TP13 : Les utilisateurs et les droits

Table des matières

1.La gestion des utilisateurs

```
guest@deb12server:~$ id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
guest@deb12server:~$ id luke
id: « luke » : utilisateur inexistant
guest@deb12server:~$ _
```

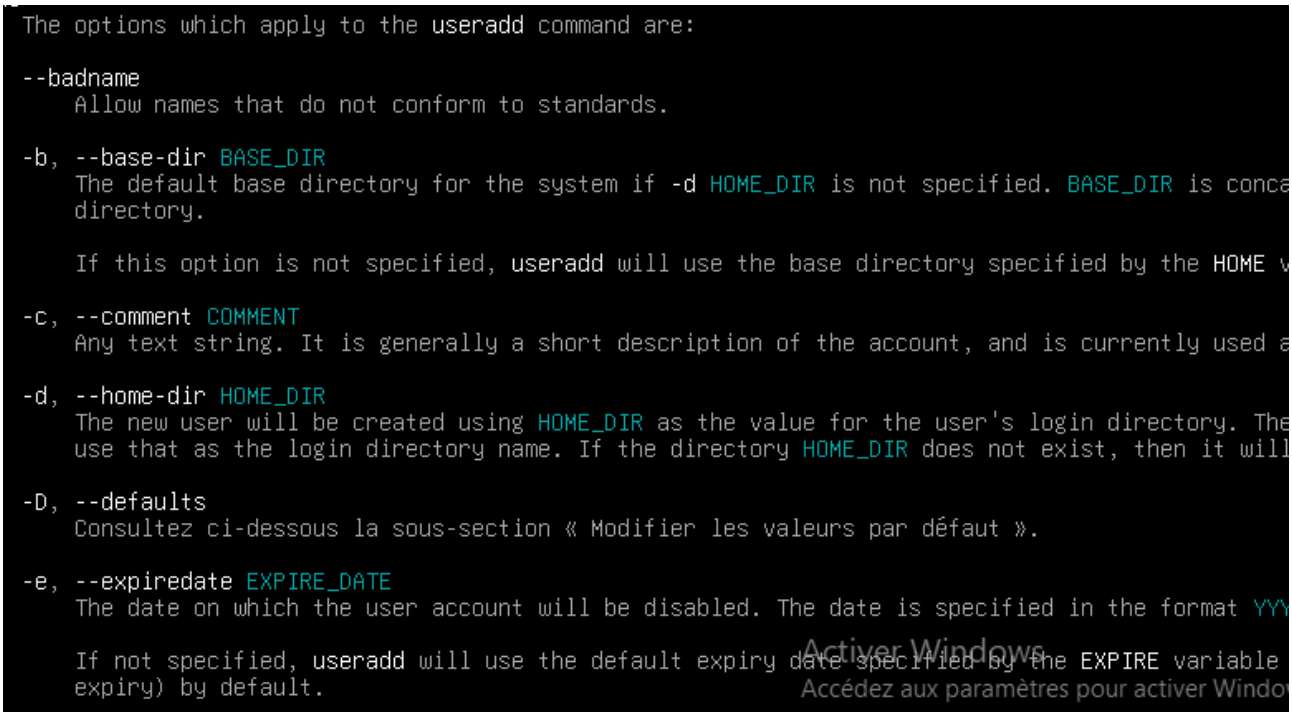
Daemon existe son uid est 1 et gid est 1 et son groupe est 1

luke n’existe pas

j’ai créé les groupes

```
root@deb12server: ~#groupadd jedi
root@deb12server: ~#groupadd rebelles
root@deb12server: ~#_
```

Je consulte le manuel pour découvrir les options de la commande useradd



Je créé des compte utilisatuer pour luke vador et solo puis je les visualise

```
root@deb12server: ~#useradd -g jedi -G rebelles -m luke
root@deb12server: ~#useradd -g jedi -m vador
root@deb12server: ~#useradd -g rebelles -m solo
root@deb12server: ~#id luke
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
root@deb12server: ~#id vador
uid=1003(vador) gid=1002(jedi) groupes=1002(jedi)
root@deb12server: ~#id solo
uid=1004(solo) gid=1003(rebelles) groupes=1003(rebelles)
```

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

```
root@deb12server: ~#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@deb12server: ~#tail -2 /etc/group
jedi:x:1002:
rebelles:x:1003:luke
```

je vien de changez le mot de passe de luke par « password »

```
root@deb12server: ~#passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
```

je vien de me connecter au compte de luke

```
deb12server login: luke
Password:
Linux deb12server 6.1.0-25-amd64
```

Je me de logue de Luke afin de remplacer le shell sh par bash

```
root@deb12server: ~#usermod -s /bin/bash luke
root@deb12server: ~#
```

Maintenant je me reconnecte a luke et j'observe le nouveau prompt

```
luke@deb12server:~$ id
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
luke@deb12server:~$
```

je crée un utilisateur Leia depuis le root et regarde ans quelle group il se situe

```
root@deb12server: ~#useradd leia
root@deb12server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@deb12server: ~#
```

son groupe principal est leia

non le répertoire personnel de l'utilisateur de leia n'est pas créé

```
root@deb12server: ~#ls -l /home
total 20
drwx------ 2 axel  axel     4096 27 sept. 15:31 axel
drwx------ 4 guest guest    4096 19 déc.  21:53 guest
drwxr-xr-x 2 luke  jedi     4096 20 déc.  16:10 luke
drwxr-xr-x 2 solo  rebelles 4096 20 déc.  15:51 solo
drwxr-xr-x 2 vador jedi     4096 20 déc.  15:50 vador
```

J'affecte leia au groupe rebelles

```
root@deb12server: ~#usermod -G rebelles leia
root@deb12server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1003(rebelles)
root@deb12server: ~#
```

J'affecte Leia au groupe jedi donc elle quitte le groupe rebelles

```
root@deb12server: ~#usermod -G jedi leia
root@deb12server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi)
root@deb12server: ~#
```

J’affecte maintenant Leia au deux groupes

```
root@deb12server: ~#usermod -G jedi,rebelles leia
root@deb12server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
```

Maintenant on veut que leia n’appartienne plus à aucun groupe secondaire

```
root@deb12server: ~#usermod -G "" leia
root@deb12server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
```

Je supprime le compte Leia

```
root@deb12server: ~#userdel leia
root@deb12server: ~#
```

je recréé le compte leia avec cette fois-ci un répertoire de connexion. A partir du compte leia, créez un répertoire ainsi qu’un fichier

```
root@deb12server: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls -l
total 0
-rw-r--r-- 1 leia leia 0 20 déc.  16:42 fichier1
$ exit
root@deb12server: /home/leia#cd
```

Je supprime le compte leia et les fichiers de son répertoire de connexion

```
root@deb12server: ~#userdel -r leia
userdel : leia spool de courrier /var/mail/leia non trouvé
root@deb12server: ~#ls -l /home/leia
ls: impossible d'accéder à '/home/leia': Aucun fichier ou dossier de ce type
root@deb12server: ~#id leia
id: « leia » : utilisateur inexistant
```

Je recréé le compte leia à l’identique avec les mêmes uid et gid

```
id: « leia » : utilisateur inexistant
root@deb12server: ~#groupadd -g 1007 leia
root@deb12server: ~#useradd -u 1007 -g leia -m -s /bin/bash leia
root@deb12server: ~#id leia
uid=1007(leia) gid=1007(leia) groupes=1007(leia)
root@deb12server: ~#passwd leia
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Les mots de passe ne correspondent pas.
Mot de passe : Erreur de manipulation du jeton d'authentification
passwd : mot de passe inchangé
root@deb12server: ~#passwd leia
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@deb12server: ~#_
```

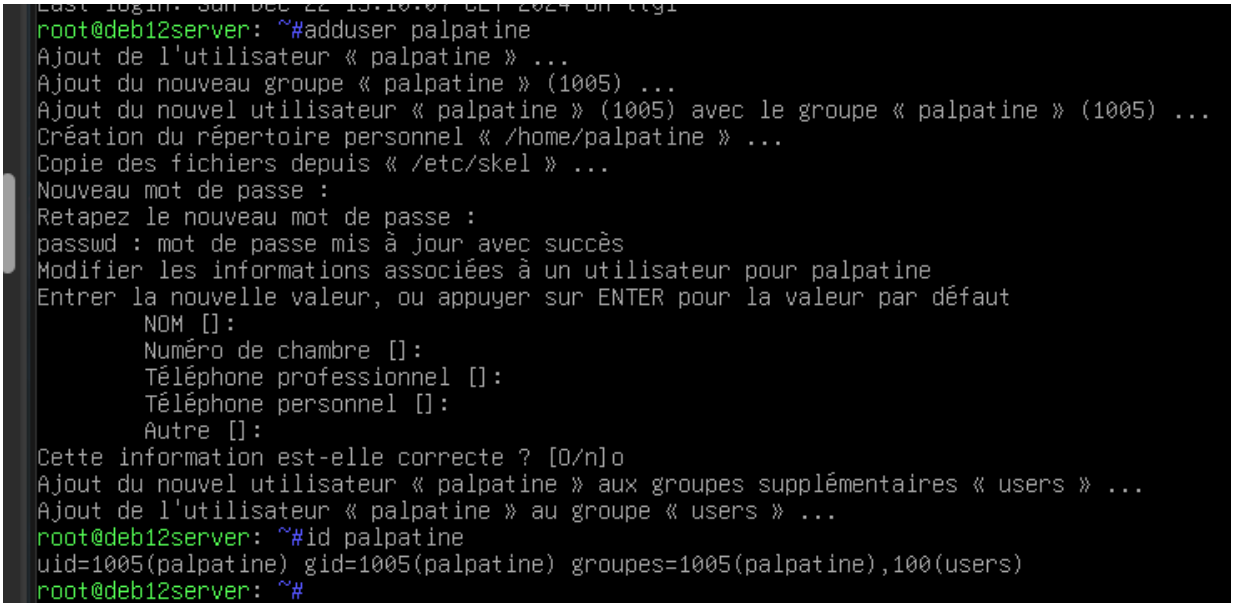
Je créé un compte toor ayant les mêmes droits que root.

```
passwd : mot de passe mis à jour avec succès
root@deb12server: ~#useradd -u 0 -o -d /root -s /bin/bash toor
useradd warning: toor's uid 0 outside of the UID_MIN 1000 and UID_MAX 60000 range.
root@deb12server: ~#id toor
uid=0(root) gid=1008(toor) groupes=0(root)
root@deb12server: ~#passwd toor
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@deb12server: ~#
```

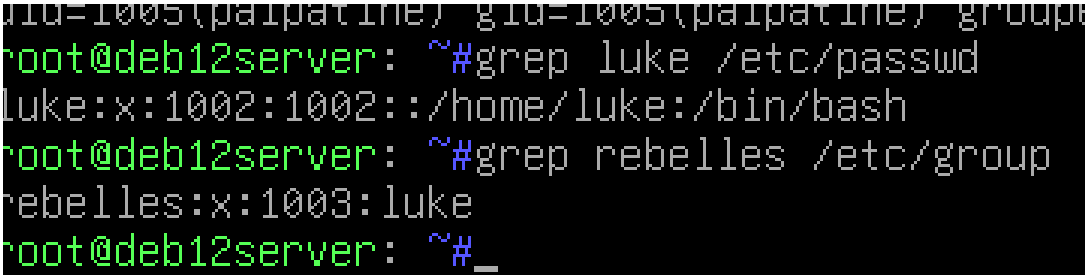
J'ouvre une deuxième console et je me connecte à toor

```
deb12server login: toor
Password:
Linux deb12server 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) 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.
Last login: Sun Dec 22 15:10:07 CET 2024 on tty1
root@deb12server: ~#
```

Je vien de créé un nouveau utilisatuer « palpatine »en respectant la charte debian avec la commande adduser



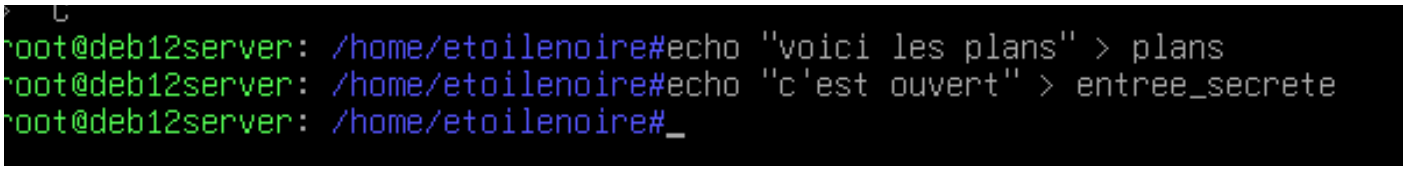
J’affiche les caractéristique de l’utilisateur local luke et du groupe local rebelles



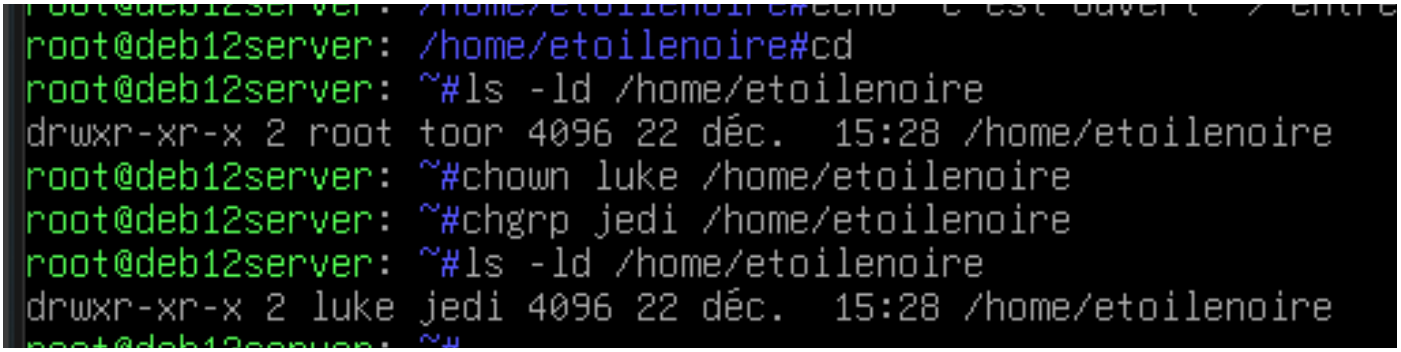
luke appartient au groupe secondaire rebelles

2.La gestion des droits

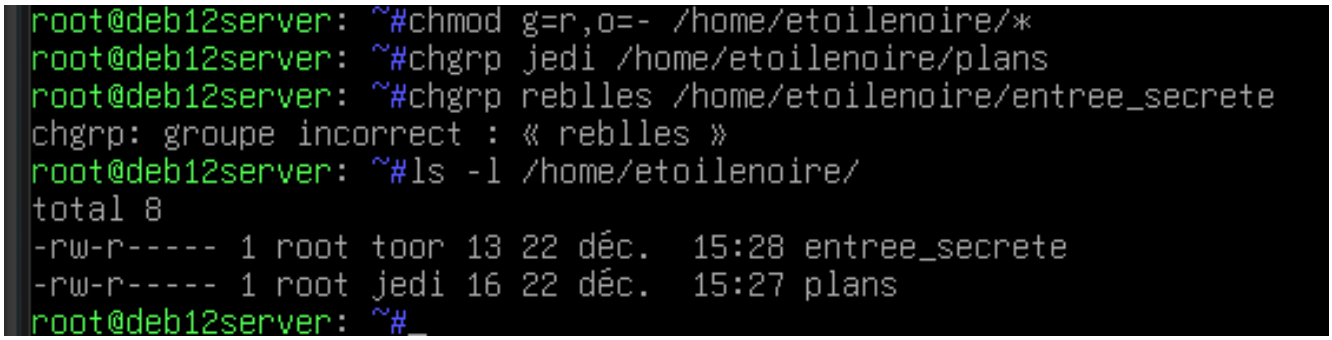
Je crée une arborescence de fichiers



Je change les caractéristiques du répertoire etoilenoire. Son propriétaire sera luke, son groupe sera jedi. Il sera accessible en lecture, écriture et accès pour le propriétaire (droits en octal). Il sera accessible en lecture et accès pour le groupe mais pas pour les autres.



Je change les caractéristiques des fichiers. Ils seront accessibles en lecture seule pour le groupe et n'auront aucun droit pour les autres. On utilise la notation symbolique. Le fichier plans sera affilié au groupe jedi et le fichier entree_secrete sera affilié au groupe rebelles



À partir du compte luke : L'utilisateur luke, en tant que propriétaire, a tous les droits sur le répertoire etoilenoire : il peut le lister, créer ou supprimer des fichiers dedans, et il a accès aux fichiers qu'il contient. En tant que membre du groupe jedi, il peut lire le fichier plans, et en tant que membre du groupe rebelles, il peut lire le fichier entree_secrete. Par contre, il ne peut pas modifier le fichier plans (ainsi que le fichier entree_secrete). Seul root peut le faire.

```
luke@deb12server:~$ ls /home/etoilenoire/
entree_secrete  plans
luke@deb12server:~$ cat /home/etoilenoire/plans
voici les plans
luke@deb12server:~$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
luke@deb12server:~$ cal > /home/etoilenoire/fichier
luke@deb12server:~$ ls /home/etoilenoire/
entree_secrete  fichier  plans
luke@deb12server:~$ rm /home/etoilenoire/fichier
luke@deb12server:~$ ls /home/etoilenoire/
entree_secrete  plans
luke@deb12server:~$ echo "===" >> /home/etoilenoire/plans
-bash: /home/etoilenoire/plans: Permission non accordée
luke@deb12server:~$
```

À partir du compte vador : L'utilisateur vador, en tant que membre du groupe jedi, peut lister le répertoire etoilenoire. Il a également accès aux fichiers qu'il contient. Par contre, il ne peut ni créer ni supprimer des fichiers dedans. En tant que membre du groupe jedi, il peut lire le fichier plans, mais pas le fichier entree_secrete. Il ne peut pas modifier le fichier plans. Seul root peut le faire

```
Fichier  Machine  Écran  Entrée  Périphériques  Aide
root@deb12server: ~#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 « fichier » ? o
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/etoienoire/entree_secrete
cat: /home/etoienoire/entree_secrete: Aucun fichier ou dossier de ce type
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$ echo "====" >> /home/etoilenoire/plans
-sh: 7: cannot create /home/etoilenoire/plans: Permission denied
$ exit
```

À partir du compte solo : L'utilisateur solo (groupe rebelles) n'a aucun droit sur le répertoire etoilenoire (cf. droits other) : il ne peut pas connaître son contenu, il ne peut ni ajouter ni supprimer des fichiers à l'intérieur. Il n'a aucun accès aux fichiers de ce répertoire, quels que soient les droits sur ces fichiers (cf. droit de lecture du groupe rebelles sur entree_secrete)

```
root@deb12server: ~#su - solo
$ ls /home/etoilenoire
entree_secrete  plans
$ 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
```

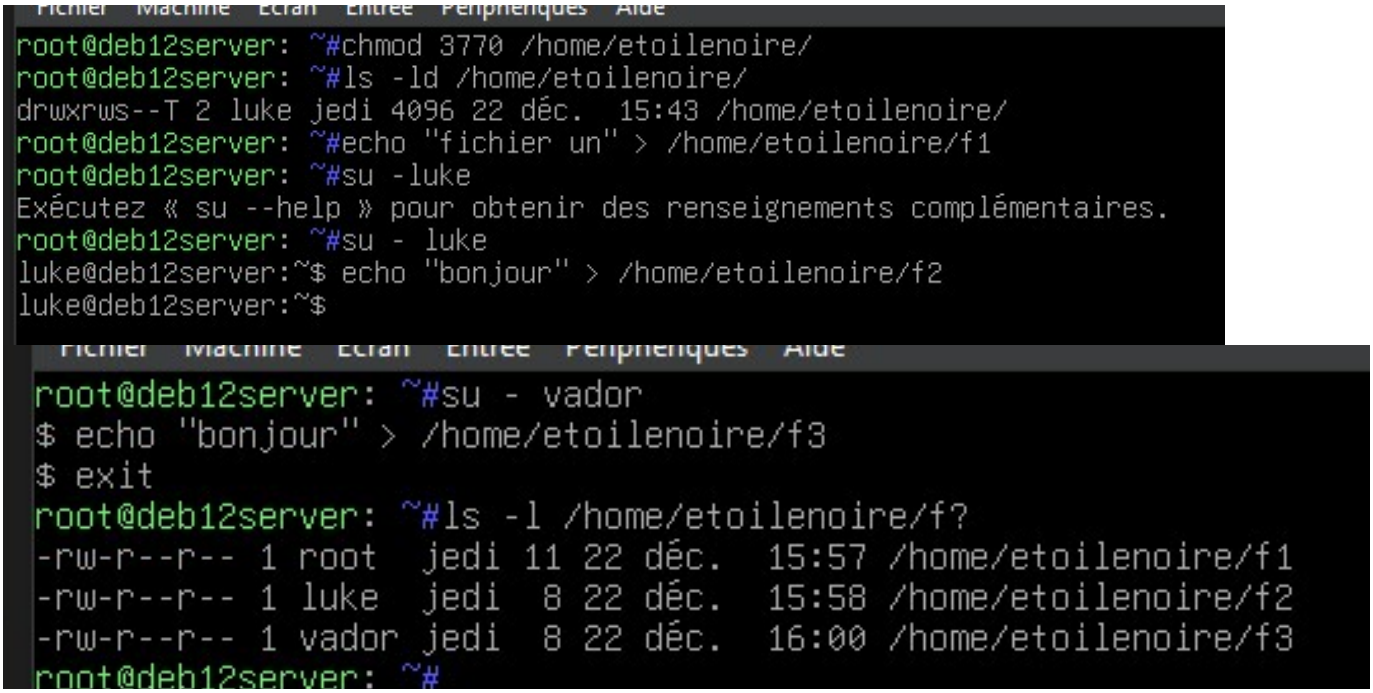
Suppression temporaire du droit d'exécution à la commande uptime. Je teste les conséquences à partir du compte luke

```
root@deb12server: ~#whereis uptime
uptime: /usr/bin/uptime /usr/share/man/man1/uptime.1.gz
root@deb12server: ~#whatis uptime
uptime (1)           - Indiquer depuis quand le système a été mis en route
root@deb12server: ~#uptime
 15:54:27 up 44 min,  2 users,  load average: 0,00, 0,00, 0,00
root@deb12server: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 19 déc.   2022 /usr/bin/uptime
root@deb12server: ~#chmod o-x /usr/bin/uptime
root@deb12server: ~#su - luke
luke@deb12server:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
```

```
Fichier  Machine  Ecran  Entrée  Périphériques  Aide
root@deb12server: ~#chmod o+x /usr/bin/uptime
root@deb12server: ~#ls -l /usr/bin/uptime
-rwxr-xr-x 1 root root 14648 19 déc.   2022 /usr/bin/uptime
root@deb12server: ~#su - luke
luke@deb12server:~$ uptime
 15:55:52 up 46 min,  2 users,  load average: 0,00, 0,00, 0,00
luke@deb12server:~$
```

3. La gestion des droits, compléments

J'ajoute des droits spéciaux (SGID et sticky-bit) au répertoire `etoilenoire`. Ensuite, pour vérifier l'impact de ces droits, je crée des fichiers dans le répertoire `etoilenoire`



Vador va essayer de détruire le fichier de luke mais on conserve le droit sticky-bit

on supprime le sticky-bit

```
$ exit
root@deb12server: ~#chmod -t /home/etoilenoire/
root@deb12server: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 22 déc.  16:00 /home/etoilenoire/
root@deb12server: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « fichier » ? o
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce type
$ exit
root@deb12server: ~#
```

root peut formater la partition /dev/sda1 ainsi que les membres du groupe disk

```
root@deb12server: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 22 déc.  15:09 /dev/sda1
root@deb12server: ~#
```

L’administrateur copie les fichiers du répertoire etoilenoire dans /tmp en conservant leurs attributs.

```
oot@deb12server: ~#cp -p /home/etoilenoire/* /tmp
oot@deb12server: ~#ls -l /tmp/plans/entree_secrete
s: impossible d'accéder à '/tmp/plans/entree_secrete': N'est pas un dossier
oot@deb12server: ~#ls -l /tmp/plans /entree_secrete
s: impossible d'accéder à '/entree_secrete': Aucun fichier ou dossier de ce type
rw-r----- 1 root jedi 16 22 déc.  15:27 /tmp/plans
oot@deb12server: ~#
```

L’administrateur donne le fichier entree_secrete à luke

```
root@deb12server: ~#chown luke /tmp/entree_secrete
root@deb12server: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke toor 13 22 déc.  15:28 /tmp/entree_secrete
root@deb12server: ~#_
```

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

Luke :

```
root@deb12server: ~#su - luke
luke@deb12server:~$ cat /tmp/entree_secrete
c'est ouvert
luke@deb12server:~$ echo "======" >> /tmp/etoilenoire/entree_secrete
-bash: /tmp/etoilenoire/entree_secrete: Aucun fichier ou dossier de ce typ
luke@deb12server:~$ cat /tmp/entree_secrete
c'est ouvert
luke@deb12server:~$  /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
luke@deb12server:~$
```

Solo :

```
root@deb12server: ~#su - solo
$ cat /tmp/entree_secrete
cat: /tmp/entree_secrete: Permission non accordée
$ echo "+++++++" >> /tmp/etoilenoire
$
```

Root :

```
root@deb12server: ~#cat /tmp/etoilenoire
+++++++
root@deb12server: ~#echo "+-+-+-+-" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@deb12server: ~#cat /tmp/etoilenoire
+++++++
root@deb12server: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@deb12server: ~#_
```

Je visualisez les droits du fichier shadow et de la commande passwd