

Sommaire

1. La gestion des utilisateurs.....2
2. La gestion des droits.....6

1. La gestion des utilisateurs

- Vérification de la présence des utilisateurs daemon et luke

```
root@DEB12Server: ~#id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
root@DEB12Server: ~#id luke
id: « luke » : utilisateur inexistant
root@DEB12Server: ~#_
```

- Création des groupes jedi et rebelles

```
root@DEB12Server: ~#groupadd jedi
root@DEB12Server: ~#groupadd rebelles
root@DEB12Server: ~#
```

- Création des comptes utilisateurs luke, vador et solo

```
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)
root@DEB12Server: ~#
```

- Affichage du contenu des dossiers passwd et group pour vérifier la présence des utilisateurs et groupes créés précédemment.

```
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
root@DEB12Server: ~#
```

- On remplace le shell par le bash pour l'utilisateur luke

```
root@DEB12Server: ~#usermod -s /bin/bash luke
root@DEB12Server: ~#_
```

```
luke@DEB12Server:~$ id
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
luke@DEB12Server:~$
```

- Création de l'utilisateur leia

```
root@DEB12Server: ~#useradd leia
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB12Server: ~#_
```

- On vérifie si l'utilisateur possède un répertoire personnel : Il n'en possède pas

```
root@DEB12Server: ~#ls -l /home
total 20
drwx----- 6 guest guest 4096 22 déc. 11:17 guest
drwxr-xr-x 2 luke jedi 4096 8 janv. 11:30 luke
drwx----- 2 sio sio 4096 26 sept. 22:06 sio
drwxr-xr-x 2 solo rebelles 4096 8 janv. 11:31 solo
drwxr-xr-x 2 vador jedi 4096 8 janv. 11:31 vador
root@DEB12Server: ~#
```

- On affecte leia au groupe rebelles

```
root@DEB12Server: ~#usermod -G rebelles leia
root@DEB12Server: ~#is leia
-bash: is : commande introuvable
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1003(rebelles)
root@DEB12Server: ~#
```

- On affecte leia au groupe jedi. Leia est enlevé du groupe rebelle

```
root@DEB12Server: ~#usermod -G jedi leia
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi)
root@DEB12Server: ~#
```

- On ajoute leia aux deux groupes

```
root@DEB12Server: ~#usermod -G jedi,rebelles leia
root@DEB12Server: ~#is leia
-bash: is : commande introuvable
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB12Server: ~#_
```

- On enlève les groupes de leia

```
root@DEB12Server: ~#usermod -G "" leia
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DEB12Server: ~#_
```

- On ajoute l'utilisateur à un groupe secondaire sans retirer ses autres groupes

```
root@DEB12Server: ~#usermod -G jedi leia
root@DEB12Server: ~#usermod -aG rebelles leia
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DEB12Server: ~#
```

- On supprime leia

```
root@DEB12Server: ~#userdel leia
root@DEB12Server: ~#_
```

- Recréation de leia avec un répertoire de connexion

```
root@DEB12Server: ~#useradd -m leia
root@DEB12Server: ~#cd /home/leia
root@DEB12Server: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls-l
-sh: 4: ls-l: not found
$ ls -l
total 0
-rw-r--r-- 1 leia leia 0 12 janv. 11:05 fichier1
$ exit
root@DEB12Server: /home/leia#cd
root@DEB12Server: ~#
```

- Suppression d'un compte utilisateur et des 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
root@DEB12Server: ~#_
```

- On recrée le compte leia à l'identique

```
root@DEB12Server: ~#groupadd -g 1005 leia
root@DEB12Server: ~#useradd -u 1005 -g leia -m -s /bin/bash leia
root@DEB12Server: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
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: ~#
```

- Création de l'utilisateur toor avec les mêmes droits que root

```
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=1006(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
```

- Connexion en tant que toor dans une seconde console

```
Debian GNU/Linux 12 DEB12Server tty2

DEB12Server login: toor
Password:
Linux DEB12Server 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) 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: Fri Jan 12 10:53:35 CET 2024 on tty1
root@DEB12Server: ~#_
```

- Création de l'utilisateur palpatine

```
root@DEB12Server: ~#adduser palpatine
Ajout de l'utilisateur « palpatine » ...
Ajout du nouveau groupe « palpatine » (1007) ...
Ajout du nouvel utilisateur « palpatine » (1007) avec le groupe « palpatine » (1007) ...
Création du répertoire personnel « /home/palpatine » ...
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 palpatine
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 « palpatine » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « palpatine » au groupe « users » ...
root@DEB12Server: ~#id palpatine
uid=1007(palpatine) gid=1007(palpatine) groupes=1007(palpatine),100(users)
root@DEB12Server: ~#_
```

- Affichage des caractéristiques de l'utilisateur luke et du groupe local rebelles

```
root@DEB12Server: ~#grep luke /etc/passwd
luke:x:1002:1002:~/home/luke:/bin/bash
root@DEB12Server: ~#grep rebelles /etc/group
rebelles:x:1003:luke
```

- Affichage des caractéristiques de l'utilisateur luke et du groupe jedi

```
root@DEB12Server: ~#getent passwd luke
luke:x:1002:1002:~/home/luke:/bin/bash
root@DEB12Server: ~#getent group jedi
jedi:x:1002:
root@DEB12Server: ~#_
```

2. La gestion des droits

- Création d'une arborescence de fichiers

```
root@DEB12Server: ~#mkdir /home/etoilenoire
root@DEB12Server: ~#cd /home/etoilenoire
root@DEB12Server: /home/etoilenoire#echo "voici les plans" > plans
root@DEB12Server: /home/etoilenoire#echo "c'est ouvert" > entree_secrete
root@DEB12Server: /home/etoilenoire#_
```

- Modification des permissions du fichier (Propriétaire Luke avec toutes les permissions, groupe jedi avec lecture et écriture, aucune pour les autres)

```
root@DEB12Server: ~#ls -ld /home/etoilenoire
drwxr-xr-x 2 root root 4096 12 janv. 11:27 /home/etoilenoire
root@DEB12Server: ~#chown luke /home/etoilenoire
root@DEB12Server: ~#chgrp jedi /home/etoilenoire
root@DEB12Server: ~#chmod 750 /home/etoilenoire
root@DEB12Server: ~#ls -ld /home/etoilenoire
drwxr-x--- 2 luke jedi 4096 12 janv. 11:27 /home/etoilenoire
root@DEB12Server: ~#_
```

- On affilie le fichier plans au groupe jedi et le fichier entree_secrete au groupe rebelles en utilisant la notation symbolique

```
root@DEB12Server: ~#chmod g=r,o=- /home/etoilenoire/*
root@DEB12Server: ~#chgrp jedi /home/etoilenoire/plans
root@DEB12Server: ~#chgrp rebelles /home/etoilenoire/entree_secrete
root@DEB12Server: ~#ls -l /home/etoilenoire/
total 8
-rw-r----- 1 root rebelles 13 12 janv. 11:27 entree_secrete
-rw-r----- 1 root jedi      16 12 janv. 11:27 plans
root@DEB12Server: ~#_
```

- On test les accès :
- A partie de luke

```
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ ls /home/etoilenoire
entree_secrete plans
luke@DEB12Server:~$ ls /home/etoilenoire/plans
/home/etoilenoire/plans
luke@DEB12Server:~$ cat /home/etoilenoire/plans
voici les plans
luke@DEB12Server:~$ cat /home/etoilenoire/entree_secrete
c'est ouvert
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:~$ exit
```

■ A partir du compte Vador

```
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 » ?
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
```

■ A partir du compte Solo

```
root@DEB12Server: ~#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
```

■ Suppression temporaire du droit d'exécution de la commande uptime

```
root@DEB12Server: ~#whereis uptime
uptime: /usr/bin/uptime /usr/share/man/man1/uptime.1.gz
root@DEB12Server: ~#whatis uptime
uptime : rien d'adéquat
root@DEB12Server: ~#uptime
 11:55:14 up 1:02, 3 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: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 19 déc. 2022 /usr/bin/uptime
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
luke@DEB12Server:~$ exit
```

```
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
 11:56:43 up 1:03, 3 users, load average: 0,04, 0,01, 0,00
luke@DEB12Server:~$ exit_
```

3. La gestion des droits, compléments

- Ajout du sticky-bit et du SGID au répertoire etoilenoire et on test l'impact de ces droits

```
root@DEB12Server: ~#chmod3770 /home/etoilenoire/
-bash: chmod3770 : commande introuvable
root@DEB12Server: ~#chmod 3770 /home/etoilenoire/
root@DEB12Server: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 12 janv. 11:44 /home/etoilenoire/
root@DEB12Server: ~#echo "fichier un" > /home/etoilenoire/f1
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ echo "bonjour" > /home/etoilenoire/f2
luke@DEB12Server:~$ exit_
```

```
root@DEB12Server: ~#su - vador
$ echo "bonjour" > /home/etoilenoire/f3
$ exit
root@DEB12Server: ~#ls -l /home/etoilenoire/f?
-rw-r--r-- 1 root jedi 11 18 janv. 20:11 /home/etoilenoire/f1
-rw-r--r-- 1 luke jedi 8 18 janv. 20:11 /home/etoilenoire/f2
-rw-r--r-- 1 vador jedi 8 18 janv. 20:13 /home/etoilenoire/f3
root@DEB12Server: ~#
```

- Tentative de destruction du fichier de luke via vador (Sticky-bit actif) : Echech

```
root@DEB12Server: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « fichier » ? y
rm: impossible de supprimer '/home/etoilenoire/f2': Opération non permise
$ exit
```

- Tentative de destruction du fichier de luke via vador (Sticky-bit désactivé) : Réussite

```
root@DEB12Server: ~#chmod -t /home/etoilenoire/
root@DEB12Server: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 18 janv. 20:13 /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 » ? y
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce type
*
```

- Vérification des permissions de la partition sda1

```
root@DEB12Server: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 18 janv. 20:05 /dev/sda1
root@DEB12Server: ~#
```

- Copie des fichiers du répertoire etoilenoire dans /tmp

```
root@DEB12Server: ~#cp -p /home/etoilenoire/* /tmp
root@DEB12Server: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 12 janv. 11:27 /tmp/entree_secrete
-rw-r----- 1 root jedi      16 12 janv. 11:27 /tmp/plans
root@DEB12Server: ~#_
```

- On 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 rebelles 13 12 janv. 11:27 /tmp/entree_secrete
root@DEB12Server: ~#_
```

- Test des accès
- A partir du compte luke :

```
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ cat /tmp/entree_secrete
c'est ouvert
luke@DEB12Server:~$ echo "=====" >> /tmp/entree_secrete
luke@DEB12Server:~$ cat /tmp/entree_secrete
c'est ouvert
=====
luke@DEB12Server:~$ /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
luke@DEB12Server:~$ exit
```

- A partir du compte solo

```
root@DEB12Server: ~#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@DEB12Server: ~#cat /tmp/entree_secrete
c'est ouvert
=====
root@DEB12Server: ~#echo "++++++" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#cat /tmp/entreesecrete
cat: /tmp/entreesecrete: Aucun fichier ou dossier de ce type
root@DEB12Server: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#_
```

- Visualisation des droits du fichier shadow et de la commande passwd

```
root@DEB12Server: ~#ls -l /etc/shadow
-rw-r----- 1 root shadow 1321 12 janv. 11:17 /etc/shadow
root@DEB12Server: ~#ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 68248 23 mars 2023 /usr/bin/passwd
root@DEB12Server: ~#
```