TP13 : Les utilisateurs et les droits

Sommaire

1. La gestion des utilisateurs.

Vérification de l’existence des comptes utilisateurs daemon et luke :

Daemon existe, son uid est 1, son gid est 1 et son groupes est 1 et Luke est inexistants

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

Création des groupes jedi et rebelles a l’aide de la commande groupadd

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

Consultation du manuel en ligne pour découvrir les options de la commande useradd a l’aide de la commande man useradd

```
USERADD(8)                                  System Management Commands                                  USERADD(8)

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 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.
Manual page useradd(8) line 1 (press h for help or q to quit)
```

Création des comptes utilisateurs luke, vador et solo, Puis visualisation de ces derniers

```
root@DEB13Server: ~#useradd -g jedi -G rebelles -m luke
root@DEB13Server: ~#useradd -g jedi -m vador
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: ~#_
```

Affichage des dernières lignes des fichiers /etc/passwd et /etc/group a l'aide de la commande tail

```
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: ~#
```

Ajout du mot « password » comme mot de passe à 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: ~#_
```

Ouverture d'une deuxième console a l'aide des touches Ctrl+alt+F2 puis connexion en tant que luke

```
Debian GNU/Linux 13 DEB13Server tty2

DEB13Server login: luke
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.
$ _
```

Déconnexion de luke puis a l'aide des touches Ctrl+alt+F1 pour retourner sur la première console puis utilisation de la commande usermod -s /bin/bash luke pour modifiez le compte utilisateur luke afin de remplacer le shell sh par bash

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

Reconnection sous le compte de luke dans la seconde console (Ctrl+alt+F2) et Observation du prompt

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

Création de l'utilisateur leia dans la première console (Ctrl+alt+F1) a l'aide de la commande useradd et son group principale est 1005

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

Non le répertoire personnel de l'utilisateur n'a pas été créer car la commande -m n'a pas été utiliser

```
root@DEB13Server: ~#ls -l /home
total 20
drwx------ 5 guest guest    4096 18 déc.  15:43 guest
drwx------ 2 luke  jedi     4096 18 déc.  16:45 luke
drwx------ 2 sio   sio      4096 18 oct.  22:47 sio
drwx------ 2 solo  rebelles 4096 18 déc.  16:31 solo
drwx------ 2 vador jedi     4096 18 déc.  16:30 vador
root@DEB13Server: ~#
```

Affectation de l'utilisateur leia au groupe rebelles comme groupe secondaire

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

Affectation de leia au groupe jedi. Leia quitte donc le groupe rebelles

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

Affectation de leia aux groupes 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: ~#_
```

Grâce a la commande usermod -G ‘’’’ leia on fait en sorte que leia n’appartienne a aucun groupe secondaire

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

Ajout du groupes secondaires rebelles a leia sans le supprimer du groupe secondaire jedi grâce a la commande -aG

```
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: ~#_
```

Suppression de l’utilisateur leia

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

On recrée le compte leia avec cette fois-ci un répertoire de connexion (commande -m) a partir du compte leia, et création d’un répertoire ainsi qu’un fichier

```
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 19 déc.  18:12 fichier1
$ exit
root@DEB13Server: /home/leia#cd
root@DEB13Server: ~#_
```

Suppression du compte utilisateur leia et les fichiers de son répertoire de connexion

```
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: ~#_
```

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

Création d’un compte toor et il va avoir les mêmes droits que root

```
root@DEB13Server: ~#useradd -u 0 -o -d /root -s /bin/bash toor
```

```
root@DEB13Server: ~#id toor
uid=0(root) gid=1008(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: ~#_
```

Ouverture d’une seconde fenêtre a l’aide des touches Ctrl+alt+F2 et connexion en tant que toor

```
Debian GNU/Linux 13 DEB13Server tty2

DEB13Server login: toor
Password:
^[[3^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: ~#_
```

Création d’un compte utilisateur (palpatine) respectant la charte Debian avec la commande adduser

```
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: ~#
```

Affichage des caractéristiques de l’utilisateur local 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.

Création d’une 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#
```

Changement des caractéristiques du répertoire etoilenoire

On change son propriétaire qui sera luke, son groupe qui sera jedi et on va enlever le droit de lecture et d’exécution pour les autres

```
root@DEB13Server: /home/etoilenoire#cd
root@DEB13Server: ~#ls -ld /home/etoilenoire
drwxr-xr-x 2 root toor 4096 20 déc.  16:12 /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 20 déc.  16:12 /home/etoilenoire
root@DEB13Server: ~#_
```

Changement des caractéristiques des fichiers

Les groupes n'auront que le droit de lecture et les autres aucun et on affilie 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 20 déc.  16:12 entree_secrete
-rw-r----- 1 root jedi     16 20 déc.  16:12 plans
root@DEB13Server: ~#_
```

Test des accès a partir du compte luke

connexion en tant que luke avec la commande su – luke (sans mdp)

```
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:~$ echo "====" >> /home/etoilenoire/plans
-bash: /home/etoilenoire/plans: Permission non accordée
luke@DEB13Server:~$ exit
```

Test des accès a partir du compte vador

connexion en tant que vador avec la commande su – vador (sans mdp)

```
root@DEB13Server: ~#su - vador
$ ls /home/etoilenoire
entree_secrete  fichier  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: Permission denied
$ 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_
```

Test des accès a partir du compte solo

connexion en tant que solo avec la commande su – solo (sans mdp)

```
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/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
$ exit_
```

Teste des conséquences à partir du compte luke

```
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
 17:58:46 up  2:24,  2 users,  load average: 0,00, 0,00, 0,00
```

On enlever le droit d’exécution au autres a l’aide de la commande chmod o-x /usr/bin/uptime sur la capture suivante on peut voir qu’il ne l’on plus alors qu’il l’avait avant. On remarque que quand on se log en luke et que l’on tape uptime la permission n’est pas accordée

```
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
```

On remet les droits d'execution au autres et donc quand on se log en luke et que l'on tape la commande uptime on y a bien accès

```
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
 18:03:51 up  2:29,  2 users,  load average: 0,12, 0,04, 0,01
luke@DEB13Server:~$ exit_
```

3. La gestion des droits, compléments.

Ajout des droits SGID et sticky-bit au répertoire etoilenoire

Pour vérifier l'impact de ces droits on va créer des fichiers dans le répertoire etoilenoire sous le compte root on va créer le fichier f, sous le compte luke on va créer le fichier f2 et sous le compte vador on va créer le fichier f3

```
root@DEB13Server: ~#chmod 3770 /home/etoilenoire/
root@DEB13Server: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 20 déc.  17:42 /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 20 déc.  18:07 /home/etoilenoire/f1
-rw-r--r-- 1 luke  jedi  8 20 déc.  18:08 /home/etoilenoire/f2
-rw-r--r-- 1 vador jedi  8 20 déc.  18:09 /home/etoilenoire/f3
root@DEB13Server: ~#
```

On va essayer de détruire le fichier de luke avec vador

On 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: ~#
```

On supprime le droit sticky-bit

```
root@DEB13Server: ~#chmod -t /home/etoilenoire/
root@DEB13Server: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 20 déc.  18:09 /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
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce nom
$ exit
root@DEB13Server: ~#
```

On constate que seuls root et les membres du groupe disk peuvent formater cette partition grâce a la commande ls -l /dev/sda1

```
root@DEB13Server: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 20 déc.  15:35 /dev/sda1
root@DEB13Server: ~#_
```

L'administrateur copie les fichiers du répertoire etoilenoire dans /tmp en conservant leurs attributs notamment grâce a l'option -p

```
root@DEB13Server: ~#cp -p /home/etoilenoire/* /tmp
root@DEB13Server: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 20 déc.  16:12 /tmp/entree_secrete
-rw-r----- 1 root jedi     16 20 déc.  16:12 /tmp/plans
root@DEB13Server: ~#_
```

L'administrateur donne le fichier entree_secrete à luke

```
root@DEB13Server: ~#chown luke /tmp/entree_secrete
root@DEB13Server: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke rebelles 13 20 déc.  16:12 /tmp/entree_secrete
root@DEB13Server: ~#_
```

Test des accès (r,w,x) au fichier /tmp/entree_secrete

A partir du compte luke :

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

Visualisation des droits du fichier shadow et de la commande passwd