
TP13 : Les utilisateurs et les droits

SOMMAIRE :

1. La gestion des utilisateurs.	1
2. La gestion des droits.	8
3. La gestion des droits, compléments.	13

1. La gestion des utilisateurs.

J'utilise la commande id pour savoir si le compte daemon et luke existe :

```
root@DEB13Serveur: ~#id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
root@DEB13Serveur: ~#id luke
id: 'luke' : utilisateur inexistant
root@DEB13Serveur: ~#_
```

Après avoir effectué les commandes je me rend compte que le compte daemon existe mais le compte luke n'existe pas.

Je crée ensuite les groupes jedi et rebelles :

```
root@DEB13Serveur: ~#groupadd jedi
root@DEB13Serveur: ~#groupadd rebelles
root@DEB13Serveur: ~#_
```

TP13 : Les utilisateurs et les droits

Je consulte le manuel en ligne afin de découvrir les options de la commande (useradd) avec l'aide de la commande man useradd :

```
USERADD(8)                                System Management Commands

NOM
    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. Depending on command line options, the useradd command will update system files and may create a 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 system's base directory.

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

    -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 use the user's login directory name. If the directory HOME_DIR does not exist, then it will be created unless the -D 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 by default.
```

Je crée le compte luke qui appartient au groupe jedi (principal) et au groupe rebelles (secondaire) :

```
root@DEB13Serveur: ~#useradd -g jedi -G rebelles -m luke
root@DEB13Serveur: ~#-g jedi -m vador
-bash: -g : commande introuvable
root@DEB13Serveur: ~#useradd -g jedi -m vador
root@DEB13Serveur: ~#useradd -g rebelles -m solo
root@DEB13Serveur: ~#id luke
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
root@DEB13Serveur: ~#id vador
uid=1003(vador) gid=1002(jedi) groupes=1002(jedi)
root@DEB13Serveur: ~#id solo
uid=1004(solo) gid=1003(rebelles) groupes=1003(rebelles)
root@DEB13Serveur: ~#
```

TP13 : Les utilisateurs et les droits

J'affiche les dernières lignes des fichiers /etc/passwd et /etc/group :

```
root@DEB13Serveur: ~#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@DEB13Serveur: ~#tail -2 /etc/group
jedi:x:1002:
rebelles:x:1003:luke
root@DEB13Serveur: ~#
```

Je mets ensuite le mot (password) comme mot de passe à l'utilisateur luke :

```
root@DEB13Serveur: ~#passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Serveur: ~#
```

j'ouvre une seconde console et je me connecte sous le compte de luke :

```
Debian GNU/Linux 13 DEB13Serveur tty2
DEB13Serveur login: luke
Password:
Linux DEB13Serveur 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.
$ _
```

Je me deconnecte de luke et je retourne sur root et je modifie le compte utilisateur luke pour remplacer le shell sh par bash :

```
root@DEB13Serveur: ~#usermod -s /bin/bash luke
root@DEB13Serveur: ~#
```

Je me reconnecte sur le compte de luke dans la seconde console et j'observe le nouveau prompt :

```
luke@DEB13Serveur:~$ id
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
luke@DEB13Serveur:~$ _
```

TP13 : Les utilisateurs et les droits

Je crée l'utilisateur leia dans la première console avec la commande useradd :

```
root@DEB13Serveur: ~#useradd leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB13Serveur: ~#_
```

Son groupe principal est : gid=1005(leia)

Je constate que le répertoire leia n'a pas été créé :

```
root@DEB13Serveur: ~#ls -l /home
total 20
drwx----- 7 guest guest 4096 19 déc. 22:26 guest
drwx----- 2 luke jedi 4096 21 déc. 15:16 luke
drwx----- 2 sio sio 4096 17 déc. 10:07 sio
drwx----- 2 solo rebelles 4096 21 déc. 15:05 solo
drwx----- 2 vador jedi 4096 21 déc. 15:04 vador
root@DEB13Serveur: ~#
```

J'affecte l'utilisateur leia au groupe rebelles comme groupe secondaire :

```
root@DEB13Serveur: ~#usermod -G rebelles leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1003(rebelles)
root@DEB13Serveur: ~#
```

J'affecte maintenant leia au groupe jedi et leia quitte le group rebelles :

```
root@DEB13Serveur: ~#usermod -G jedi leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi)
root@DEB13Serveur: ~#
```

J'affecte ensuite leia aux groupe jedi et rebelles :

```
root@DEB13Serveur: ~#usermod -G jedi,rebelles leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB13Serveur: ~#
```

TP13 : Les utilisateurs et les droits

Maintenant nous voulons que leia n'appartiennent plus à aucun groupe secondaire :

```
root@DEB13Serveur: ~#usermod -G "" leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB13Serveur: ~#
```

On veut ajouter l'utilisateur à un groupe secondaire sans le retirer des autres groupes secondaires avec l'option -a :

```
root@DEB13Serveur: ~#usermod -G jedi leia
root@DEB13Serveur: ~#usermod -aG rebelles leia
root@DEB13Serveur: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB13Serveur: ~#_
```

Je supprime maintenant le compte leia :

```
root@DEB13Serveur: ~#userdel leia
root@DEB13Serveur: ~#_
```

Je recrée le compte leia avec cette fois-ci une répertoire de connexion et à partir du compte de leia je crée un répertoire ainsi qu'un fichier :

```
root@DEB13Serveur: ~#useradd -m leia
root@DEB13Serveur: ~#cd /home/leia
root@DEB13Serveur: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls -l
total 0
-rw-rw-r-- 1 leia leia 0 21 déc. 15:32 fichier1
$ exit
root@DEB13Serveur: /home/leia#cd
root@DEB13Serveur: ~#
```

Je supprime le compte utilisateur et les fichiers de son répertoire de connexion :

```
root@DEB13Serveur: ~#userdel -r leia
userdel : leia spool de courrier /var/mail/leia non trouvé
root@DEB13Serveur: ~# userdel -r leia
userdel : l'utilisateur 'leia' n'existe pas
root@DEB13Serveur: ~#ls -l /home/leia
ls: impossible d'accéder à '/home/leia': Aucun fichier ou dossier de ce nom
root@DEB13Serveur: ~#id leia
id: 'leia' : utilisateur inexistant
root@DEB13Serveur: ~#
```

TP13 : Les utilisateurs et les droits

Je recrée le compte leia à l'identique :

```
root@DEB13Serveur: ~#groupadd -g 1007 leia
root@DEB13Serveur: ~#useradd -u 1007 -g leia -m -s /bin/bash leia
root@DEB13Serveur: ~#id leia
uid=1007(leia) gid=1007(leia) groupes=1007(leia)
root@DEB13Serveur: ~#passwd leia
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Serveur: ~#
```

Je crée le compte toor ayant les mêmes droits que root :

```
root@DEB13Serveur: ~#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@DEB13Serveur: ~#id toor
uid=0(root) gid=1008(toor) groupes=0(root)
root@DEB13Serveur: ~#passwd toor
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB13Serveur: ~#
```

J'ouvre la seconde console et je me connecte au compte toor :

```
Debian GNU/Linux 13 DEB13Serveur tty2
DEB13Serveur login: toor
Password:
Linux DEB13Serveur 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@DEB13Serveur: ~#
```

J'ajoute le compte utilisateur palpatine :

```
root@DEB13Serveur: ~#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@DEB13Serveur: ~#
```

TP13 : Les utilisateurs et les droits

```
root@DEB13Serveur: ~#id palpatine
uid=1005(palpatine) gid=1005(palpatine) groupes=1005(palpatine),100(users)
root@DEB13Serveur: ~#
```

J'affiche les caractéristiques de l'utilisateur local luke au groupe local rebelles :

```
root@DEB13Serveur: ~#grep luke /etc/passwd
luke:x:1002:1002::/home/luke:/bin/bash
root@DEB13Serveur: ~#grep rebelles /etc/group
rebelles:x:1003:luke
root@DEB13Serveur: ~#
```

J'affiche les caractéristiques de l'utilisateur luke et du groupe jedi :

```
root@DEB13Serveur: ~#getent passwd luke
luke:x:1002:1002::/home/luke:/bin/bash
root@DEB13Serveur: ~#getent passwd jedi
root@DEB13Serveur: ~#getent group jedi
jedi:x:1002:
root@DEB13Serveur: ~#_
```

2. La gestion des droits.

Je crée une arborescence de fichiers :

```
root@DEB13Serveur: ~#mkdir /home/etoilenoire
root@DEB13Serveur: ~#cd /home/etoilenoire
root@DEB13Serveur: /home/etoilenoire#echo "voici les plans" > plans
root@DEB13Serveur: /home/etoilenoire#echo "c'est ouvert" > entree_secrete
root@DEB13Serveur: /home/etoilenoire#_
```

Je change les caractéristiques du répertoire etoilenoire :

```
root@DEB13Serveur: ~#ls -ld /home/etoilenoire
drwxr-xr-x 2 root toor 4096 21 déc. 15:52 /home/etoilenoire
root@DEB13Serveur: ~#chown luke /home/etoilenoire
root@DEB13Serveur: ~#chgrp jedi /home/etoilenoire
root@DEB13Serveur: ~#chmod 750 /home/etoilenoire
root@DEB13Serveur: ~#ls -ld /home/etoilenoire
drwxr-x--- 2 luke jedi 4096 21 déc. 15:52 /home/etoilenoire
root@DEB13Serveur: ~#_
```

TP13 : Les utilisateurs et les droits

Je change les caractéristiques des fichiers :

```
root@DEB13Serveur: ~#chmod g=r,o=- /home/etoilenoire/*
root@DEB13Serveur: ~#chgrp jedi /home/etoilenoire/plans
root@DEB13Serveur: ~#chgrp rebelles /home/etoilenoire/entree_secrete
root@DEB13Serveur: ~#ls -l /home/etoilenoire/
total 8
-rw-r----- 1 root rebelles 13 21 déc. 15:52 entree_secrete
-rw-r----- 1 root jedi 16 21 déc. 15:52 plans
root@DEB13Serveur: ~#_
```

Test des accès :

à partir du compte luke :

```
root@DEB13Serveur: ~#su - luke
luke@DEB13Serveur:~$ ls /home/etoilenoire/
entree_secrete plans
luke@DEB13Serveur:~$ cat /home/etoilenoire/plans
voici les plans
luke@DEB13Serveur:~$ cat /home/etoilenoire/entree_secrete
c'est ouvert
luke@DEB13Serveur:~$ cal > /home/etoilenoire/fichier
luke@DEB13Serveur:~$ ls /home/etoilenoire/
entree_secrete fichier plans
luke@DEB13Serveur:~$ rm /home/etoilenoire/fichier
luke@DEB13Serveur:~$ ls /home/etoilenoire/
entree_secrete plans
luke@DEB13Serveur:~$ echo "====" >> /home/etoilenoire/plans
-bash: /home/etoilenoire/plans: Permission non accordée
luke@DEB13Serveur:~$
```

Maintenant à partir du compte vador :

```
root@DEB13Serveur: ~#su - vador
$ ls /home/etoilenoire
entree_secrete plans
$ rm /home/etoilenoire/plans
rm: impossible de supprimer '/home/etoilenoire/plans': Permission non accordée
$ cal > /home/etoilenoire/fichier
-sh: 3: cannot create /home/etoilenoire/fichier: Permission denied
$ cat /home/etoilenoire/plans
cat: /home/etoilenoire/plans: Permission non accordée
$ 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
$
```

TP13 : Les utilisateurs et les droits

à partir du compte solo :

```
root@DEB13Serveur: ~#su - solo
$ ls /home/etoilenoire
ls: impossible d'ouvrir le répertoire '/home/etoilenoire': Permission non accordée
$ cat > /home/etoilenoire/fichier
-sh: 2: cannot create /home/etoilenoire/fichier: Permission denied
$ rm -f /home/etoilenoire/entree_secrete
rm: impossible de supprimer '/home/etoilenoire/entree_secrete': Permission non accordée
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$
```

Je supprime temporairement le droit d'execution à la commande uptime et je teste les conséquences à partir du compte luke :

```
root@DEB13Serveur: ~#wheris uptime
-bash: wheris : commande introuvable
root@DEB13Serveur: ~#whatis uptime
uptime (1)          - Indiquer depuis quand le système a été mis en route
root@DEB13Serveur: ~#uptime
 16:17:15 up  1:26,  2 users,  load average: 0,03, 0,01, 0,00
root@DEB13Serveur: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Serveur: ~#chmod o-x /usr/bin/uptime
root@DEB13Serveur: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Serveur: ~#su - luke
luke@DEB13Serveur:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
luke@DEB13Serveur:~$ _
```

```
root@DEB13Serveur: ~#chmod o+x /usr/bin/uptime
root@DEB13Serveur: ~#ls -l /usr/bin/uptime
-rwxr-xr-x 1 root root 14648 30 juil. 13:58 /usr/bin/uptime
root@DEB13Serveur: ~#su - luke
luke@DEB13Serveur:~$ uptime
 16:19:32 up  1:29,  2 users,  load average: 0,00, 0,00, 0,00
luke@DEB13Serveur:~$ _
```

TP13 : Les utilisateurs et les droits

3. La gestion des droits, compléments.

J'ajoute les droits spéciaux au répertoire etoilenoire et je vérifie l'impact :

compte luke :

```
root@DEB13Serveur: ~#chmod 3770 /home/etoilenoire
root@DEB13Serveur: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 21 déc. 16:04 /home/etoilenoire/
root@DEB13Serveur: ~#echo "fichier un" > /home/etoilenoire/f1
root@DEB13Serveur: ~#su - luke
luke@DEB13Serveur:~$ echo "bonjour" > /home/etoilenoire/f2
luke@DEB13Serveur:~$ _
```

Compte vador :

```
root@DEB13Serveur: ~#su - vador
$ echo "bonjour" > /home/etoilenoire/f3
$ exit
root@DEB13Serveur: ~#ls -l /home/etoilenoire/f?
-rw-r--r-- 1 root jedi 11 21 déc. 16:22 /home/etoilenoire/f1
-rw-r--r-- 1 luke jedi 8 21 déc. 16:22 /home/etoilenoire/f2
-rw-r--r-- 1 vador jedi 8 21 déc. 16:24 /home/etoilenoire/f3
root@DEB13Serveur: ~#
```

Maintenant vador va essayer de détruire le fichier de luke :

```
root@DEB13Serveur: ~#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
$
```

Je supprime le droit sticky-bit :

```
root@DEB13Serveur: ~#chmod -t /home/etoilenoire/
root@DEB13Serveur: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 21 déc. 16:24 /home/etoilenoire/
root@DEB13Serveur: ~#su - vador
$ rm /home/etoilenoire/f2
rm: supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « regular file » ? y
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce nom
$ exit
root@DEB13Serveur: ~#
```

TP13 : Les utilisateurs et les droits

Je regarde qui peut formater la partition /dev/sdal :

```
root@DEB13Serveur: ~#chmod -t /home/etoilenoire/
root@DEB13Serveur: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 21 déc. 16:24 /home/etoilenoire/
root@DEB13Serveur: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « regular file » ? y
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce nom
$ exit
root@DEB13Serveur: ~#
```

Seuls root et les membres du groupe disk peuvent formater cette partition.

Je copie les fichiers du répertoire etoilenoire dans /tmp en conservant leurs attributs :

```
root@DEB13Serveur: ~#cp -p /home/etoilenoire/* /tmp
root@DEB13Serveur: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 21 déc. 15:52 /tmp/entree_secrete
-rw-r----- 1 root jedi      16 21 déc. 15:52 /tmp/plans
root@DEB13Serveur: ~#_
```

Je donne le fichier entree_secrete à luke :

```
root@DEB13Serveur: ~#chown luke /tmp/entree_secrete
root@DEB13Serveur: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke rebelles 13 21 déc. 15:52 /tmp/entree_secrete
root@DEB13Serveur: ~#_
```

Je teste les accès (r,w,x) au fichier /tmp/entree_secrete à partir du compte luke :

```
root@DEB13Serveur: ~#su - luke
luke@DEB13Serveur:~$ cat /tmp/entree_secrete
c'est ouvert
luke@DEB13Serveur:~$ echo "=====" >> /tmp/entree_secrete
luke@DEB13Serveur:~$ cat /tmp/entree_secrete
c'est ouvert
=====
luke@DEB13Serveur:~$ /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
luke@DEB13Serveur:~$ _
```

TP13 : Les utilisateurs et les droits

à partir du compte solo :

```
root@DEB13Serveur: ~#su - solo
$ cat /tmp/entree_secrete
c'est ouvert
=====
$ echo "+++++" >> /tmp/entree_secrete
-sh: 2: cannot create /tmp/entree_secrete: Permission denied
$
```

à partir du compte root :

```
root@DEB13Serveur: ~#cat /tmp/entree_secrete
c'est ouvert
=====
root@DEB13Serveur: ~# echo "+="+="+=" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB13Serveur: ~#cat /tmp/entree_secrete
c'est ouvert
=====
root@DEB13Serveur: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB13Serveur: ~#
```

Je visualise les droits du fichier shadow et de la commande passwd :

```
root@DEB13Serveur: ~#ls -l /etc/shadow
-rw-r----- 1 root shadow 1346 21 déc. 15:46 /etc/shadow
root@DEB13Serveur: ~#ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 118168 19 avril 2025 /usr/bin/passwd
root@DEB13Serveur: ~#_
```