:
scard:x:487:
shadow:x:15:
sshd:x:498:
```

```
sys:x:3:
systemd-journal:x:493:
tape:x:497:
trusted:x:42:
tty:x:5:
utmp:x:22:
uucp:x:14:
video:x:33:gdm
vnc:x:491:
wheel:x:10:
winbind:x:486:
www:x:8:
xok:x:41:
users:x:100:
```

Important : Notez que la valeur du GID du groupe root est toujours de 0 et les GID des utilisateurs normaux est de **100**. Les GID des comptes système sont inclus entre 100 et 499.

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 indiquait historiquement que le système utilisait le fichier **/etc/gshadow** pour stocker des mots de passe cryptés. Depuis la version 9.1 d'openSUSE l'utilisation de ce fichier a été abandonné et les éventuels mots de passe des groupes sont inscrits directement dans le fichier **/etc/group**. 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. Sous les versions actuelles donc de SLES et d'openSUSE, les deux caractères **x** et **!** produisent essentiellement le même résultat,
- 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**.

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

```
SLES12SP1:~ # grpck -r
```

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

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 :

```
SLES12SP1:~ # cat /etc/passwd
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
ftpsecure:x:488:65534:Secure FTP User:/var/lib/empty:/bin/false
games:x:12:100:Games account:/var/games:/bin/bash
gdm:x:486:485:Gnome Display Manager daemon:/var/lib/gdm:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:499:499:User for D-Bus:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
```

```
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
nscd:x:496:495:User for nscd:/run/nscd:/sbin/nologin
ntp:x:74:492:NTP daemon:/var/lib/ntp:/bin/false
openslp:x:494:2:openslp daemon:/var/lib/empty:/sbin/nologin
polkitd:x:497:496:User for polkitd:/var/lib/polkit:/sbin/nologin
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
pulse:x:490:489:PulseAudio daemon:/var/lib/pulseaudio:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
rpc:x:495:65534:user for rpcbind:/var/lib/empty:/sbin/nologin
rtkit:x:491:490:RealtimeKit:/proc:/bin/false
scard:x:487:487:Smart Card Reader:/var/run/pcscd:/usr/sbin/nologin
sshd:x:498:498:SSH daemon:/var/lib/sshd:/bin/false
statd:x:489:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
usbmux:x:493:65534:usbmuxd daemon:/var/lib/usbmuxd:/sbin/nologin
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
vnc:x:492:491:user for VNC:/var/lib/empty:/sbin/nologin
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
trainee:x:1000:100:trainee:/home/trainee:/bin/bash
```

Important : Notez que la valeur de l'UID de root est de **0** et que les UID des utilisateurs normaux commencent à **1000**. Les UID des comptes système sont inclus entre 100 et 499.

Chaque ligne dans ce fichier 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 :

```
SLES12SP1:~ # cat /etc/shadow
at:!:16922::::::
bin:*:16765::::::
daemon:*:16765::::::
ftp:*:16765::::::
ftpsecure:!:16922::::::
games:*:16765::::::
gdm:!:16922::::::
lp:*:16765::::::
mail:*:16765::::::
man:*:16765::::::
messagebus:!:16765::::::
news:*:16765::::::
nobody:*:16765::::::
nscd:!:16765::::::
ntp:!:16922::::::
openslp:!:16765::::::
polkitd:!:16765::::::
postfix:!:16922::::::
pulse:!:16922::::::
root:$6$g0tHJ9vyIfFt$rbm.rf7p6XZMxMqbqa/BGDeA7E7RkC9n89w8cWdpAxkUmwk7BPcMv7Zy9nVAn7f/7zQJzcRcsIqp5bRx1e8iX/:16922
::::::
rpc:!:16765::::::
rtkit:!:16922::::::
scard:!:16922::::::
sshd:!:16765::::::
statd:!:16922::::::
usbmux:!:16922::::::
uucp:*:16765::::::
vnc:!:16922::::::
wwwrun:*:16765::::::
trainee:$6$OZyVqj4ekgmu$Cw0T.n6gNv.vTdAT6dFxrrSeHW/V3r43jWFczPG0lxg5SB9iMUcQ6MFLz9NuTTas289xe/ULsJhE2HdJbraGA.:16
```

```
922:0:99999:7:::
```

Chaque ligne dans ce fichier 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 :

```
SLES12SP1:~ # pwck -r
user 'pulse': directory '/var/lib/pulseaudio' does not exist
user 'usbmux': directory '/var/lib/usbmuxd' 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

```
SLES12SP1:~ # 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

```
SLES12SP1:~ # 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

```
SLES12SP1:~ # 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

```
SLES12SP1:~ # newgrp --help
Usage: newgrp [-] [group]
```

gpasswd

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

Options de la commande

```
SLES12SP1:~ # 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
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

Code Retour	Description
12	Impossible de créer le répertoire personnel de l'utilisateur
13	Impossible de créer le spool mail de l'utilisateur
14	Impossible de mettre à jour SELinux

Options de la commande

```
SLES12SP1:~ # 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

```
SLES12SP1:~ # userdel --help
Usage: userdel [options] LOGIN

Options:
```

```
  -f, --force                   force removal of files,
                                even if not owned by 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

```
SLES12SP1:~ # 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

```
SLES12SP1:~ # passwd --help
Usage: passwd [options] [LOGIN]

Options:
  -a, --all                   report password status on all accounts
```

```
  -d, --delete                  delete the password for the named account
  -e, --expire                  force expire the password for the named account
  -h, --help                    display this help message and exit
  -k, --keep-tokens             change password only if expired
  -i, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -l, --lock                    lock the password of the named account
  -n, --mindays MIN_DAYS        set minimum number of days before password
                                change to MIN_DAYS
  -q, --quiet                   quiet mode
  -r, --repository REPOSITORY   change password in REPOSITORY repository
  -R, --root CHROOT_DIR         directory to chroot into
  -S, --status                  report password status on the named account
  -u, --unlock                  unlock the password of the named account
  -w, --warndays WARN_DAYS      set expiration warning days to WARN_DAYS
  -x, --maxdays MAX_DAYS        set maximum number of days before password
                                change to MAX_DAYS
```

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

```
SLES12SP1:~ # 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 :

```
SLES12SP1:~ # cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
NO_GROUPS=true
UMASK=022
GROUPS=
```

Dans ce fichier, nous trouvons les directives suivantes :

- **GROUP** - identifie le groupe principal par défaut de l'utilisateur quand sauf dans le cas où le groupe principal est spécifié par l'option **-g** de la commande,
- **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,
- **UMASK** - indique l'umask de l'utilisateur. Cette valeur prend le dessus sur la valeur indiqué dans le fichier **/etc/login.defs**,
- **GROUPS** - identifie le ou les groupes secondaire de l'utilisateur?

Cette même information peut être visualisée en utilisant la commande **useradd** :

```
SLES12SP1:~ # 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 :

```
SLES12SP1:~ # ls -la /etc/skel
total 36
drwxr-xr-x 1 root root  234 May  1  2016 .
drwxr-xr-x 1 root root 5200 Oct  8 04:01 ..
-rw------- 1 root root    0 May 18  1996 .bash_history
```

```
-rw-r--r-- 1 root root 1177 Sep 26  2014 .bashrc
drwx------ 1 root root    0 Sep 21  2014 .config
-rw-r--r-- 1 root root 1637 Sep 11  2014 .emacs
drwxr-xr-x 1 root root    0 Sep 21  2014 .fonts
-rw-r--r-- 1 root root  305 Aug 21  2015 .i18n
-rw-r--r-- 1 root root  861 Sep 11  2014 .inputrc
drwx------ 1 root root    0 Sep 21  2014 .local
-rw-r--r-- 1 root root 6043 Dec  5  2014 .muttrc
-rw-r--r-- 1 root root 1028 Sep 26  2014 .profile
-rw-r--r-- 1 root root 1952 Aug 21  2015 .xim.template
-rwxr-xr-x 1 root root 1112 Sep 22  2014 .xinitrc.template
drwxr-xr-x 1 root root    0 Sep 21  2014 bin
drwxr-xr-x 1 root root   20 May  1  2016 public_html
```

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

```
SLES12SP1:~ # id trainee
uid=1000(trainee) gid=100(users) groups=100(users)
```

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

```
SLES12SP1:~ # groups trainee
trainee : users
```

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
#
# SYS_UID_MIN to SYS_UID_MAX inclusive is the range for
# UIDs for dynamically allocated administrative and system accounts.
# UID_MIN to UID_MAX inclusive is the range of UIDs of dynamically
# allocated user accounts.
```

```
#
UID_MIN          1000
UID_MAX         60000
# System accounts
SYS_UID_MIN       100
SYS_UID_MAX       499

#
# Min/max values for automatic gid selection in groupadd
#
# SYS_GID_MIN to SYS_GID_MAX inclusive is the range for
# GIDs for dynamically allocated administrative and system groups.
# GID_MIN to GID_MAX inclusive is the range of GIDs of dynamically
# allocated groups.
#
GID_MIN          1000
GID_MAX         60000
# System accounts
SYS_GID_MIN       100
SYS_GID_MAX       499

#
```

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 **807** :

```
SLES12SP1:~ # groupadd groupe1; groupadd groupe2; groupadd -g 807 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** :

```
SLES12SP1:~ # useradd -g groupe2 fenestros2; useradd -g 807 fenestros3; useradd -g groupe1 fenestros1
SLES12SP1:~ # usermod -G groupe1,groupe3 fenestros2
SLES12SP1:~ # usermod -c "tux1" fenestros1
```

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

```
SLES12SP1:~ # cat /etc/passwd
...
fenestros2:x:1001:1001::/home/fenestros2:/bin/bash
fenestros3:x:1002:807::/home/fenestros3:/bin/bash
fenestros1:x:1003:1000::/home/fenestros1:/bin/bash
```

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

```
SLES12SP1:~ # cat /etc/group
...
groupe1:x:1000:fenestros2
groupe2:x:1001:
groupe3:x:807:fenestros2
```

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

```
SLES12SP1:~ # 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/group** :

```
SLES12SP1:~ # cat /etc/group
...
groupe1:x:1000:fenestros2
groupe2:x:1001:
groupe3:$6$YhGJG17yII$3iI7ivXhA.hKHeAS6aQ65Zvzx2qw32Z85VjqdfeYy7e8CVDAyxF3pNz91ACr9YUG0w/hikramJkvjhz5Fy9Bb.:807:
fenestros2
```

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

Devenez maintenant l'utilisateur **fenestros1** grâce à la commande **su** et contrôlez les groupes de l'utilisateur :

```
SLES12SP1:~ # su fenestros1
fenestros1@SLES12SP1:/root> groups
groupe1
```

Rejoignez le groupe3 et contrôlez vos groupes :

```
fenestros1@SLES12SP1:/root> newgrp groupe3
Password: fenestros
fenestros1@SLES12SP1:/root> groups
groupe3 groupe1
fenestros1@SLES12SP1:/root> id
uid=1003(fenestros1) gid=807(groupe3) groups=1000(groupe1),807(groupe3)
```

Important : Notez que le mot de passe saisi ne sera **pas** visible.

Sortez du terminal de fenestros1 du groupe3 et contrôlez de nouveau vos groupes :

```
fenestros1@SLES12SP1:/root> exit
exit
fenestros1@SLES12SP1:/root> groups
groupe1
fenestros1@SLES12SP1:/root> id
uid=1003(fenestros1) gid=1000(groupe1) groups=1000(groupe1)
```

Important : Notez ce qui se passe quand **fenestros1** saisit la commande **newgrp** en fournissant le mot de passe correct. Le système génère un terminal fils dans lequel le groupe principal de fenestros1 est devenu **groupe3**. Quand fenestros1 quitte le shell fils, son groupe principal redevient **groupe1**.

Dernièrement, redevenez **root** :

```
fenestros1@SLES12SP1:/root> exit
exit
SLES12SP1:~ #
```

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

```
SLES12SP1:~ # 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** :

```
SLES12SP1:~ # userdel fenestros3
no crontab for fenestros3
```

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

```
SLES12SP1:~ # 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 demeurre sur la machine.

Important : Dans notre cas les répertoires personnels des utilisateurs n'ont pas été créés parce que nous n'avons pas spécifié la création du répertoire lors de l'utilisation de la commande **useradd**.

Créez un utilisateur **test** en spécifiant la création de son répertoire personnel :

```
SLES12SP1:~ # useradd -m test
SLES12SP1:~ # ls -l /home
total 0
drwxr-xr-x 1 test    users 234 Oct  8 07:12 test
drwxr-xr-x 1 trainee users 456 May  3  2016 trainee
```

Créez maintenant les répertoires personnels de fenestros1 et fenestros2 :

```
SLES12SP1:~ # mkdir /home/fenestros1 /home/fenestros2
```

Copiez le contenu du répertoire **/etc/skel** dans les répertoires **/home/fenestros1** et **/home/fenestros2** :

```
SLES12SP1:~ # cp -r /etc/skel/* /home/fenestros1 && cp -r /etc/skel/.[a-zA-Z]* /home/fenestros1
SLES12SP1:~ # cp -r /etc/skel/* /home/fenestros2 && cp -r /etc/skel/.[a-zA-Z]* /home/fenestros2
```

Modifiez le propriétaire et le groupe pour les répertoires **/home/fenestros1** et **/home/fenestros2** :

```
SLES12SP1:~ # chown -R fenestros1:groupe1 /home/fenestros1
SLES12SP1:~ # chown -R fenestros2:groupe2 /home/fenestros2
```

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

```
SLES12SP1:~ # passwd fenestros1
New password: fenestros1
BAD PASSWORD: it is based on a dictionary word
Retype new password: fenestros1
passwd: password updated successfully
SLES12SP1:~ # passwd fenestros2
New password: fenestros2
BAD PASSWORD: it is based on a dictionary word
Retype new password: fenestros2
passwd: password 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

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** :

```
SLES12SP1:~ # ls /etc/pam.d
```

```
atd                                 cups                    runuser-l
chage                               gdm                     samba
chfn                                gdm-autologin           screen
chpasswd                            gdm-launch-environment  smtp
chsh                                gdm-password            sshd
common-account                      gnomesu-pam             su
common-account-pc                   groupadd                su-l
common-account.pam-config-backup    groupdel                sudo
common-auth                         groupmod                systemd-user
common-auth-pc                      init                    useradd
common-auth.pam-config-backup       login                   userdel
common-password                     newusers                usermod
common-password-pc                  other                   vlock
common-password.pam-config-backup   passwd                  vsftpd
common-session                      polkit-1                xdm
common-session-pc                   ppp                     xdm-np
common-session.pam-config-backup    remote                  xlock
crond                               runuser                 xscreensaver
```

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** :

```
SLES12SP1:~ # ls /lib/security
pam_access.so         pam_issue.so      pam_permit.so      pam_time.so
pam_cracklib.so       pam_keyinit.so    pam_pwcheck.so     pam_timestamp.so
pam_cryptpass.so      pam_lastlog.so    pam_pwhistory.so   pam_tty_audit.so
pam_debug.so          pam_limits.so     pam_rhosts.so      pam_umask.so
pam_deny.so           pam_listfile.so   pam_rootok.so      pam_unix.so
pam_echo.so           pam_localuser.so  pam_securetty.so   pam_unix2.so
pam_env.so            pam_loginuid.so   pam_selinux.so     pam_unix_acct.so
pam_exec.so           pam_mail.so       pam_sepermit.so    pam_unix_auth.so
pam_faildelay.so      pam_mkhomedir.so  pam_shells.so      pam_unix_passwd.so
pam_filter.so         pam_motd.so       pam_smbpass.so     pam_unix_session.so
pam_ftp.so            pam_mount.so      pam_stress.so      pam_warn.so
```

```
pam_gnome_keyring.so  pam_namespace.so  pam_succeed_if.so  pam_wheel.so
pam_group.so          pam_nologin.so    pam_systemd.so     pam_winbind.so
pam_homecheck.so      pam_opie.so       pam_tally2.so      pam_xauth.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** :

```
SLES12SP1:~ # cat /etc/pam.d/login
#%PAM-1.0
auth     requisite    pam_nologin.so
auth     [user_unknown=ignore success=ok ignore=ignore auth_err=die default=bad]pam_securetty.so
auth     include    common-auth
account  include    common-account
password include    common-password
session  required   pam_loginuid.so
session  include    common-session
#session  optional       pam_lastlog.so nowtmp showfailed
session  optional       pam_mail.so standard
```

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**.

Configuration

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

```
SLES12SP1:~ # ls /etc/security
access.conf  namespace.conf  pam_mount.conf.xml  sepermit.conf
group.conf   namespace.init  pam_winbind.conf    time.conf
limits.conf  pam_env.conf    pwquality.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
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.

Utiliser des Mots de Passe Complexe

La complexité des mots de passe est gérée par le module **pam_cracklib.so** et est configurée par l'édition du fichier **/etc/security/pwquality.conf** :

```
SLES12SP1:~ # cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
```

```
# Number of characters in the new password that must not be present in the
# old password.
# difok = 5
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 9
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
```

```
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for the words from the passwd entry GECOS string of the user.
# The check is enabled if the value is not 0.
# gecoscheck = 0
#
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
```

Pour que 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, il convient de modifier ce fichiar ainsi :

```
SLES12SP1:~ # cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 5
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -2
#
```

```
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for the words from the passwd entry GECOS string of the user.
# The check is enabled if the value is not 0.
# gecoscheck = 0
#
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
```

/etc/pam.d/other

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** :

```
SLES12SP1:~ # cat /etc/pam.d/other
#%PAM-1.0
auth     required    pam_warn.so
auth     required    pam_deny.so
account  required   pam_warn.so
account  required    pam_deny.so
password required   pam_warn.so
password required   pam_deny.so
session  required       pam_warn.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 :

```
SLES12SP1:~ # pwd
/root
```

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

```
SLES12SP1:~ # su fenestros2
fenestros2@SLES12SP1:/root>
```

Contrôlez votre répertoire courant de travail :

```
fenestros2@SLES12SP1:/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@SLES12SP1:/root> exit
exit
```

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

```
SLES12SP1:~ # su - fenestros2
fenestros2@SLES12SP1:~>
```

Contrôlez votre répertoire courant de travail :

```
fenestros2@SLES12SP1:~> 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

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 :

```
fenestros2@SLES12SP1:~> exit
logout
SLES12SP1:~ # cat /etc/sudoers
## sudoers file.
##
## This file MUST be edited with the 'visudo' command as root.
## Failure to use 'visudo' may result in syntax or file permission errors
## that prevent sudo from running.
##
## See the sudoers man page for the details on how to write a sudoers file.
##

##
## Host alias specification
##
## Groups of machines. These may include host names (optionally with wildcards),
## IP addresses, network numbers or netgroups.
# Host_Alias    WEBSERVERS = www1, www2, www3

##
## User alias specification
##
## Groups of users.  These may consist of user names, uids, Unix groups,
## or netgroups.
# User_Alias    ADMINS = millert, dowdy, mikef
```

```
##
## Cmnd alias specification
##
## Groups of commands.  Often used to group related commands together.
# Cmnd_Alias    PROCESSES = /usr/bin/nice, /bin/kill, /usr/bin/renice, \
#               /usr/bin/pkill, /usr/bin/top

##
## Defaults specification
##
## Prevent environment variables from influencing programs in an
## unexpected or harmful way (CVE-2005-2959, CVE-2005-4158, CVE-2006-0151)
Defaults always_set_home
## Path that will be used for every command run from sudo
Defaults secure_path="/usr/sbin:/usr/bin:/sbin:/bin"
Defaults env_reset
## Change env_reset to !env_reset in previous line to keep all environment variables
## Following list will no longer be necessary after this change

Defaults env_keep = "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 XDG_SESSION_COOKIE"
## Comment out the preceding line and uncomment the following one if you need
## to use special input methods. This may allow users to compromise  the root
## account if they are allowed to run commands without authentication.
#Defaults env_keep = "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 XDG_SESSION_COOKIE
XMODIFIERS GTK_IM_MODULE QT_IM_MODULE QT_IM_SWITCHER"

## Do not insult users when they enter an incorrect password.
Defaults !insults

##
## Uncomment to enable logging of a command's output, except for
## sudoreplay and reboot.  Use sudoreplay to play back logged sessions.
```

```
# Defaults log_output
# Defaults!/usr/bin/sudoreplay !log_output
# Defaults!/sbin/reboot !log_output

## In the default (unconfigured) configuration, sudo asks for the root password.
## This allows use of an ordinary user account for administration of a freshly
## installed system. When configuring sudo, delete the two
## following lines:
Defaults targetpw   # ask for the password of the target user i.e. root
ALL ALL=(ALL) ALL   # WARNING! Only use this together with 'Defaults targetpw'!

##
## Runas alias specification
##

##
## User privilege specification
##
root ALL=(ALL) ALL

## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL) ALL

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

## Read drop-in files from /etc/sudoers.d
## (the '#' here does not indicate 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**. Saisissez donc la commande suivante :

```
# visudo [Entrée]
```

Éditez la ligne suivante en ôtant le caractère **#** :

```
...
#%wheel ALL=(ALL) ALL
...
```

Vous obtiendrez un résultat similaire à celui-ci :

```
...
%wheel  ALL=(ALL) ALL
...
```

Sauvegardez votre fichier.

Important : A ce stade, **root** et les membres du groupe **wheel** peuvent administrer le système.

<html>

</html>