Dernière mise-à-jour : 2020/01/30 03:27

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.

A faire - 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 **sudo su -** et le mot de passe **trainee**.

Groupes

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

```
root@ubuntu:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,trainee
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
```

```
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:trainee
floppy:x:25:
tape:x:26:
sudo:x:27:trainee
audio:x:29:pulse
dip:x:30:trainee
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:trainee
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
netdev:x:102:
crontab:x:103:
syslog:x:104:
```

```
fuse:x:105:
messagebus:x:106:
ssl-cert:x:107:
lpadmin:x:108:trainee
scanner:x:109:saned
mlocate:x:110:
ssh:x:111:
utempter:x:112:
avahi-autoipd:x:113:
rtkit:x:114:
saned:x:115:
whoopsie:x:116:
avahi:x:117:
lightdm:x:118:
nopasswdlogin:x:119:
bluetooth:x:120:
colord:x:121:
pulse:x:122:
pulse-access:x:123:
trainee:x:1000:
sambashare:x:124:trainee
vboxsf:x:999:
```

Notez que la valeur du GID (Group ID) de root est de **0** et que les GID des utilisateurs normaux commencent à **1000** (voir **trainee**).

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@ubuntu:~# cat /etc/gshadow
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::syslog,trainee
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
man:*::
proxy:*::
kmem:*::
dialout:*::
fax:*::
voice:*::
cdrom:*::trainee
floppy:*::
tape:*::
sudo:*::trainee
audio:*::pulse
dip:*::trainee
www-data:*::
backup:*::
operator:*::
list:*::
irc:*::
```

```
src:*::
gnats:*::
shadow:*::
utmp:*::
video:*::
sasl:*::
plugdev:*::trainee
staff:*::
games:*::
users:*::
nogroup:*::
libuuid:!::
netdev:!::
crontab:!::
syslog:!::
fuse:!::
messagebus:!::
ssl-cert:!::
lpadmin:!::trainee
scanner:!::saned
mlocate:!::
ssh:!::
utempter:!::
avahi-autoipd:!::
rtkit:!::
saned:!::
whoopsie:!::
avahi:!::
lightdm:!::
nopasswdlogin:!::
bluetooth:!::
colord:!::
pulse:!::
pulse-access:!::
```

```
trainee:!::
sambashare:!::trainee
vboxsf:!::
```

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@ubuntu:~# grpck -r
```

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

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 un des deux comandes 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

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@ubuntu:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
trainee:x:1000:1000:trainee,,,:/home/trainee:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
```

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 1 et 999.

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 :

```
root@ubuntu:~# cat /etc/shadow
root:!:16340:0:99999:7:::
daemon:*:16273:0:99999:7:::
bin:*:16273:0:99999:7:::
sys:*:16273:0:99999:7:::
sync:*:16273:0:99999:7:::
games:*:16273:0:99999:7:::
man:*:16273:0:99999:7:::
lp:*:16273:0:99999:7:::
mail:*:16273:0:99999:7:::
news:*:16273:0:99999:7:::
uucp:*:16273:0:99999:7:::
proxy:*:16273:0:99999:7:::
www-data:*:16273:0:99999:7:::
backup:*:16273:0:99999:7:::
list:*:16273:0:99999:7:::
irc:*:16273:0:99999:7:::
gnats:*:16273:0:99999:7:::
nobody:*:16273:0:99999:7:::
libuuid:!:16273:0:99999:7:::
syslog:*:16273:0:99999:7:::
messagebus:*:16273:0:99999:7:::
usbmux:*:16273:0:99999:7:::
dnsmasq:*:16273:0:99999:7:::
avahi-autoipd:*:16273:0:99999:7:::
kernoops:*:16273:0:99999:7:::
rtkit:*:16273:0:99999:7:::
saned:*:16273:0:99999:7:::
whoopsie:*:16273:0:99999:7:::
speech-dispatcher:!:16273:0:99999:7:::
```

```
avahi:*:16273:0:99999:7:::
lightdm:*:16273:0:99999:7:::
colord:*:16273:0:99999:7:::
hplip:*:16273:0:99999:7:::
pulse:*:16273:0:99999:7:::
trainee:$6$5ZUj7cng$DN4OYb8zALVs06aLBCpTzuW9xQ07apFIMJJfg9iFscw6W/7SMjKix1lbKim8aU7YC1MlzA.aqyuuSHAMfEZ/r/:16340:
0:99999:7:::
vboxadd:!:16341::::::
```

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 :

```
root@ubuntu:~# pwck -r
utilisateur lp : le répertoire « /var/spool/lpd » n'existe pas
utilisateur news : le répertoire « /var/spool/news » n'existe pas
utilisateur uucp : le répertoire « /var/spool/uucp » n'existe pas
utilisateur www-data : le répertoire « /var/www » n'existe pas
utilisateur list : le répertoire « /var/list » n'existe pas
utilisateur irc : le répertoire « /var/run/ircd » n'existe pas
utilisateur gnats : le répertoire « /var/lib/gnats » n'existe pas
utilisateur nobody : le répertoire « /nonexistent » n'existe pas
```

```
utilisateur syslog : le répertoire « /home/syslog » n'existe pas
utilisateur usbmux : le répertoire « /home/usbmux » n'existe pas
utilisateur saned : le répertoire « /home/saned » n'existe pas
utilisateur whoopsie : le répertoire « /nonexistent » n'existe pas
utilisateur speech-dispatcher : le répertoire « /var/run/speech-dispatcher » n'existe pas
utilisateur hplip : le répertoire « /var/run/hplip » 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
```

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 comandes 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@ubuntu:~# groupadd --help
Syntaxe: groupadd [options] GROUPE

Options:
  -f, --force                   terminer avec succès si le groupe existe déjà
                                ou interrompre -g si le GID est déjà utilisé
  -g, --gid GID                 utiliser cet identifiant (GID) pour le nouveau groupe
  -h, --help                    afficher ce message d'aide et quitter
  -K, --key CLÉ=VALEUR          ignorer les valeurs par défaut de /etc/login.defs
  -o, --non-unique              autoriser la création de groupes avec des identifiants
                                (GID) non uniques
  -p, --password MOT_DE_PASSE   utiliser ce mot de passe chiffré pour le nouveau groupe
  -r, --system                  créer un compte système
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
```

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

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

Cette commande ne prend pas d'options.

groupmod

Cette commande est utilisée pour modifier un groupe existant.

Options de la commande

```
root@ubuntu:~# groupmod --help
Syntaxe: groupmod [options] GROUPE

Options:
  -g, --gid GID                 modifier l'identifiant de groupe en
                                utilisant GID comme valeur
  -h, --help                    afficher ce message d'aide et quitter
  -n, --new-name NOUVEAU_GROUPE renommer en NOUVEAU_GROUPE
  -o, --non-unique              utiliser un identifiant de groupe déjà
                                utilisé
  -p, --password MOT_DE_PASSE   remplacer le mot de passe par le mot de
                                passe chiffré MOT_DE_PASSE
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
```

newgrp

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

Options de la commande

```
root@ubuntu:~# newgrp --help
Syntaxe : newgrp [-] [groupe]
```

gpasswd

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

Options de la commande

```
root@ubuntu:~# gpasswd --help
Utilisation : gpasswd [options] GROUPE

Options :
  -a, --ADD UTILISATEUR      ajouter UTILISATEUR au groupe GROUPE
  -d, --delete UTILISATEUR   supprimer UTILISATEUR du groupe GROUPE
  -h, --help                    afficher ce message d'aide et quitter
  -Q, --root REP_CHROOT       répertoire dans lequel chrooter
  -r, --remove-password        supprimer le mot de passe du groupe GROUPE
  -R, --restrict                 restreindre l'accès au groupe GROUPE à ses membres
  -M, --members UTILISATEUR,…
                                définir la liste des membres du groupe GROUPE
  -A, --administrators ADMIN,…
                                définir la liste des administrateurs du GROUPE
```

```
À l'exception des options A et M, les options ne peuvent pas être combinées.
```

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@ubuntu:~# useradd --help
Utilisation : useradd [options] LOGIN
              useradd -D
              useradd -D [options]

Options :
  -b, --base-dir REP_BASE       répertoire de base pour le répertoire personnel
                                du compte du nouvel utilisateur
```

```
  -c, --comment COMMENTAIRE     définir le champ « GECOS » du compte du
                                nouvel utilisateur
  -d, --home-dir REP_PERS       répertoire personnel pour le compte du
                                nouvel utilisateur
  -D, --defaults                afficher ou enregistrer la configuration
                                par défaut modifiée de « useradd »
  -e, --expiredate DATE_EXPIR   fixer la date de fin de validité du
                                compte à DATE_EXPIR
  -f, --inactive INACTIF        fixer la durée d'inactivité du mot de passe
  -g, --gid GROUPE              forcer l'utilisation de GROUPE pour le
                                compte du nouvel utilisateur
  -G, --groups GROUPES          liste des GROUPES supplémentaires pour le
                                compte du nouvel utilisateur
  -h, --help                    afficher ce message d'aide et quitter
  -k, --skel REP_SQEL           définir un autre répertoire « skel »
  -K, --key CLÉ=VALEUR          ignorer les valeurs par défaut de /etc/login.defs
  -l, --no-log-init             ne pas ajouter l'utilisateur aux bases de
                                données lastlog et faillog
  -m, --create-home             créer le répertoire personnel pour le
                                compte du nouvel utilisateur
  -M, --no-create-home          ne pas créer de répertoire personnel pour
                                le compte du nouvel utilisateur
  -N, --no-user-group           ne pas créer de groupe de même nom que
                                l'utilisateur
  -o, --non-unique              autoriser la création d'un utilisateur
                                avec un identifiant d'utilisateur (UID)
                                dupliqué (non unique)
  -p, --password MOT_DE_PASSE   utiliser un mot de passe chiffré pour le
                                compte du nouvel utilisateur
  -r, --system                  créer un compte système
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
  -s, --shell INTERPRÉTEUR      interpréteur de commandes initial pour le
                                compte du nouvel utilisateur
  -u, --uid UID                 forcer l'utilisation de l'identifiant
```

```
                                « UID » pour le compte du nouvel utilisateur
  -U, --user-group              créer un groupe ayant le même nom que
                                l'utilisateur
  -Z, --selinux-user SEUSER     utiliser un SEUSER particulier pour la
                                correspondance de l'utilisateur SELinux
```

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

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@ubuntu:~# userdel --help
Utilisation : userdel [options] LOGIN

Options :
  -f, --force                   forcer la suppression des fichiers, même
                                s'ils n'appartiennent pas à l'utilisateur
  -h, --help                    afficher ce message d'aide et quitter
  -r, --remove                  supprimer le répertoire personnel et le
```

```
                                spool du courrier
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
  -Z, --selinux-user            supprimer toute correspondance d'utilisateur SELinux pour le compte d'utilisateur
```

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 récent, cette limite passe à plus de 4,2 Milliards.

usermod

Cette commande est utilisée pour modifier un utilisateur existant.

Options de la commande

```
root@ubuntu:~# usermod --help
Utilisation : usermod [options] LOGIN

Options :
  -c, --comment COMMENT         définir une nouvelle valeur pour le champ
                                « GECOS »
  -d, --home REP_PERS           définir un nouveau répertoire personnel
                                pour le compte de l'utilisateur
  -e, --expiredate DATE_EXPIR   fixer la date de fin de validité du compte
                                à DATE_EXPIR
  -f, --inactive INACTIF        fixer la durée d'inactivité du mot de passe
                                après sa fin de validité à INACTIF
  -g, --gid GROUPE              forcer l'utilisation de GROUPE comme
                                nouveau groupe primaire
```

```
  -G, --groups GROUPES          définir une nouvelle liste de groupes
                                supplémentaires
  -a, --append                  ajouter l'utilisateur aux GROUPES
                                supplémentaires mentionnés par l'option -G
                                sans supprimer l 'utilisateur des autres
                                groupes
  -h, --help                    afficher ce message d'aide et quitter
  -l, --login IDENTIFIANT       définir un nouveau nom pour le compte
  -L, --lock                    bloquer le compte de l'utilisateur
  -m, --move-home               déplacer le contenu du répertoire personnel
                                vers le nouvel emplacement (à n'utiliser
                                qu'avec -d)
  -o, --non-unique              autoriser l'utilisation d'un identifiant
                                d'utilisateur (UID) dupliqué (non unique)
  -p, --password MOT_DE_PASSE   utiliser un mot de passe chiffré pour le
                                nouveau mot de passe
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
  -s, --shell INTERPRÉTEUR      nouvel interpréteur de commandes initial
                                pour le compte de l'utilisateur
  -u, --uid UID                 définir un nouvel identifiant (UID) pour le
                                compte de l'utilisateur
  -U, --unlock                  déverrouiller le compte de l'utilisateur
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remvoe range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remvoe range of subordinate gids
  -Z, --selinux-user            nouvelle correspondance de l'utilisateur SELinux pour le compte d'utilisateur
```

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@ubuntu:~# passwd --help
Utilisation : passwd [options] [LOGIN]

Options :
  -a, --all                     afficher l'état des mots de passe de tous
                                les comptes
  -d, --delete                  supprimer le mot de passe du compte indiqué
  -e, --expire                  forcer la fin de validité du compte indiqué
  -h, --help                    afficher ce message d'aide et quitter
  -k, --keep-tokens             ne changer le mot de passe que s'il
                                est arrivé en fin de validité
  -i, --inactive INACTIF        fixer la durée d'inactivation du mot de
                                passe après sa fin de validité à INACTIF
  -l, --lock                    bloquer le compte indiqué
  -n, --mindays JOURS_MIN       fixer le nombre minimum de jours avant le
                                changement de mot de passe à JOURS_MIN
  -q, --quiet                  mode silencieux
  -r, --repository DÉPÔT        changer le mot de passe dans le dépôt DÉPÔT
  -R, --root RÉP_CHROOT        répertoire dans lequel chrooter
  -S, --status                  afficher l'état du mot de passe du compte
                                indiqué
  -u, --unlock                  déverrouiller le compte indiqué
  -w, --warndays JOURS_AVERT    fixer le nombre de jours d'avertissement
                                de fin de validité à JOURS_AVERT
  -x, --maxdays JOURS_MAX       fixer le nombre maximum de jours avant le
```

```
                                changement de mot de passe à JOURS_MAX
```

Notez l'option **-l** qui permet de verrouiller un compte en placant 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@ubuntu:~# chage --help
Utilisation : chage [options] LOGIN

Options :
  -d, --lastday DERNIER_JOUR    fixer la dernière modification du mot de
                                passe à DERNIER_JOUR
  -E, --expiredate FIN_VALIDITÉ fixer la date de fin de validité du compte
                                à FIN_VALIDITÉ
  -h, --help                    afficher ce message d'aide et quitter
  -I, --inactive INACTIF        fixer la durée d'inactivité du mot de
                                passe après sa fin de validité à INACTIF
  -l, --list                    afficher les informations concernant la
                                validité du compte au cours du temps
  -m, --mindays JOURS_MIN       fixer le nombre minimum de jours avant la
                                modification du mot de passe à JOURS_MIN
  -M, --maxdays JOURS_MAX       fixer le nombre maximum de jours avant la
```

```
                                modification du mot de passe à JOURS_MAX
  -R, --root RÉP_CHROOT       répertoire dans lequel chrooter
  -W, --warndays JOURS_AVERT    fixer le nombre de jours d'avertissement
                                de fin de validité à JOURS_AVERT
```

Configuration

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

```
root@ubuntu:~# cat /etc/default/useradd
# Default values for useradd(8)
#
# The SHELL variable specifies the default login shell on your
# system.
# Similar to DHSELL in adduser. However, we use "sh" here because
# useradd is a low level utility and should be as general
# as possible
SHELL=/bin/sh
#
# The default group for users
# 100=users on Debian systems
# Same as USERS_GID in adduser
# This argument is used when the -n flag is specified.
# The default behavior (when -n and -g are not specified) is to create a
# primary user group with the same name as the user being added to the
# system.
# GROUP=100
#
# The default home directory. Same as DHOME for adduser
# HOME=/home
#
# The number of days after a password expires until the account
```

```
# is permanently disabled
# INACTIVE=-1
#
# The default expire date
# EXPIRE=
#
# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
# SKEL=/etc/skel
#
# Defines whether the mail spool should be created while
# creating the account
# 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** :

```
root@ubuntu:~# useradd -D
GROUP=100
HOME=/home
```

```
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

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

```
root@ubuntu:~# ls -la /etc/skel/
total 40
drwxr-xr-x   2 root root  4096 juil. 23 00:14 .
drwxr-xr-x 131 root root 12288 sept. 29 14:08 ..
-rw-r--r--   1 root root   220 avril  9 03:03 .bash_logout
-rw-r--r--   1 root root  3637 avril  9 03:03 .bashrc
-rw-r--r--   1 root root  8980 oct.   4  2013 examples.desktop
-rw-r--r--   1 root root   675 avril  9 03:03 .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@ubuntu:~# id trainee
uid=1000(trainee) gid=1000(trainee)
groupes=1000(trainee),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),124(sambashare)
```

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

```
root@ubuntu:~# groups trainee
trainee : trainee adm cdrom sudo dip plugdev lpadmin sambashare
```

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          1000
UID_MAX         60000
# System accounts
#SYS_UID_MIN          100
#SYS_UID_MAX          999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN          1000
GID_MAX         60000
# System accounts
#SYS_GID_MIN          100
#SYS_GID_MAX          999
...
```

LAB #1

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

```
root@ubuntu:~# 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** :

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

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

```
root@ubuntu:~# cat /etc/passwd
```

```
...
fenestros2:x:1001:1002::/home/fenestros2:
fenestros3:x:1002:807::/home/fenestros3:
fenestros1:x:1003:1001:tux1:/home/fenestros1:
```

Notez que utilisateur manque n'a pas de shell de défini. De même le système n'a pas créé les répertoire personnels dans **/home** :

```
root@ubuntu:~# ls -l /home
total 4
drwxr-xr-x 15 trainee trainee 4096 sept. 29 14:08 trainee
```

Supprimez donc les trois utilisateurs précédement créés :

```
root@ubuntu:~# userdel fenestros1
root@ubuntu:~# userdel fenestros2
root@ubuntu:~# userdel fenestros3
```

Recréez maintenant les trois utilisateurs :

```
root@ubuntu:~# useradd -m -u 1001 -s /bin/sh -g groupe2 fenestros2; useradd  -m -u 1002 -s /bin/sh -g 807
fenestros3; useradd  -m -u 1003 -s /bin/sh -g groupe1 fenestros1
```

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

```
root@ubuntu:~# cat /etc/passwd
...
fenestros2:x:1001:1002::/home/fenestros2:/bin/sh
fenestros3:x:1002:807::/home/fenestros3:/bin/sh
fenestros1:x:1003:1001::/home/fenestros1:/bin/sh
```

Vérifiez ensuite que les répertoires ont été créés dans **/home** :

```
root@ubuntu:~# ls -l /home
```

```
total 16
drwxr-xr-x  2 fenestros1 groupe1 4096 oct.   1 16:43 fenestros1
drwxr-xr-x  2 fenestros2 groupe2 4096 oct.   1 16:43 fenestros2
drwxr-xr-x  2 fenestros3 groupe3 4096 oct.   1 16:43 fenestros3
drwxr-xr-x 15 trainee    trainee 4096 sept. 29 14:08 trainee
```

Maintenant, exécutez les deux commandes suivantes :

```
root@ubuntu:~# usermod -G groupe1,groupe3 fenestros2
root@ubuntu:~# usermod -c "tux1" fenestros1
```

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

```
root@ubuntu:~# cat /etc/group
...
groupe1:x:1001:fenestros2
groupe2:x:1002:
groupe3:x:807:fenestros2
```

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

```
root@ubuntu:~# gpasswd groupe3
Changement du mot de passe pour le groupe groupe3
Nouveau mot de passe : fenestros
Nouveau mot de passe (pour vérification) : fenestros
```

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

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

```
root@debian:~# cat /etc/gshadow
```

```
...
groupe1:!::fenestros2
groupe2:!::
groupe3:$6$Et8poQVnMg/Dm$RliMdK.P1wZFN0bkoxYuLUcgs9FjJ.fxyxNc81rGnFBe1J.hwbm.dOYdPry2wlIecVF7OkbtwN3eHrvIi27lg/::
fenestros2
```

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

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

```
root@ubuntu:~# gpasswd -A fenestros1 groupe3
```

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

```
root@ubuntu:~# cat /etc/gshadow
...
groupe1:!::fenestros2
groupe2:!::
groupe3:$6$Et8poQVnMg/Dm$RliMdK.P1wZFN0bkoxYuLUcgs9FjJ.fxyxNc81rGnFBe1J.hwbm.dOYdPry2wlIecVF7OkbtwN3eHrvIi27lg/:f
enestros1:fenestros2
```

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@ubuntu:~# groupdel groupe3
groupdel : impossible de supprimer le groupe primaire de l'utilisateur « fenestros3 »
```

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@ubuntu:~# userdel fenestros3
```

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

```
root@ubuntu:~# groupdel groupe3
```

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 pour vérifier :

```
root@ubuntu:~# ls -ld /home/fenestros3
drwxr-xr-x 2 1002 807 4096 oct.   1 16:43 /home/fenestros3
```

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

```
root@ubuntu:~# find /home -user 1002 -exec rm -rf {} \;
find: "/home/fenestros3": Aucun fichier ou dossier de ce type
root@ubuntu:~# ls -ld /home/fenestros3
ls: impossible d'accéder à /home/fenestros3: Aucun fichier ou dossier de ce type
```

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@ubuntu:~# passwd fenestros1
Entrez le nouveau mot de passe UNIX : fenestros1
Retapez le nouveau mot de passe UNIX : fenestros1
passwd : le mot de passe a été mis à jour avec succès
root@ubuntu:~# passwd fenestros2
Entrez le nouveau mot de passe UNIX : fenestros2
Retapez le nouveau mot de passe UNIX : fenestros2
passwd : le mot de passe a été mis à jour avec succès
```

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

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@ubuntu:~# pwd
/root
```

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

```
root@ubuntu:~# su fenestros2
```

Contrôlez votre répertoire courant de travail :

```
$ pwd
/root
```

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

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** :

```
$ exit
```

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

```
root@ubuntu:~# su - fenestros2
```

Contrôlez votre répertoire courant de travail :

```
$ pwd
/home/fenestros2
```

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

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** ainsi que les fichiers se trouvant dans le répertoire **/etc/sudoers.d**. Saisissez la commande suivante :

```
root@ubuntu:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

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

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Notez la présence de la ligne en commentaire **# %sudo ALL=(ALL) ALL**. Cette ligne possède le format **Qui Où = (En tant que qui) Quoi**. La ligne implique donc que les membres du groupe **sudo** 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**.

Vérifiez maintenant si l'utilisateur **trainee** est membre du groupe **sudo** :

```
root@ubuntu:~# groups trainee
trainee : trainee adm cdrom sudo dip plugdev lpadmin sambashare
```

L'utilisateur **trainee**, étant membre du groupe **sudo**, peut administrer le système.

<html>

- Pas d’Utilisation Commerciale - Pas de Modification 3.0 France.

</html>
