



Gestion des utilisateurs

Serveur Linux CentOS

Table des matières

1	Introduction	3
2	Types de comptes	3
3	Créer un utilisateur (useradd)	4
4	Changer les options par défaut de useradd	7
4.1	Changer de mot de passe (passwd).....	8
5	Supprimer un utilisateur (userdel)	9
6	Modifier les attributs d'un utilisateur (usermod).....	10
7	Divers.....	12
7.1	Afficher le UID et les GID	12
7.2	Afficher le Shell courant	12
7.3	Changer de Shell.....	12
7.4	Afficher les shells valides.....	13
7.5	chfn.....	14
7.6	finger	15
8	Mode batch	16
8.1	newusers	16
8.2	chpasswd	16

1 Introduction

Linux étant multiutilisateur, les personnes employant celui-ci doivent être identifiées afin d'assurer la confidentialité. Chaque personne doit avoir un compte usager pour pouvoir accéder au système.

Pour identifier tous ces utilisateurs au niveau du système, un numéro unique leur sera attribué : le **UID** (User's ID). Le propriétaire d'un fichier est déterminé par ce numéro. Ces utilisateurs seront aussi dotés d'un nom d'utilisateur unique (**login**) et d'un mot de passe (**password**) pour qu'ils puissent s'authentifier lors de leur connexion au système.

2 Types de comptes

Les comptes utilisateur ne sont pas tous égaux sur Linux. On distingue trois types :

Superutilisateur (root): c'est l'utilisateur le plus important du système du point de vue de l'administration. Il n'est pas concerné par les droits d'accès aux fichiers. Son **UID** égal à **0** (zéro) lui confère sa spécificité. Ce superutilisateur aura donc à sa charge les tâches d'administration du système.

Comptes systèmes (bin, daemon, sync, apache...): on trouve sur le système toute une série de comptes qui ne sont pas affectés à des personnes. Ceux-ci servent à faciliter la gestion des droits d'accès de certaines application et démons. Ainsi en lançant le serveur Web sous l'identité du compte "**apache**", on pourra aisément limiter ses droits d'accès à certains fichiers.

D'une façon générale, on ne lance jamais un service exposé aux attaques réseau comme un serveur Web sous l'identité de **root**. Sinon, quelqu'un de mal intentionné qui réussirait à exploiter une faille de sécurité du logiciel obtiendrait automatiquement les droits d'administration. Toujours pour des raisons de sécurité, on fera en sorte que personne ne puisse se connecter à la machine à partir de l'un de ces comptes. Les UID compris entre 1 et 999 sont généralement utilisés pour ces comptes.

Comptes ordinaires : Tous les autres comptes utilisateur sont associés à des personnes; leur vocation est de permettre à des utilisateurs standard de se connecter. L'UID d'un utilisateur sera un nombre supérieur ou égal à 1000.

3 Créer un utilisateur (useradd)

La commande **useradd** permet d'ajouter un nouvel usager.

Ajouter un utilisateur **hakimb** sans spécifier son UID :

```
[root@localhost ~]# useradd hakimb
```

- Une entrée est ajoutée dans le fichier **/etc/passwd** sans le mot de passe.
- Un user id par défaut (UID) est assigné à l'utilisateur **hakimb**.
- Par défaut RedHat crée un nouveau groupe qui sera assigné à cet utilisateur.
- Création d'un répertoire usager, par défaut **/home/hakimb**
- Copier le contenu de **/etc/skel** dans **/home/hakimb**

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/dev/null
rpm:x:37:37:/:/var/lib/rpm:/bin/bash
ntp:x:38:38:/:etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42:/:/var/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
hakimb:x:1000:0:/:/home/hakimb:/bin/bash
```

Note:

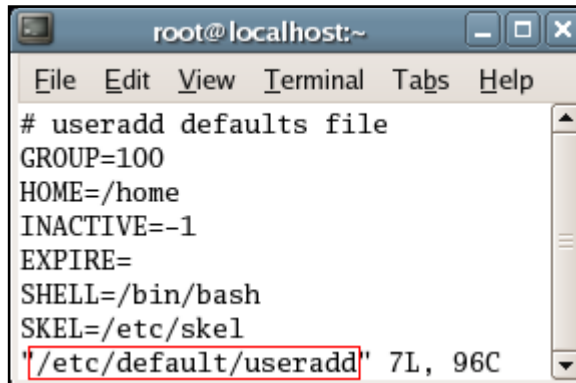
Les options par défaut pour la création des utilisateurs sont spécifiées dans les fichiers:

/etc/login.defs

```
# *REQUIRED*
# Directory where mailboxes reside, _or_ name of file,
# relative to the home directory. If you _do_ define
# both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#QMAIL_DIR Maildir
MAIL_DIR /var/spool/mail
#MAIL_FILE .mail

# Password aging controls:
#
# PASS_MAX_DAYS Maximum number of days a password may be used.
# PASS_MIN_DAYS Minimum number of days allowed between password
# changes.
# PASS_MIN_LEN Minimum acceptable password length.
# PASS_WARN_AGE Number of days warning given before a password
# expires.
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN 1000
UID_MAX 60000
#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN 1000
GID_MAX 60000
#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD /usr/sbin/userdel_local
#
# If useradd should create home directories for users by default
# On RH systems, we do.
# This option is ORed with the -m flag on
# useradd command line.
#
CREATE_HOME yes
```

Les valeurs par défaut de la commande **useradd** se trouvent dans le fichier **/etc/default/useradd** :



```
root@localhost:~  
File Edit View Terminal Tabs Help  
# useradd defaults file  
GROUP=100  
HOME=/home  
INACTIVE=-1  
EXPIRE=  
SHELL=/bin/bash  
SKEL=/etc/skel  
"/etc/default/useradd" 7L, 96C
```

Ajouter un utilisateur **usager2** en spécifiant son UID

```
[root@localhost ~]# useradd -u 1040 usager2
```

Ajouter un utilisateur **usager3** en spécifiant son groupe par défaut

```
[root@localhost ~]# useradd -g dev usager3
```

Ajouter un utilisateur **usager4** en spécifiant son groupe par défaut et ses groupes secondaires

```
[root@localhost ~]# useradd -g dev -G test,prod usager4
```

Ajouter un utilisateur **usager5** en spécifiant un commentaire

```
[root@localhost ~]#  
useradd -c 'Consultant pour projet x' usager5
```

Pour ajouter un utilisateur **usager6** en spécifiant une date d'expiration

```
[root@localhost ~]# useradd -e 2024-10-30 usager6
```

Ajouter un utilisateur **usager7** en spécifiant un shell

```
[root@localhost ~]# useradd -s /bin/bash usager7
```

Ajouter un utilisateur **usager8** en spécifiant son répertoire personnel

```
[root@localhost ~]# useradd -d /home2/usager8 usager8
```

4 Changer les options par défaut de useradd

On peut changer les options par défaut de la commande **useradd** en modifiant directement le fichier **/etc/default/useradd** ou bien en utilisant la commande **useradd** avec l'option **-D**.

Changer le répertoire usager par défaut

```
[root@localhost ~]# useradd -D -b /usagers
```

Changer le groupe par défaut

```
[root@localhost ~]# useradd -D -g dev
```

Par défaut si dans la commande **useradd**, le groupe n'est pas spécifié (option **-g**), **RedHat** crée un groupe privé qui porte le même nom que l'utilisateur. Si on veut que le nouvel usager soit dans le groupe par défaut, on doit utiliser l'option **-n** avec la commande **useradd** :

```
[root@localhost ~]# useradd -n usager22
```

Combinaison

```
[root@localhost ~]# useradd -D -b /usagers -g dev
```

Changer le Shell par défaut

```
[root@localhost ~]# useradd -D -s /bin/csh
```

Changer la date d'expiration par défaut

```
[root@localhost ~]# useradd -D -e 2040-12-31
```

Pour visualiser les valeurs par défaut de useradd

```
[root@localhost ~]# useradd -D
```

Ou bien afficher le contenu du fichier **/etc/default/useradd**

4.1 Changer de mot de passe (passwd)

La commande `passwd` permet de changer le mot de passe d'un utilisateur. Seul l'administrateur peut changer le mot de passe d'un autre utilisateur que lui-même.

La commande suivante permet à **bob** de changer son mot de passe:

```
[bob@localhost ~]$ passwd
```

La commande suivante permet à **root** de changer le mot de passe de **bob**:

```
[root@localhost ~]# passwd bob
```

Les informations sur les mots de passe sont stockées dans le fichier **/etc/shadow** :

```
root:$1$uýÿgRMXÊ$liVDUY/YaSms2G8TkMKzN1:12642:0:99999:7
:::
bin:!:12642:0:99999:7:::
daemon:!:12642:0:99999:7:::
adm:!:12642:0:99999:7:::
rpc:!!:12642:0:99999:7:::
...
xfs:!!:12642:0:99999:7:::
nscd:!!:12642:0:99999:7:::
ident:!!:12642:0:99999:7:::
radvd:!!:12642:0:99999:7:::
bob:!!:12642:0:99999:7:::
```


5 Supprimer un utilisateur (userdel)

Supprimer un utilisateur sans supprimer son répertoire personnel :

```
[root@localhost ~]# useradd usager1
```

```
[root@localhost ~]# su - usager1
```

```
[usager1@localhost ~]$ touch fichier
```

```
[usager1@localhost ~]$ ls -l
```

```
-rw-rw-r-- 1 usager1 usager1 0 Oct 18 11:08 fichier
```

```
[usager1@localhost ~]$ exit
```

```
logout
```

```
[root@localhost ~]# userdel usager1
```

```
[root@localhost ~]# cd /home/usager1
```

```
[root@localhost ~]# ls -l
```

```
-rw-rw-r-- 1 508 1010 0 Oct 18 11:08 fichier
```

Supprimer un utilisateur et son répertoire personnel :

```
[root@localhost ~]# userdel -r usager2
```

La commande précédente supprime l'utilisateur usager2 ainsi que son répertoire personnel. Les fichiers appartenant à cet usager et qui se trouvent en dehors de son répertoire personnel ne sont pas supprimés.

On peut les supprimer avec la commande suivante :

```
[root@localhost ~]#
```

```
find / -type f -uid 508 -print -exec rm {} \;
```

6 Modifier les attributs d'un utilisateur (usermod)

Changer de répertoire par défaut

```
[root@localhost ~]# usermod -d /usagers/marco marco  
ou bien  
[root@localhost ~]# usermod -d /usagers/marco -m marco  
(m pour déplacer les fichiers dans le nouveau  
répertoire)
```

Changer de UID

```
[root@localhost ~]# usermod -u 4444 usager1
```

Changer de groupe :

```
[root@localhost ~]# usermod -g 2222 usager1
```

On peut aussi utiliser le nom du groupe :

```
[root@localhost ~]# usermod -g dev usager1
```

Changer de date d'expiration(mm/dd/yy) :

```
[root@localhost ~]# usermod -e 2025-01-01 usager1
```

Changer de shell :

```
[root@localhost ~]# usermod -s /bin/csh usager1
```

Désactiver un utilisateur

Désactivé	Réactivé
<code>usermod -e 2000-01-01 usager1</code>	<code>usermod -e 2099-01-01 usager1</code>
<code>usermod -s /bin/false usager1</code>	<code>usermod -s /bin/bash usager1</code>
<code>usermod -L usager1</code>	<code>usermod -U usager1</code>
<code>passwd -l hakimb</code>	<code>passwd -u hakimb</code>

- Le caractère **!** est placé devant le mot de passe encrypté pour le désactivé.
- **/bin/false** est un shell qui ne fait rien.
- **/sbin/nologin** est un shell qui ne fait rien mais affiche le message : **'This account is currently not available'**

Changer de groupes secondaires

```
[root@localhost ~]# usermod -G prod, dev usager1
```

7 Divers

7.1 Afficher le UID et les GID

```
[root@localhost ~]# id
uid=0 (root)
gid=0 (root)
groups=0 (root) , 1 (bin) , 2 (daemon) , 3 (sys) , 4 (adm) , 6 (disk) , 10 (wheel)
```

```
[root@localhost ~]# id -g
0
```

```
[root@localhost ~]# id -G
0 1 2 3 4 6 10
```

```
[root@localhost ~]# id -gn
root
```

```
[root@localhost ~]# id -Gn
root bin daemon sys adm disk wheel
```

7.2 Afficher le Shell courant

Pour afficher le Shell courant :

```
[root@localhost ~]# echo $SHELL
```

7.3 Changer de Shell

Pour changer le Shell par défaut de d'un utilisateur :

```
[root@localhost ~]# chsh usager1
```

ou bien

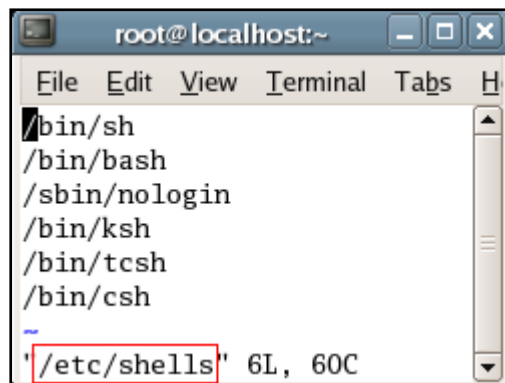
```
[root@localhost ~]# usermod -s /bin/csh usager1
```

7.4 Afficher les shells valides

Pour afficher la liste des Shells valides :

```
[root@localhost ~]# chsh -l
```

La liste des Shells valides se trouve dans le fichier **/etc/shells** :



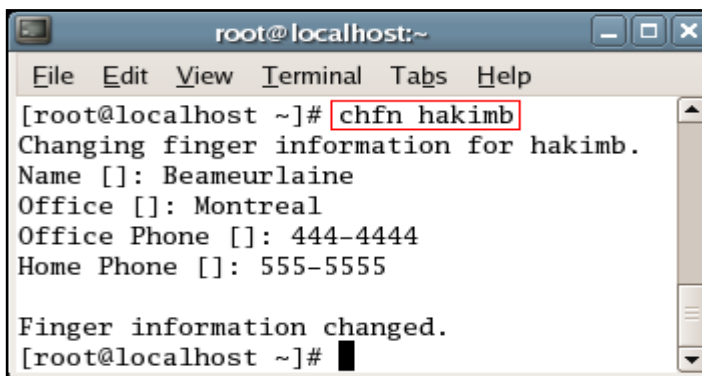
```
root@localhost:~  
File Edit View Terminal Tabs H  
/bin/sh  
/bin/bash  
/sbin/nologin  
/bin/ksh  
/bin/tcsh  
/bin/csh  
"/etc/shells" 6L, 60C
```

7.5 chfn

La commande **chfn** permet de changer les informations utilisées par **finger**. Seul l'administrateur peut changer les informations d'un autre utilisateur que lui-même. Si aucune option n'est précisée, **chfn** demande champ par champ à entrer les modifications.

Options

-f nom	Change le nom et le prénom.
-o bureau	Change le nom du bureau.
-p btel	Change le numéro de téléphone du bureau.
-h mtel	Change le numéro de téléphone personnel.



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# chfn hakimb  
Changing finger information for hakimb.  
Name []: Beameurlaine  
Office []: Montreal  
Office Phone []: 444-4444  
Home Phone []: 555-5555  
  
Finger information changed.  
[root@localhost ~]#
```

Fichier **/etc/passwd** :

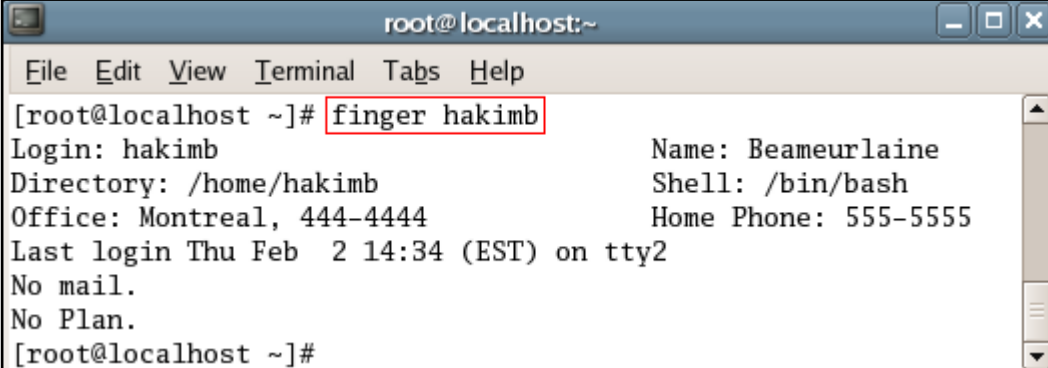
```
hakimb:x:1000:0:Beameurlaine,Montreal,444-4444,555-5555:/home/hakimb:/bin/bash
```

7.6 finger

La commande **finger** permet d'affiche des informations concernant un ou plusieurs *utilisateurs* ainsi que les fichiers **.plan**, **.project** et **.forward** contenus dans les racines des *utilisateurs*. Vous pouvez préciser le nom de login (exact), le prénom ou le nom de famille (**finger** renverra tous les utilisateurs dont l'un des noms correspond).

Options

-l	Permet d'utiliser le format long (par défaut).
-m	Les noms donnés ne doivent correspondre qu'à des noms de login.
-p	N'affiche pas les fichiers .plan et .project .
-s	Permet d'utiliser le format court.



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# finger hakimb  
Login: hakimb                      Name: Beameurlaine  
Directory: /home/hakimb           Shell: /bin/bash  
Office: Montreal, 444-4444        Home Phone: 555-5555  
Last login Thu Feb  2 14:34 (EST) on tty2  
No mail.  
No Plan.  
[root@localhost ~]#
```

8 Mode batch

8.1 newusers

Mise à jour et création de comptes usager en mode batch.

En premier créer la liste des usagers dans un fichier (par exemple **liste.users**)

```
user1:secret:1001:3000::/home/user1:/bin/bash  
user2:secret:1002:3000::/home/user2:/bin/bash  
user3:secret:1003:3000::/home/user3:/bin/bash  
user4:secret:1004:3000::/home/user4:/bin/bash  
user5:secret:1005:3000::/home/user5:/bin/bash
```

Ensuite exécuter la commande :

```
[root@localhost ~]# newusers liste.users
```

8.2 chpasswd

Mise à jour des mots de passes mode batch.

En premier créer la liste dans un fichier (par exemple **liste.passwd**)

```
user1:secret1  
user2:secret2  
user3:secret3  
user4:secret4  
user5:secret5
```

Ensuite exécuter la commande :

```
[root@localhost ~]# cat liste.passed | chpasswd
```