Niveau : Admin Junior	Numéro de la Leçon	Dernière Modification
2/4	<progrecss 1/12 style=inline />	2020/01/30 03:28

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.

<note important> Afin de mettre en pratique les exemples dans cette unité, vous devez vous connecter à votre système en tant que root grâce à la commande **su -** et le mot de passe **fenestros**. </note>

Groupes

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

```
opensuse:~ # cat /etc/group
at:!:25:
audio:x:17:pulse
avahi:!:105:
bin:x:1:daemon
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:!:109:
kmem:x:9:
lock:x:54:
lp:x:7:
mail:x:12:
maildrop:!:59:
man:x:62:
messagebus:!:104:
modem:x:43:
news:x:13:
nobody:x:65533:
nogroup:x:65534:nobody
ntadmin:!:71:
ntp:!:103:
postfix:!:51:
public:x:32:
pulse:!:107:
pulse-access:!:108:
root:x:0:
rtkit:!:106:
shadow:x:15:
sshd:!:102:
sys:x:3:
tape:!:101:
trusted:x:42:
tty:x:5:
utmp:x:22:
uucp:x:14:
video:x:33:
wheel:x:10:trainee
www:x:8:
xok:x:41:
users:x:100:
vboxsf:!:1000:
```

<note important> Notez que la valeur du GID (Group ID) de root est de **0** et que les GID des utilisateurs normaux est de **100** (voir **trainee**). </note>

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, openSUSE a abandonné l'utilisation du fichier /etc/gshadow 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 :

```
opensuse:~ # grpck -r
Checking `/etc/group'
```

<note important> L'option **-r** permet la vérification des erreurs sans le modifier. </note>

Dans le cas où il est nécessaire de régénérer un des deux fichiers, il convient d'utiliser un 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**

Utilisateurs

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

```
opensuse:~ # cat /etc/passwd
```

```
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
avahi:x:103:105:User for Avahi:/var/run/avahi-daemon:/bin/false
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
dnsmasq:x:102:65534:dnsmasq:/var/lib/empty:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
gdm:x:107:109: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:101:104: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
ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
pulse:x:105:107:PulseAudio daemon:/var/lib/pulseaudio:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
rtkit:x:104:106:RealtimeKit:/proc:/bin/false
sshd:x:100:102:SSH daemon:/var/lib/sshd:/bin/false
statd:x:106:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
usbmux:x:108:65534:usbmuxd daemon:/var/lib/usbmuxd:/sbin/nologin
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
trainee:x:1000:100:trainee:/home/trainee:/bin/bash
vboxadd:x:109:1::/var/run/vboxadd:/bin/false
```

<note 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. </note>

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 :

```
opensuse:~ # cat /etc/shadow
at:*:15111:0:99999:7:::
avahi:*:15035:0:99999:7:::
bin:*:15035::::::
daemon:*:15035::::::
dnsmasq:*:15035:0:99999:7:::
ftp:*:15035::::::
games:*:15035::::::
gdm:*:15035:0:99999:7:::
lp:*:15035::::::
mail:*:15035::::::
man:*:15035::::::
messagebus:*:15035:0:99999:7:::
news:*:15035::::::
nobody:*:15035::::::
ntp:*:15035:0:99999:7:::
postfix:*:15035:0:99999:7:::
pulse:*:15035:0:99999:7:::
root:$2a$05$vjaGlr9oXOAbGv1rwcoYn.zd59GevXgDrPPESbsikCTwrnvMfctBS:15111::::::
rtkit:*:15035:0:99999:7:::
sshd:*:15035:0:99999:7:::
statd:*:15035:0:99999:7:::
usbmux:*:15111:0:99999:7:::
uucp:*:15035::::::
wwwrun:*:15035::::::
trainee:$2a$05$KZSJtWwMIvyLcQJuxTbaHuXWokuhYVSSBp.yqUa606iGgTrpaY7R.:15111:0:99999:7:::
```

```
vboxadd:*:15183:0:99999:7:::
```

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 :

```
opensuse:~ # pwck -r
Checking `/etc/passwd'
User `pulse': directory `/var/lib/pulseaudio' does not exist.
User `usbmux': directory `/var/lib/usbmuxd' does not exist.
User `vboxadd': directory `/var/run/vboxadd' does not exist.
Checking `/etc/shadow'.
```

<note 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. </note>

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

```
opensuse:~ # groupadd --help
Usage: groupadd [-D binddn] [-g gid [-o]] [-r] [-P path] [-p password] group
groupadd - create a new group

  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -g gid         Force the new groupid to be the given number
  -o             Allow duplicate (non-unique) UID
  -P path        Search passwd, shadow and group file in "path"
  -p password    Encrypted password as returned by crypt(3)
  -r, --system   Create a system account
 --service srv   Add account to nameservice 'srv'
      --help     Give this help list
      --usage    Give a short usage message
  -v, --version  Print program version
Valid services for --service are: files, ldap
```

groupdel

Cette commande est utilisée pour supprimer un groupe.

Options de la commande

```
opensuse:~ # groupdel --help
Usage: groupdel [-D binddn] [-P path] group
groupdel - delete a group

  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -P path        Search passwd, shadow and group file in "path"
 --service srv   Add account to nameservice 'srv'
      --help     Give this help list
  -u, --usage    Give a short usage message
  -v, --version  Print program version
Valid services for --service are: files, ldap
```

groupmod

Cette commande est utilisée pour modifier un groupe existant.

Options de la commande

```
opensuse:~ # groupmod --help
Usage: groupmod [-g gid [-o]] [-n new_name] group
groupmod - modify a group entry

  -D binddn      Use dn "binddn" to bind to the LDAP directory
```

```
  -g gid         Change the groupid to the given number
  -k skeldir     Specify an alternative skel directory
  -n name        Change group name.
  -o             Allow duplicate (non-unique) UID
  -P path        Search passwd, shadow and group file in "path"
  -p password    Encrypted password as returned by crypt(3)
  -A user        Add the user to the group entry
  -R user        Remove the user from the group entry
  --service srv  Use nameservice 'srv'
      --help     Give this help list
      --usage    Give a short usage message
  -v, --version  Print program version
Valid services are: files, ldap
```

newgrp

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

Options de la commande

```
opensuse:~ # newgrp --help
Usage: newgrp [-l|-c command] [group]
newgrp - change the effective group id

  -l, --login    reinitialize environment as if logged in
  -c  command    Execute `command' with new group
      --help     Give this help list
  -u, --usage    Give a short usage message
  -v, --version  Print program version
```

gpasswd

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

Options de la commande

```
opensuse:~ # gpasswd --help
Usage: gpasswd [-r|-l|-u] group
gpasswd - change group password

  -r             Remove the password for this group
  -l             Locks the password entry for "group"
  -u             Try to unlock the password entry for "group"
  --service srv  Use nameservice 'srv'
  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -P path        Search group file in "path"
  --help         Give this help list
  --usage        Give a short usage message
  --version      Print program version
  --stdin        Receive input from stdin instead of /dev/tty
Valid services for -r are: files, nis, nisplus, ldap
```

Utilisateurs

useradd

Cette commande est utilisée pour 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

```
opensuse:~ # useradd --help
Usage: useradd ...
useradd - create a new user

  -c comment     Set the GECOS field for the new account
 --show-defaults Print default values
 --save-defaults Save modified default values
  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -d homedir     Home directory for the new user
  -e expire      Date on which the new account will be disabled
  -f inactive    Days after a password expires until account is disabled
  -G group,...   List of supplementary groups
  -g gid         Name/number of the users primary group
  -k skeldir     Specify an alternative skel directory
  -m             Create home directory for the new user
  -o             Allow duplicate (non-unique) UID
  -P path        Search passwd, shadow and group file in "path"
  -p password    Encrypted password as returned by crypt(3)
  -u uid         Force the new userid to be the given number
```

```
  -U umask       Umask value used for creating home directory
  -r, --system   Create a system account
  -s shell       Name of the user's login shell
 --service srv   Add account to nameservice 'srv'
      --help     Give this help list
      --usage    Give a short usage message
  -v, --version  Print program version
Valid services for --service are: files, ldap
```

userdel

Cette commande est utilisée pour utilisée pour supprimer un utilisateur.

Options de la commande

```
opensuse:~ # userdel --help
Usage: userdel [-D binddn] [-P path] [-r [-f]] user
userdel - delete a user and related files

  -r             Remove home directory and mail spool
  -f             Force removal of files, even if not owned by user
  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -P path        Search passwd, shadow and group file in "path"
 --service srv   Add account to nameservice 'srv'
      --help     Give this help list
  -u, --usage    Give a short usage message
  -v, --version  Print program version
Valid services for --service are: files, ldap
```

usermod

Cette commande est utilisée pour utilisée pour modifier un utilisateur existant.

Options de la commande

```
opensuse:~ # usermod --help
Usage: usermod ...
usermod - modify a user account

  -c comment     Set the GECOS field for the new account
  -D binddn      Use dn "binddn" to bind to the LDAP directory
  -d homedir     Home directory for the new user
  -e expire      Date on which the new account will be disabled
  -f inactive    Days after a password expires until account is disabled
  -G group,...   List of supplementary groups
  -g gid         Name/number of the users primary group
  -l login       Change login name.
  -m             Move home directory to the new path
  -o             Allow duplicate (non-unique) UID
  -A group,...   List of groups the user should be added to
  -R group,...   List of groups the user should be removed from
  -P path        Search passwd, shadow and group file in "path"
  -p password    Encrypted password as returned by crypt(3)
  -s shell       Name of the user's login shell
  -u uid         Change the userid to the given number
  --service srv  Use nameservice 'srv'
  -L             Locks the password entry for "user"
  -U             Try to unlock the password entry for "user"
      --help     Give this help list
      --usage    Give a short usage message
  -v, --version  Print program version
```

```
Valid services are: files, ldap
```

passwd

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

Options de la commande

```
opensuse:~ # passwd --help
Usage: passwd [-f|-g|-s|-k[-q]] [account]
       passwd [-D binddn] [-n min] [-x max] [-w warn] [-i inact] account
       passwd {-l|-u|-d|-S[-a]|-e} account
       passwd --stdin [account]
passwd - change password information

  -f             Change the finger (GECOS) information
  -s             Change the login shell
  -g             Change the group password
  -k             Change the password only if expired
  -q             Try to be quiet
  -S             Show the password attributes
  -a             Only with -S, show for all accounts
  -d             Delete the password for the named account
  -l             Locks the password entry for "account"
  -u             Try to unlock the password entry for "account"
  -e             Force the user to change password at next login
  -n min         Set minimum field for "account"
  -x max         Set maximum field for "account"
  -w warn        Set warn field for "account"
  --service srv  Use nameservice 'srv'
  -D binddn      Use dn "binddn" to bind to the LDAP directory
```

```
  -P path        Search passwd and shadow file in "path"
  --stdin        Read new password from stdin (root only)
  --help         Give this help list
  --usage        Give a short usage message
  --version      Print program version
Valid services are: files, nis, nisplus, ldap
```

Configuration

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

```
opensuse:~ # cat /etc/default/useradd
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
GROUPS=video
CREATE_MAIL_SPOOL=no
UMASK=022
```

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,
- **GROUPS** - identifie le ou les groupes secondaire 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**.

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

```
opensuse:~ # useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
GROUPS=video
CREATE_MAIL_SPOOL=no
UMASK=022
```

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

```
opensuse:~ # ls -la /etc/skel
total 60
drwxr-xr-x   6 root root  4096 May 17  2011 .
drwxr-xr-x 115 root root 12288 Dec  9 09:54 ..
-rw-------   1 root root     0 May 18  1996 .bash_history
-rw-r--r--   1 root root  1177 Feb 27  2011 .bashrc
-rw-r--r--   1 root root  1637 Feb 15  2010 .emacs
drwxr-xr-x   2 root root  4096 Feb 18  2011 .fonts
-rw-r--r--   1 root root   861 May 19  2006 .inputrc
drwxr-xr-x   2 root root  4096 Feb 18  2011 .mozilla
-rw-r--r--   1 root root  1028 Feb 27  2011 .profile
-rw-r--r--   1 root root  1002 Feb 22  2011 .vimrc
-rw-r--r--   1 root root  1940 Feb 18  2011 .xim.template
```

```
-rwxr-xr-x   1 root root  1455 Apr  6  2011 .xinitrc.template
drwxr-xr-x   2 root root  4096 Feb 18  2011 bin
drwxr-xr-x   2 root root  4096 Mar  2  2011 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 :

```
opensuse:~ # id trainee
uid=1000(trainee) gid=100(users) groups=100(users),10(wheel)
```

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

```
opensuse:~ # groups trainee
trainee : users wheel
```

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
#
# SYSTEM_UID_MIN to SYSTEM_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.
#
SYSTEM_UID_MIN        100
SYSTEM_UID_MAX        499
UID_MIN          1000
UID_MAX         60000

#
# Min/max values for automatic gid selection in groupadd
#
# SYSTEM_GID_MIN to SYSTEM_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.
#
SYSTEM_GID_MIN        100
SYSTEM_GID_MAX        499
GID_MIN          1000
GID_MAX         60000
...
```

T.P. #1

Créez maintenant trois groupes **groupe1**, **groupe2** et **groupe3**. La valeur du GID du groupe **groupe3** doit être de **807** :

```
opensuse:~ # 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** :

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

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

```
opensuse:~ # cat /etc/passwd
...
fenestros2:x:1001:1002::/home/fenestros2:/bin/bash
fenestros3:x:1002:807::/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:

```
opensuse:~ # cat /etc/group
...
groupe1:!:1001:fenestros2
groupe2:!:1002:
groupe3:!:807:fenestros2
```

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

```
opensuse:~ # gpasswd groupe3
Changing the password for group groupe3.
New Password: fenestros
Re-enter new password: fenestros
Password changed.
```

<note important> Notez que les mots de passe saisis ne seront **pas** visibles. </note>

Consultez le fichier **/etc/group** :

```
opensuse:~ # cat /etc/group
...
groupe1:!:1001:fenestros2
groupe2:!:1002:
groupe3:$1$dou68i4E$FNMKvHqm2SJv8kb8JbOCj0:807:fenestros2
```

<note important> Notez la présence du mot de passe crypté pour le **groupe3**. </note>

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

```
opensuse:~ # su fenestros1
fenestros1@opensuse:/root> groups
groupe1 video
fenestros1@opensuse:/root> newgrp groupe3
Password:
fenestros1@opensuse:/root> groups
```

```
groupe3 groupe1 video
```

Rejoignez le groupe3 et contrôlez vos groupes :

```
fenestros1@opensuse:/root> newgrp groupe3
Password: fenestros
fenestros1@opensuse:/root> groups
groupe3 groupe1 video
```

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

```
fenestros1@opensuse:/root> exit
exit
fenestros1@opensuse:/root> groups
groupe1 video
```

<note 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**. </note>

Dernièrement, redevenez **root** :

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

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

```
# groupdel groupe3 [Entrée]
```

Vous obtiendrez un résultat similaire à celui-ci :

```
opensuse:~ # groupdel groupe3
groupdel: GID `807' is primary group of `fenestros3'.
```

```
groupdel: Cannot remove user's primary group.
```

<note important> En effet, vous ne pouvez pas supprimer un groupe tant qu'un utilisateur le possède comme son groupe principal. </note>

Supprimez donc l'utilisateur **fenestros3** :

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

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

```
opensuse:~ # groupdel groupe3
```

<note important> Notez que cette fois-ci la commande est exécutée sans erreur. </note>

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

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

```
root@debian:~# useradd -m test
```

Vérifiez que l'utilisateur test a un répertoire personnel :

```
opensuse:~ # ls -l /home
total 8
drwxr-xr-x  6 test    users 4096 Dec 18 13:43 test
drwxr-xr-x 35 trainee users 4096 Dec 18 13:27 trainee
```

Créez maintenant les répertoires personnels de fenestros1 et fenestros2 :

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

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

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

```
opensuse:~ # chown -R fenestros1:groupe1 /home/fenestros1
opensuse:~ # 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 :

```
opensuse:~ # passwd fenestros1
Changing password for fenestros1.
New Password: fenestros1
Bad password: it is based on a dictionary word
Reenter New Password: fenestros1
Password changed.
opensuse:~ # passwd fenestros2
Changing password for fenestros2.
New Password: fenestros2
Bad password: it is based on a dictionary word
Reenter New Password: fenestros2
Password changed.
```

<note 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. </note>

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 :

```
opensuse:~ # pwd
/root
```

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

```
opensuse:~ # su fenestros2
```

Contrôlez votre répertoire courant de travail :

```
fenestros2@opensuse:/root> pwd
/root
```

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

<note 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**. </note>

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

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

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

```
opensuse:~ # su - fenestros2
```

Contrôlez votre répertoire courant de travail :

```
fenestros2@opensuse:~> pwd
/home/fenestros2
```

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

<note important> Notez que **root** peut devenir n'importe quel utilisateur **sans** avoir besoin de connaître son mot de passe. </note>

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 :

```
opensuse:~ # 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

# User alias specification

# Cmnd alias specification

# 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
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"

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

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

# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
```

<note 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. </note>

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.

<note important> A ce stade, **root** et les membres du groupe **wheel** peuvent administrer le système. </note>

~~DISCUSSION:off~~

Donner votre Avis

{(rater>id=opensuse_11_l106|name=cette page|type=rate|trace=user|tracedetails=1)}