

Dersim Besiktas
TP13 : Les utilisateurs et les droits

SOMMAIRE

1. La gestion des utilisateurs.....	2
2. La gestion des droits.....	11
3. La gestion des droits, compléments.....	15

1. La gestion des utilisateurs

On vérifie si les comptes utilisateurs daemon et luke existent on peut voir que seul daemon existe et son user id est 1

```
root@DEB13Server: ~# id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
root@DEB13Server: ~# id luke
id: 'luke' : utilisateur inexistant
root@DEB13Server: ~# _
```

Avec la commande **groupadd** je crée les groupes **jedi** et **rebelles**

```
root@DEB13Server: ~# groupadd jedi
root@DEB13Server: ~# groupadd rebelles
root@DEB13Server: ~# _
```

A l'aide de la commande **man useradd** je peux consulter le manuel

```
USERADD(8)                                     System Management Commands                                     USERADD(8)
NAME
  useradd - créer un nouvel utilisateur ou modifier les informations par défaut appliquées aux nouveaux utilisateurs
SYNOPSIS
  useradd [options] LOGIN
  useradd -D
  useradd -D [options]
DESCRIPTION
  useradd is a low level utility for adding users. On Debian, administrators should usually use adduser(8) instead.

  When invoked without the -D option, the useradd command creates a new user account using the values specified on the command line plus the default values from the system. Depending on command line options, the useradd command will update system files and may also create the new user's home directory and copy initial files.

  By default, a group will also be created for the new user (see -g, -N, -U, and USERGROUPS_ENAB).
OPTIONS
  The options which apply to the useradd command are:

  --badname
    Allow names that do not conform to standards.

  -b, --base-dir BASE_DIR
    The default base directory for the system if -d HOME_DIR is not specified. BASE_DIR is concatenated with the account name to define the home directory.

    If this option is not specified, useradd will use the base directory specified by the HOME variable in /etc/default/useradd, or /home by default.

  -c, --comment COMMENT
    Any text string. It is generally a short description of the account, and is currently used as the field for the user's full name.

  -d, --home-dir HOME_DIR
    The new user will be created using HOME_DIR as the value for the user's login directory. The default is to append the LOGIN name to BASE_DIR and use that as the login directory name. If the directory HOME_DIR does not exist, then it will be created unless the -M option is specified.

  -D, --defaults
    Consultez ci-dessous la sous-section « Modifier les valeurs par défaut ».

  -e, --expiredate EXPIRE_DATE
    The date on which the user account will be disabled. The date is specified in the format YYYY-MM-DD.

    If not specified, useradd will use the default expiry date specified by the EXPIRE variable in /etc/default/useradd, or an empty string (no expiry) by default.
```

je crée les comptes utilisateurs luke,vador et solo à l'aide de la commande useradd

Le paramètre g permet de mettre un utilisateur dans un groupe principal et le paramètre G pour que l'utilisateur puisse appartenir à un groupe secondaire

```
root@DEB13Server: ~#useradd -g jedi -G rebelles -m luke
root@DEB13Server: ~#useradd -g jedi -m vador
root@DEB13Server: ~#user add -g rebelles -m solo
root@DEB13Server: ~#useradd -g rebelles -m solo
root@DEB13Server: ~#id luke
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
root@DEB13Server: ~#id vador
uid=1003(vador) gid=1002(jedi) groupes=1002(jedi)
root@DEB13Server: ~#id solo
uid=1004(solo) gid=1003(rebelles) groupes=1003(rebelles)
root@DEB13Server: ~#
```

Avec la commande tail j'affiche les dernières lignes des fichiers

```
root@DEB13Server: ~#tail -3 /etc/passwd
luke:x:1002:1002::/home/luke:/bin/sh
vador:x:1003:1002::/home/vador:/bin/sh
solo:x:1004:1003::/home/solo:/bin/sh
root@DEB13Server: ~#tail -2 /etc/group
jedi:x:1002:
rebelles:x:1003:luke
root@DEB13Server: ~#_
```

Je mets le mot « password » pour l'utilisateur **luke**

```
root@DEB13Server: ~#passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Server: ~#
```

Depuis une nouvelle console je me log en tant que root et la a commande

usermod -s /bin/bash luke sert à modifier le shell par défaut de l'utilisateur luke

```
root@DEB13Server: ~#usermod -s /bin/bash luke
root@DEB13Server: ~#
```

Je me connecte sur l'utilisateur luke et je saisis la commande **id** puis je retourne sur la deuxième fenêtre de console pour être sur root

```
luke@DEB13Server:~$ id
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
luke@DEB13Server:~$ exit_
```

Je crée l'utilisateur leia avec la commande **useradd** et on peut constater que le nom du groupe est le même que celui du nom de l'utilisateur

```
root@DEB13Server: ~# useradd leia
root@DEB13Server: ~# id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB13Server: ~#_
```

Lors de la création de l'utilisateur , le répertoire n'a pas été créé car la création automatique n'a pas été activé

```
root@DEB13Server: ~# ls -l /home
total 20
drwx----- 5 guest guest 4096 17 déc. 15:25 guest
drwx----- 2 luke jedi 4096 17 déc. 16:51 luke
drwx----- 2 sio sio 4096 18 oct. 22:47 sio
drwx----- 2 solo rebelles 4096 17 déc. 16:52 solo
drwx----- 2 vador jedi 4096 17 déc. 16:51 vador
root@DEB13Server: ~#_
```

J'affecte leia au groupe secondaire rebelles avec le paramètre -G

```
root@DEB13Server: ~# usermod -G rebelles leia
root@DEB13Server: ~# id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1003(rebelles)
root@DEB13Server: ~#
```

Je fais la même chose mais pour l'affecter au groupe secondaire jedi

```
root@DEB13Server: ~# usermod -G jedi leia
root@DEB13Server: ~# id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi)
root@DEB13Server: ~#_
```

J'affecte leia aux groupes secondaire **jedi** et **rebelles**

```
root@DEB13Server: ~# usermod -G jedi,rebelles leia
root@DEB13Server: ~# id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB13Server: ~#_
```

Avec les guillemets l'utilisateur leia n'appartient plus à un groupe

```
root@DEB13Server: ~# usermod -G "" leia
root@DEB13Server: ~# id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB13Server: ~#_
```

A l'aide de l'option **a** je peux affecter un groupe secondaire sans retirer les autres groupes secondaires

```
root@DEB13Server: ~#usermod -G jedi leia
root@DEB13Server: ~#usermod -aG rebelles leia
root@DEB13Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB13Server: ~#
```

Je supprime l'utilisateur **leia**

```
root@DEB13Server: ~#userdel leia
root@DEB13Server: ~#_
```

Je recrée le compte **leia** mais cette fois-ci en lui créant un répertoire

```
root@DEB13Server: ~#useradd -m leia
root@DEB13Server: ~#cd /home/leia
root@DEB13Server: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls -l
total 0
-rw-rw-r-- 1 leia leia 0 17 déc. 17:37 fichier1
$ exit
root@DEB13Server: /home/leia#cd
root@DEB13Server: ~#
```

Je supprime le compte utilisateur leia ainsi que les fichiers

```
root@DEB13Server: ~# userdel -r leia
userdel : leia spool de courrier /var/mail/leia non trouvé
root@DEB13Server: ~# ls -l /home/leia
ls: impossible d'accéder à '/home/leia': Aucun fichier ou dossier de ce nom
root@DEB13Server: ~# id leia
id: 'leia' : utilisateur inexistant
root@DEB13Server: ~#_
```

Je recrée le compte leia à l'identique avec les mêmes uid et gid

```
root@DEB13Server: ~# groupadd -g 1007 leia
root@DEB13Server: ~# useradd -u 1007 -g leia -m -s /bin/bash leia
root@DEB13Server: ~# id leia
uid=1007(leia) gid=1007(leia) groupes=1007(leia)
root@DEB13Server: ~# passwd
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Server: ~#
```

Je crée le compte toor

```
root@DEB13Server: ~# useradd -u 0 -o -d /root -s /bin/bash toor
useradd attention: l'uid de toor, 0, est en dehors de la plage UID_MIN 1000 et UID_MAX 60000 .
root@DEB13Server: ~# id toor
uid=0(root) gid=1000(toor) groupes=0(root)
root@DEB13Server: ~# passwd toor
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Server: ~#_
```

Depuis une nouvelle console je me log sur le user **toor**

```
DEB13Server login: toor
Password:
Linux DEB13Server 6.12.48+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48-1 (2025-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@DEB13Server: ~#
```

Je crée un nouvel utilisateur en respectant la charte Debian

```
root@DEB13Server: ~#adduser palpatine
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour palpatine
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Is the information correct? [Y/n] y
root@DEB13Server: ~#id palpatine
uid=1005(palpatine) gid=1005(palpatine) groupes=1005(palpatine),100(users)
root@DEB13Server: ~#
```

Avec la commande **grep** j'extrais les caractéristiques de l'utilisateur **luke** et du groupe local **rebelles**

```
root@DEB13Server: ~#grep luke /etc/passwd
luke:x:1002:1002:~/home/luke:/bin/bash
root@DEB13Server: ~#grep rebelles /etc/group
rebelles:x:1003:luke
root@DEB13Server: ~#
```

2. La gestion des droits

Je crée l'arborescence de fichiers

```
root@DEB13Server: ~#mkdir /home/etoilenoire
root@DEB13Server: ~#cd /home/etoilenoire
root@DEB13Server: /home/etoilenoire#echo "voici les plans" > plans
root@DEB13Server: /home/etoilenoire#echo "c'est ouvert" > entree_secrete
root@DEB13Server: /home/etoilenoire#_
```

Je change le propriétaire et le groupe

```
root@DEB13Server: ~#cd
root@DEB13Server: ~#ls -ld /home/etoilenoire
drwxr-x--- 2 root root 4096 17 déc. 17:57 /home/etoilenoire
root@DEB13Server: ~#chown luke /home/etoilenoire
root@DEB13Server: ~#chgrp jedi /home/etoilenoire
root@DEB13Server: ~#chmod 750 /home/etoilenoire
root@DEB13Server: ~#ls -ld /home/etoilenoire
drwxr-x--- 2 luke jedi 4096 17 déc. 17:57 /home/etoilenoire
root@DEB13Server: ~#
```

J'affecte le fichier **plans** au groupe **jedi** et le fichier **entree_secrete** au groupe **rebelles**

```
root@DEB13Server: ~#chmod g=r,o=- /home/etoilenoire/*
root@DEB13Server: ~#chgrp jedi /home/etoilenoire/plans
root@DEB13Server: ~#chgrp rebelles /home/etoilenoire/entree_secrete
root@DEB13Server: ~#ls -l /home/etoilenoire/
total 8
-rw-r----- 1 root rebelles 13 17 déc. 17:57 entree_secrete
-rw-r----- 1 root jedi 16 17 déc. 17:57 plans
root@DEB13Server: ~#_
```

Je me connecte sur l'utilisateur luke, l'utilisateur a tout les droits sauf le droit de modifier le fichier plan

```
root@DEB13Server: ~#su - luke
luke@DEB13Server:~$ ls /home/etoilenoire/
entree_secrete plans
luke@DEB13Server:~$ cat /home/etoilenoire/plans
voici les plans
luke@DEB13Server:~$ cat /home/etoilenoire/entree_secrete
c'est ouvert
luke@DEB13Server:~$ cal > /home/etoilenoire/fichier
luke@DEB13Server:~$ ls /home/etoilenoire/
entree_secrete fichier plans
luke@DEB13Server:~$ rm /home/etoilenoire/fichier
luke@DEB13Server:~$ ls /home/etoilenoire/
entree_secrete plans
luke@DEB13Server:~$ echo "====" >> /home/etoilenoire/plans
-bash: /home/etoilenoire/plans: Permission non accordée
luke@DEB13Server:~$ exit_
```

L'utilisateur vador peut lister le répertoire etoilenoire mais ne peut pas lire le fichier **entree_secrete** et ne peut pas modifier le fichier **plans**

```
root@DEB13Server: ~#su - vador
$ ls /home/etoilenoire
entree_secrete plans
$ rm /home/etoilenoire/plans
rm : supprimer '/home/etoilenoire/plans' qui est protégé en écriture et est du type « regular file » ? y
rm: impossible de supprimer '/home/etoilenoire/plans': Permission non accordée
$ cal > /home/etoilenoire/fichier
-sh: 3: cannot create /home/etoilenoire/fichier: Directory nonexistent
$ cat /home/etoilenoire/plans
voici les plans
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$ echo "===" >> /home/etoilenoire/plans
-sh: 6: cannot create /home/etoilenoire/plans: Permission denied
$ exit
```

L'utilisateur solo n'a aucun accès aux fichiers du répertoire **etoilenoire**

```
root@DEB13Server: ~#su - solo
$ ls /home/etoilenoire
ls: impossible d'ouvrir le répertoire '/home/etoilenoire': Permission non accordée
$ cal > /home/etoilenoire/fichier
-sh: 2: cannot create /home/etoilenoire/fichier: Permission denied
$ rm -f /home/etoilenoire/fichier/entree_secrete
rm: impossible de supprimer '/home/etoilenoire/fichier/entree_secrete': Permission non accordée
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$ exit
```

Je supprime temporairement le droit d'exécution à l'aide de la commande **uptime**

```
root@DEB13Server: ~#whereis uptime
uptime: /usr/bin/uptime /usr/share/man/man1/uptime.1.gz
root@DEB13Server: ~#whatis uptime
uptime (1) - Indiquer depuis quand le système a été mis en route
root@DEB13Server: ~#uptime
 18:40:08 up 1:59, 2 users, load average: 0,07, 0,02, 0,00
root@DEB13Server: ~#ls -l /usr/bin/uptime
-rwxr-xr-x 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Server: ~#chmod o-x /usr/bin/uptime
root@DEB13Server: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Server: ~#su - luke
luke@DEB13Server:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
luke@DEB13Server:~$ exit

root@DEB13Server: ~#chmod o+x /usr/bin/uptime
root@DEB13Server: ~#ls -l /usr/bin/uptime
-rwxr-xr-x 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Server: ~#su - luke
luke@DEB13Server:~$ uptime
 18:42:51 up 2:02, 2 users, load average: 0,00, 0,00, 0,00
luke@DEB13Server:~$ _
```

3. La gestion des droits, compléments

J'ajoute les droits **SGID** et **sticky-bit** au répertoire **etoilenoire**

```
root@DEB13Server: ~#chmod 3770 /home/etoilenoire/
root@DEB13Server: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 17 déc. 18:16 /home/etoilenoire/
root@DEB13Server: ~#echo "fichier un" > /home/etoilenoire/f1
root@DEB13Server: ~#su - luke
luke@DEB13Server:~$ echo "bonjour" > /home/etoilenoire/f2
luke@DEB13Server:~$ exit
root@DEB13Server: ~#su - vador
$ echo "bonjour" > /home/etoilenoire/f3
$ exit
root@DEB13Server: ~#ls -l /home/etoilenoire/f?
-rw-r--r-- 1 root jedi 11 17 déc. 18:44 /home/etoilenoire/f1
-rw-r--r-- 1 luke jedi 8 17 déc. 18:44 /home/etoilenoire/f2
-rw-r--r-- 1 vador jedi 8 17 déc. 18:48 /home/etoilenoire/f3
root@DEB13Server: ~#_
```

Je conserve le droit **sticky-bit**

```
root@DEB13Server: ~#su - vador
$ rm /home/etoilenoire/f2
rm: supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « regular file » ? y
rm: impossible de supprimer '/home/etoilenoire/f2': Opération non permise
$ exit
root@DEB13Server: ~#_
```

Je supprime le droit **sticky-bit**

```
root@DEB13Server: ~#chmod -t /home/etoilenoire/
root@DEB13Server: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 17 déc. 18:47 /home/etoilenoire/
root@DEB13Server: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « regular file » ? y
$ exit
root@DEB13Server: ~#
```

Seul **root** et les membres du groupe **disk** peuvent formater

```
root@DEB13Server: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 17 déc. 16:40 /dev/sda1
root@DEB13Server: ~#
```

Je copie les fichiers du répertoire **etoilenoire** dans **/tmp** à l'aide de la commande **cp -p**

```
root@DEB13Server: ~#cp -p /home/etoilenoire/* /tmp
root@DEB13Server: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 17 déc. 17:57 /tmp/entree_secrete
-rw-r----- 1 root jedi 16 17 déc. 17:57 /tmp/plans
root@DEB13Server: ~#_
```

```
root@DEB13Server: ~#chown luke /tmp/entree_secrete
root@DEB13Server: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke rebelles 13 17 déc. 17:57 /tmp/entree_secrete
root@DEB13Server: ~#
```

A partir de l'utilisateur **luke** je test les droits d'accès

```
root@DEB13Server: ~#su - luke
luke@DEB13Server:~$ cat /tmp/entree_secrete
c'est ouvert
luke@DEB13Server:~$ echo "=====" >> /tmp/entree_secrete
luke@DEB13Server:~$ cat /tmp/entree_secrete
c'est ouvert
=====  
luke@DEB13Server:~$ /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
luke@DEB13Server:~$ exit
```

A partir du compte **solo** :

```
root@DEB13Server: ~#cat /tmp/entree_secrete
c'est ouvert
=====  
root@DEB13Server: ~#echo "+++++" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB13Server: ~#exit
```

A partir du compte **root** :

```
root@DEB13Server: ~#cat /tmp/entree_secrete
c'est ouvert
root@DEB13Server: ~#echo "+++++" >> /tmp/entree_secrete
root@DEB13Server: ~#cat /tmp/entree_secrete
c'est ouvert
+++++=
root@DEB13Server: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB13Server: ~#_
```

```
root@DEB13Server: ~#ls -l /etc/shadow
-rw-r----- 1 root shadow 1274 17 déc. 19:25 /etc/shadow
root@DEB13Server: ~#ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 118168 19 avril 2025 /usr/bin/passwd
root@DEB13Server: ~#_
```