



# Utilisateurs et droits

# Sommaire

UID et GID.....	3
Création de groupe.....	3
Création d'utilisateurs.....	4
Faire rejoindre les utilisateurs dans un groupe.....	5
Définir les droits pour le dossier.....	7
Tester les accès à partir de l'utilisateur "luke".....	8
Tester les accès à partir de l'utilisateur "vador".....	9
Tester les accès à partir de l'utilisateur "solo".....	10
Afficher les caractéristiques d'un utilisateur et d'un groupe.....	11
Afficher les annuaires pour la gestion des comptes et de mots de passe.....	12
Création d'un utilisateur lola.....	13
Gestion des comptes secondaires.....	14
Attribuer un mot de passe de manière scriptable.....	15
Recherche d'un utilisateur dans les annuaires.....	15
Suppression d'un utilisateur.....	16
Attribuer le droit SGID et Sticky-bit.....	16
Ajout de fichiers F1 et F2.....	17
Tester la suppression du fichier de luke avec le compte "vador".....	17
Permission de formater la partition.....	18
Copier le dossier en conservant les attributs.....	18
Visualisation des droits des fichiers passwd et shadow.....	19
Conclusion.....	20

## UID et GID

Pour voir quels sont leurs UID et GID, on peut consulter le fichier `/etc/passwd` en utilisant la commande `cat`.

```
cat /etc/passwd
```

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

L'utilisateur "daemon" existe bien sur Linux, son UID est 1 et son GID est 1

```
administrateur:x:1000:1000:administrateur,,,:/home/administrateur:/bin/bash
```

L'utilisateur "administrateur" existe aussi sur Linux, son UID est 1000 et son GID est 1000.

Un "UID" est un identifiant unique propre à l'utilisateur tandis qu'un "GID" est un identifiant unique propre au groupe d'utilisateurs.

## Création de groupe

Pour créer un groupe, on peut utiliser la commande `addgroup` suivi du nom du groupe en question.

```
root@Debian-12-Bookworm:~# addgroup jedi
Ajout du groupe « jedi » (GID 1001)...
Fait.
```

```
root@Debian-12-Bookworm:~# addgroup rebelles
Ajout du groupe « rebelles » (GID 1003)...
Fait.
```

Automatiquement, cette commande va attribuer un GID à la fois pour le groupe "jedi" et pour le groupe "rebelles".

# Création d'utilisateurs

Pour créer un utilisateur sur Linux, on peut utiliser la commande "adduser" suivi du nom de l'utilisateur en question (par exemple: **luke**, **vador** et **solo**). Après saisie de cette commande, le mot de passe ainsi que les informations personnelles sont demandés.

```
root@Debian-12-Bookworm:~# adduser luke
Ajout de l'utilisateur « luke » ...
Ajout du nouveau groupe « luke » (1004) ...
Ajout du nouvel utilisateur « luke » (1004) avec le groupe « luke » (1004) ...
Création du répertoire personnel « /home/luke » ...
Copie des fichiers depuis « /etc/skel » ...
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 luke
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [0/n]o
Ajout du nouvel utilisateur « luke » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « luke » au groupe « users » ...
```

```
root@Debian-12-Bookworm:~# /sbin/adduser vador
Ajout de l'utilisateur « vador » ...
Ajout du nouveau groupe « vador » (1005) ...
Ajout du nouvel utilisateur « vador » (1005) avec le groupe « vador » (1005) ...
Création du répertoire personnel « /home/vador » ...
Copie des fichiers depuis « /etc/skel » ...
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 vador
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [0/n]o
Ajout du nouvel utilisateur « vador » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « vador » au groupe « users » ...
```

```
root@Debian-12-Bookworm:~# /sbin/adduser solo
Ajout de l'utilisateur « solo » ...
Ajout du nouveau groupe « solo » (1006) ...
Ajout du nouvel utilisateur « solo » (1006) avec le groupe « solo » (1006) ...
Création du répertoire personnel « /home/solo » ...
Copie des fichiers depuis « /etc/skel » ...
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 solo
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [0/n]0
Ajout du nouvel utilisateur « solo » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « solo » au groupe « users » ...
```

Pour vérifier que ces utilisateurs ont bien été créés, il faut lire le contenu du fichier `/etc/passwd` en utilisant la commande `cat`:

```
luke:x:1004:1004:,,,:/home/luke:/bin/bash
vador:x:1005:1005:,,,:/home/vador:/bin/bash
solo:x:1006:1006:,,,:/home/solo:/bin/bash
```

On voit bien que les utilisateurs `luke`, `vador` et `solo` ont leur propre UID et GID. Ils ont chacun leur propre répertoire utilisateur et ils utilisent tous l'interpréteur BASH (`/bin/bash`).

## Faire rejoindre les utilisateurs dans un groupe

Pour faire rejoindre les utilisateurs dans un groupe, on utilise la commande `usermod`. Cette dernière prend deux arguments: le nom du groupe et le nom de l'utilisateur. L'option `-a` permet d'ajouter l'utilisateur au groupe

```
root@Debian-12-Bookworm:~# usermod -G jedi luke
root@Debian-12-Bookworm:~# usermod -G rebelles luke
root@Debian-12-Bookworm:~# usermod -G jedi vador
root@Debian-12-Bookworm:~# usermod -G rebelles solo
```

Pour être sûr que ces utilisateurs sont bien dans leurs groupes, on lit le fichier `/etc/group` avec la commande `cat`:

```
jedi:x:1001:luke,vador
rebelles:x:1003:luke,solo
```

On voit bien que l'utilisateur `luke` est dans le groupe **jedi** et **rebelles**.

Pour changer le mot de passe, on utilise la commande `passwd` suivi du nom d'utilisateur en question.

```
root@Debian-12-Bookworm:~# passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
```

Après avoir changé le mot de passe, on teste la connexion à l'utilisateur `luke` avec la commande `login`.

```
root@Debian-12-Bookworm:~# login luke
Mot de passe :
Linux Debian-12-Bookworm 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian
6.1.38-1 (2023-07-14) 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.
luke@Debian-12-Bookworm:~$
```

On voit bien dans le terminal qu'on a réussi à se connecter en tant que "luke".

## Définir les droits pour le dossier

On change les caractéristiques du répertoire *etoilenoire* : son propriétaire sera *luke*, son groupe *jedi*. Il sera accessible en *rwX* pour son propriétaire. Il sera accessible en lecture et parcours (accès au contenu du répertoire) au groupe mais pas aux autres.

```
root@Debian-12-Bookworm:~# mkdir /home/etoilenoire
root@Debian-12-Bookworm:~# cd /home/etoilenoire/
root@Debian-12-Bookworm:/home/etoilenoire# echo "voici les plans" > plans
root@Debian-12-Bookworm:/home/etoilenoire# echo "c'est ouvert" >
entree_secrets
root@Debian-12-Bookworm:/home/etoilenoire# cd ..
root@Debian-12-Bookworm:/home# chown luke:jedi etoilenoire/
root@Debian-12-Bookworm:/home# chmod 740 etoilenoire/
```

Pour afficher les droits sur un dossier spécifique, on peut utiliser la commande `ls`.

```
root@Debian-12-Bookworm:/home# ls -l
total 20
drwx----- 19 administrateur administrateur 4096 27 févr. 08:36 administrateur
drwxr----- 2 luke jedi 4096 6 févr. 10:07 etoilenoire
drwx----- 2 luke luke 4096 6 févr. 10:07 luke
drwx----- 2 solo solo 4096 6 févr. 09:25 solo
drwx----- 2 vador vador 4096 6 févr. 09:24 vador
root@Debian-12-Bookworm:/home# █
```

On voit que les fichiers "**entree\_secrets**" et "**plans**" appartiennent au propriétaire "**luke**" ainsi qu'au groupe "**jedi**".

On change les caractéristiques des fichiers : ils seront accessibles en lecture seule pour le groupe et n'auront aucun droit pour les autres. On affilie le fichier *plans* au groupe *jedi* et le fichier *entree\_secrete* au groupe *rebelles*.

```
root@Debian-12-Bookworm:/home/etoilenoire# chmod 640 *
root@Debian-12-Bookworm:/home/etoilenoire# chown :jedi plans
root@Debian-12-Bookworm:/home/etoilenoire# chown :rebelles entree_secrets
root@Debian-12-Bookworm:/home/etoilenoire# ls -l
total 8
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
```

## Tester les accès à partir de l'utilisateur "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.*

```
luke@Debian-12-Bookworm:~$ ls -l ../
total 20
drwx----- 19 administrateur administrateur 4096 27 févr. 08:36 administrateur
drwxr----- 2 luke jedi 4096 27 févr. 09:12 etoilenoire
drwx----- 3 luke luke 4096 27 févr. 09:10 luke
drwx----- 2 solo solo 4096 6 févr. 09:25 solo
drwx----- 2 vador vador 4096 6 févr. 09:24 vador
luke@Debian-12-Bookworm:~$ cd ../etoilenoire/
luke@Debian-12-Bookworm:/home/etoilenoire$ ls
entree_secrets plans
luke@Debian-12-Bookworm:/home/etoilenoire$ ls -l
total 8
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
luke@Debian-12-Bookworm:/home/etoilenoire$ echo "bonjour" > salutation
luke@Debian-12-Bookworm:/home/etoilenoire$ echo "merci" > remerciement
luke@Debian-12-Bookworm:/home/etoilenoire$ ls -l
total 16
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
-rw-r--r-- 1 luke luke 6 27 févr. 09:21 remerciement
-rw-r--r-- 1 luke luke 8 27 févr. 09:20 salutation
luke@Debian-12-Bookworm:/home/etoilenoire$ cat salutation remerciement
bonjour
merci
luke@Debian-12-Bookworm:/home/etoilenoire$ rm salutation remerciement
luke@Debian-12-Bookworm:/home/etoilenoire$
```

*En tant que membre du groupe jedi, il peut lire le fichier, 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.*

```
luke@Debian-12-Bookworm:/home/etoilenoire$ ls -l
total 8
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
luke@Debian-12-Bookworm:/home/etoilenoire$ cat entree_secrets
c'est ouvert
luke@Debian-12-Bookworm:/home/etoilenoire$ echo "c'est fermé" > entree_secrets
-bash: entree_secrets: Permission non accordée
luke@Debian-12-Bookworm:/home/etoilenoire$
```



## Tester les accès à partir de l'utilisateur "solo"

*L'utilisateur solo n'a aucun droit sur le répertoire etoilenoire.*

```
solo@Debian-12-Bookworm:~$ cd ../etoilenoire/  
-bash: cd: ../etoilenoire/: Permission non accordée  
solo@Debian-12-Bookworm:~$ █
```

```
root@Debian-12-Bookworm:/home# chmod -x /bin/uptime  
root@Debian-12-Bookworm:/home# uptime  
bash: /usr/bin/uptime: Permission non accordée █  
root@Debian-12-Bookworm:/home# █
```

```
root@Debian-12-Bookworm:~# ls -l /bin/uptime  
-rw-r--r-- 1 root root 14648 19 déc. 2022 /bin/uptime  
root@Debian-12-Bookworm:~# █
```

# Afficher les caractéristiques d'un utilisateur et d'un groupe

Pour voir les caractéristiques d'un utilisateur (luke par exemple), il faut utiliser la commande "id" suivi du nom de l'utilisateur.

```
root@Debian-12-Bookworm:~# id luke
uid=1004(luke) gid=1004(luke) groupes=1004(luke),100(users),1001(jedi),1003(rebelles)
```

Cela donne les informations sur son UID, son GID ainsi que les groupes auxquels il fait partie. Par exemple, l'utilisateur "luke" fait partie du groupe "luke", "jedi" et "rebelles", son UID est 1004 et son GID est 1004 aussi.

Pour voir les caractéristiques d'un groupe, il faut utiliser la commande getent. Elle permet de récupérer les informations depuis la base de données.

Par exemple, si on veut obtenir des informations sur le groupe "rebelles", il faut taper la commande "getent group rebelles".

```
root@Debian-12-Bookworm:~# getent group rebelles
rebelles:x:1003:luke,solo
root@Debian-12-Bookworm:~# █
```

On peut voir que le groupe "rebelles" à des utilisateurs qui sont luke et solo. Son GID est 1003.



## Création d'un utilisateur lola

```
root@Debian-12-Bookworm:~# adduser lola
Ajout de l'utilisateur « lola » ...
Ajout du nouveau groupe « lola » (1007) ...
Ajout du nouvel utilisateur « lola » (1007) avec le groupe « lola » (1007) ...
Création du répertoire personnel « /home/lola » ...
Copie des fichiers depuis « /etc/skel » ...
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 lola
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [0/n]
Ajout du nouvel utilisateur « lola » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « lola » au groupe « users » ...

drwx----- 2 lola          lola          4096 5 mars 08:53 lola
```

Lorsque qu'on crée l'utilisateur "lola", elle fera partie du groupe qui aura le même nom que le sien. Autrement dit, L'utilisateur "lola" fait partie du groupe qui s'appelle "lola".

## Gestion des comptes secondaires

Pour que l'utilisateur puisse faire partie d'un ou plusieurs groupes, la commande `usermod` sera utilisée.

Si on veut affecter "lola" au groupe "rebelles":

```
root@Debian-12-Bookworm:/home# usermod -aG rebelles lola
root@Debian-12-Bookworm:/home# groups lola
lola : lola users rebelles
```

"groups" est une commande qui permet de lister tous les groupes auxquels l'utilisateur fait partie.

Si on veut affecter l'utilisateur "lola" au groupe "jedi". Elle quitte le groupe "rebelles":

```
root@Debian-12-Bookworm:/home# usermod -aG jedi lola
root@Debian-12-Bookworm:/home# usermod -rG rebelles lola
root@Debian-12-Bookworm:/home# groups lola
lola : lola users jedi
```

Si on veut que lola appartienne à la fois au groupe "jedi" et "rebelles":

```
root@Debian-12-Bookworm:/home# usermod -aG rebelles lola
root@Debian-12-Bookworm:/home# groups lola
lola : lola users jedi rebelles
```

Si on veut que "lola" n'appartienne plus à aucun groupe secondaire:

```
root@Debian-12-Bookworm:/home# usermod -rG jedi lola
root@Debian-12-Bookworm:/home# usermod -rG rebelles lola
root@Debian-12-Bookworm:/home# groups lola
lola : lola users
```

# Attribuer un mot de passe de manière scriptable

Pour attribuer un mot de passe de manière scriptable, on peut créer un fichier shell qui permet d'exécuter des instructions pour les lignes de commandes. Après modification de ce fichier, il faut lui donner le droit d'exécution grâce à la commande `chmod`.

```
GNU nano 7.2                                mdp_lola.sh
#!/usr/bin/env sh

echo ">>> Changement de mot de passe\n"
passwd lola
echo "\n>>> Le mot de passe a bien été changé\n"

root@Debian-12-Bookworm:~# chmod +x mdp_lola.sh

root@Debian-12-Bookworm:~# ./mdp_lola.sh
>>> Changement de mot de passe

Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès

>>> Le mot de passe a bien été changé
```

On voit que le script fonctionne sans erreur et que le mot de passe de lola a bien été changé.

## Recherche d'un utilisateur dans les annuaires

```
root@Debian-12-Bookworm:~# cat /etc/passwd | grep "lola"
lola:x:1007:1007:,,,:/home/lola:/bin/bash
root@Debian-12-Bookworm:~# cat /etc/shadow | grep "lola"
lola:$y$j9T$CWmZhL7h1MPGKGSnotgDF1$JxuVD0me080qsjIfzdghbIOF3r9e/AGyn9qoqxJC2N8:
19787:0:99999:7:::
root@Debian-12-Bookworm:~# cat /etc/group | grep "lola"
users:x:100:administrateur,luke,vador,lola
lola:x:1007:
root@Debian-12-Bookworm:~#
```

## Suppression d'un utilisateur

Pour supprimer un utilisateur, on peut utiliser la commande "deluser".

```
root@Debian-12-Bookworm:~# deluser lola
Suppression du crontab ...
Suppression de l'utilisateur « lola » ...
Fait.
```

Après suppression de l'utilisateur "lola", il faut aussi supprimer son répertoire utilisateur grâce à la commande "rm".

```
root@Debian-12-Bookworm:~# rm -rf /home/lola
root@Debian-12-Bookworm:~# █
```

## Attribuer le droit SGID et Sticky-bit

Pour attribuer le droit SGID et Sticky-bit, on utilise la commande "chmod".

L'argument g+s signifie qu'on ajoute l'attribut "S" (SGID) pour le groupe.

L'argument +t signifie qu'on ajoute l'attribut "T" (Sticky-bit) pour le groupe.

```
root@Debian-12-Bookworm:/home# chmod g+s etoilenoire/
root@Debian-12-Bookworm:/home# chmod +t etoilenoire/
```

```
root@Debian-12-Bookworm:/home# ls -l
total 20
drwx----- 19 administrateur administrateur 4096  5 mars  08:36 administrateur
drwxr-S--T  2 luke             jedi         4096 27 févr. 09:21 etoilenoire
drwx-----  3 luke             luke         4096 27 févr. 09:10 luke
drwx-----  2 solo             solo         4096 27 févr. 09:48 solo
drwx-----  3 vador             vador        4096 27 févr. 09:38 vador
```

## Ajout de fichiers F1 et F2

```
root@Debian-12-Bookworm:/home/etoilenoire# echo "root" > F1
root@Debian-12-Bookworm:/home/etoilenoire# login luke
```

```
luke@Debian-12-Bookworm:/home/etoilenoire$ echo "luke" > F2
luke@Debian-12-Bookworm:/home/etoilenoire$ ls
entree_secrets  F1  F2  plans
luke@Debian-12-Bookworm:/home/etoilenoire$ ls -l
total 16
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r--r-- 1 root jedi      5  5 mars 10:12 F1
-rw-r--r-- 1 luke jedi      5  5 mars 10:14 F2
-rw-r----- 1 root jedi     13 27 févr. 09:12 plans
```

## Tester la suppression du fichier de luke avec le compte "vador"

```
root@Debian-12-Bookworm:/home# ls -l --color
total 24
drwx----- 19 administrateur administrateur 4096 12 mars 08:35 administrateur
drwxr-S--T  2 luke jedi 4096 5 mars 10:14 etoilenoire
drwxr----T  2 root root 4096 12 mars 08:43 etoilenoire-backup
drwx----- 3 luke luke 4096 27 févr. 09:10 luke
drwx----- 2 solo solo 4096 27 févr. 09:48 solo
drwx----- 3 vador vador 4096 27 févr. 09:38 vador
root@Debian-12-Bookworm:/home# login vador
Mot de passe :
Linux Debian-12-Bookworm 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) 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.
Dernière connexion : mardi 12 mars 2024 à 08:43:48 CET sur pts/0
vador@Debian-12-Bookworm:~$ cd ..
vador@Debian-12-Bookworm:/home$ rm ./etoilenoire/F2
rm: impossible de supprimer './etoilenoire/F2': Permission non accordée
vador@Debian-12-Bookworm:/home$
```

Le sticky-bit ne peut être affecté uniquement pour le propriétaire du dossier "etoilenoire". Depuis l'utilisateur "vador", il n'est pas possible de supprimer un fichier qui est dans ce répertoire.

## Permission de formater la partition

```
root@Debian-12-Bookworm:~# ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 12 mars 08:35 /dev/sda1
root@Debian-12-Bookworm:~# █
```

Le superutilisateur "root" ainsi que le groupe "disk" ont le droit de formater la partition /dev/sda1.

## Copier le dossier en conservant les attributs

```
root@Debian-12-Bookworm:/home# ls -l
total 24
drwx----- 19 administrateur administrateur 4096 12 mars 08:35 administrateur
drwxr-S--T 2 luke jedi 4096 5 mars 10:14 etoilenoire
drwxr---T 2 root root 4096 12 mars 08:43 etoilenoire-backup
drwx----- 3 luke luke 4096 27 févr. 09:10 luke
drwx----- 2 solo solo 4096 27 févr. 09:48 solo
drwx----- 3 vador vador 4096 27 févr. 09:38 vador
```

```
root@Debian-12-Bookworm:/home# cp -r etoilenoire /tmp/
root@Debian-12-Bookworm:/home# ls -l /tmp
total 48
drwxr---T 2 root root 4096 12 mars 09:00 etoilenoire
```

Lorsqu'on copie le répertoire "etoilenoire" vers le dossier /tmp, on voit que l'attribut "T" (sticky-bit) est bien conservé. En revanche, l'attribut "S" (SGID) n'a pas été conservé. Donner le fichier à un utilisateur

Pour donner le fichier à un utilisateur en question, on utilise la commande chown.

```
root@Debian-12-Bookworm:/home/etoilenoire# ls -l
total 16
-rw-r----- 1 root rebelles 13 27 févr. 09:12 entree_secrets
-rw-r--r-- 1 root jedi 5 5 mars 10:12 F1
-rw-r--r-- 1 luke jedi 5 5 mars 10:14 F2
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
root@Debian-12-Bookworm:/home/etoilenoire# chown luke: entree_secrets
root@Debian-12-Bookworm:/home/etoilenoire# ls -l
total 16
-rw-r----- 1 luke luke 13 27 févr. 09:12 entree_secrets
-rw-r--r-- 1 root jedi 5 5 mars 10:12 F1
-rw-r--r-- 1 luke jedi 5 5 mars 10:14 F2
-rw-r----- 1 root jedi 13 27 févr. 09:12 plans
root@Debian-12-Bookworm:/home/etoilenoire# █
```

On voit que le fichier "entree\_secrets" appartient désormais à "luke".

## Visualisation des droits des fichiers passwd et shadow.

```
root@Debian-12-Bookworm:/home/etoilenoire# ls -l /etc/shadow /etc/passwd
-rw-r--r-- 1 root root 2151 5 mars 09:44 /etc/passwd
-rw-r----- 1 root shadow 1365 5 mars 09:44 /etc/shadow
root@Debian-12-Bookworm:/home/etoilenoire# █
```

On constate que l'utilisateur root a le droit de lecture et d'écriture sur ces deux fichiers. Le groupe root ainsi que les autres peuvent lire le fichier /etc/passwd. Les utilisateurs du groupe "shadow" peuvent lire le fichier le fichier /etc/shadow mais pas les autres utilisateurs.

## **Conclusion**

En conclusion, les permissions sont très utilisées pour garder les données sensibles. Ce qui permet de garantir la confidentialité et de limiter les risques.