BTS 1 - Services Informatiques aux Organisations

TP13 – Les utilisateurs et les droits

Table des matières

1. La gestion des utilisateurs 2
2. La gestion des droits 10
3. La gestion des droits, compléments 15

1. La gestion des utilisateurs

La commande id daemon permet d'afficher les informations sur l'utilisateur daemon, notamment son uid, gid, et ses groupes.

La commande id luke permettrait d'afficher les informations de l'utilisateur luke, mais comme il n'existe pas, cela affiche une erreur.

Est-ce que les comptes utilisateurs daemon et luke existent et, si oui, quels sont leurs uid, gid et leur(s) groupe(s) ?
L'utilisateur daemon existe et son uid, gid, et groupe sont définis à 1 (daemon) et l'utilisateur luke n'existe pas encore donc il n'a ni uid ni gid et ni groupe associé.

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

Les commandes groupadd jedi et groupadd rebelles permet de créer les groupes jedi et rebelles.

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

La commande man useradd permet de consulter le manuel de la commande useradd

```
root@DEB12Server: ~#man useradd_
```

```
USERADD(8)                                  Commandes de gestion du système                                  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. Le compte luke appartient au groupe jedi (groupe principal) et au groupe rebelles (groupe secondaire). Le compte vador appartient au groupe jedi. Le compte solo fait partie du groupe rebelles.

La commande useradd -g jedi -G rebelles -m luke permet de créer l'utilisateur luke avec le groupe principal jedi et le groupe secondaire rebelles en générant son répertoire personnel.

La commande useradd -g jedi -m vador permet de créer l'utilisateur vador avec le groupe principal jedi et son répertoire personnel.

La commande useradd -g rebelles -m solo crée l'utilisateur solo avec le groupe principal rebelles et son répertoire personnel.

La commande id vador affiche les informations de l'utilisateur vador son uid, gid et ses groupes.

La commande id solo affiche les informations de l'utilisateur solo, son uid, gid et ses groupes.

```
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: ~#_
```

La commande tail -3 /etc/passwd permet d'afficher les trois dernières lignes du fichier passwd qui contient les informations des utilisateurs du système.

La commande tail -2 /etc/group permet d'afficher les deux dernières lignes du fichier group, qui contient les informations des groupes du système.

```
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: ~#_
```

La commande passwd luke permet de définir/modifier le mot de passe pour l'utilisateur luke.

```
root@DEB12Server: ~#passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@DEB12Server: ~#_
```

Connexion au compte d'utilisateur luke :

```
Debian GNU/Linux 12 DEB12Server tty2

DEB12Server login: luke
Password:
Linux DEB12Server 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) 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.
$
```

La commande id affiche les informations d'identité de l'utilisateur courant, dont l'uid, gid et les groupes auxquels il appartient.

Remarque : La commande id sans argument affiche les informations de l'utilisateur courant.

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

La commande useradd leia permet de créer un nouvel utilisateur nommé leia

La commande id leia permet d'afficher les informations d'identité de l'utilisateur leia, notamment son uid**,** gid et ses groupes.

Remarque : Par défaut, la création d'un compte utilisateur entraîne également la création d'un compte groupe du même nom que l'utilisateur. Ce groupe devient le groupe principal de l'utilisateur nouvellement créé.

Créez l'utilisateur leia dans la première console avec la commande useradd (sous le compte root). **Quel est son groupe principal ?** Son groupe principal est le 1005 appartenant à leia.

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

La commande ls -l /home permet d'afficher la liste détaillée des répertoires présents dans le dossier /home.

Est-ce que le répertoire personnel de l'utilisateur leia a été créé ? Le répertoire personnel de l'utilisateur leia n'a pas été créé.

```
root@DEB12Server: ~#ls -l /home
total 20
drwx------ 5 guest guest    4096 21 déc.  08:45 guest
drwxr-xr-x 2 luke  jedi     4096 21 déc.  10:15 luke
drwx------ 3 nina  nina     4096 21 déc.  05:36 nina
drwxr-xr-x 2 solo  rebelles 4096 21 déc.  10:01 solo
drwxr-xr-x 2 vador jedi     4096 21 déc.  10:00 vador
root@DEB12Server: ~#
```

La commande usermod -G rebelles leia permet l'ajout de l'utilisateur leia au groupe rebelles et remplace tous ses groupes secondaires existants par rebelles.

La commande id leia permet de vérifier les groupes auxquels appartient l'utilisateur leia après modification.

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

La commande usermod -G jedi leia permet de remplacer tous les groupes secondaires de leia par jedi.

La commande id leia permet de vérifier les groupes auxquels appartient l'utilisateur leia après modification.

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

La commande usermod -G jedi, rebelles leia permet l'ajout du compte leia aux groupes secondaires jedi et rebelles.

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

La commande usermod -G "" leia retire leia de tous ses groupes secondaires.

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

La commande usermod -G jedi leia remplace tous les groupes secondaires de leia par jedi.

La commande usermod -aG rebelles leia permet l'ajoute du compte leia au groupe secondaire rebelles sans affecter ses groupes existants (option -a pour append).

```
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: ~#_
```

La commande userdel leia supprime l'utilisateur leia.

La commande useradd -m leia permet de créer l'utilisateur leia avec son répertoire personnel.

La commande su – leia permet la connexion au compte d'utilisateur leia

```
root@DEB12Server: ~#userdel leia
root@DEB12Server: ~#useradd -m leia
root@DEB12Server: ~#cd /home/leia
root@DEB12Server: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls -l
total 0
-rw-r--r-- 1 leia leia 0 21 déc.  10:27 fichier1
$ cd
$ exit
root@DEB12Server: /home/leia#cd
root@DEB12Server: ~#_
```

La commande userdel -r leia supprime l'utilisateur leia.

La commande ls -l /home/leia permet de vérifier si le répertoire personnel de leia a été supprimé.

```
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: ~#
```

La commande groupadd -g 1007 leia permet de créer un groupe leia avec un identifiant de groupe=1007.

La commande useradd -u 1007 -g leia -m -s /bin/bash leia permet de créer l'utilisateur leia avec un uid=1007, groupe principal=leia et le shell /bin/bash

La commande passwd leia permet de définir/modifier le mot de passe pour l'utilisateur leia.

```
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 :
passwd : mot de passe mis à jour avec succès
root@DEB12Server: ~#
```

La commande useradd -u 0 -o -d /root -s /bin/bash toor permet de créer un utilisateur toor avec un uid=0 (identique à root)

La commande id toor permet d'afficher l'uid, le gid et les groupes de toor.

La commande passwd toor permet de définir/modifie le mot de passe pour l'utilisateur toor

```
root@DEB12Server: ~#useradd -u 0 -o -d /root -s /bin/bash toor
useradd : l'utilisateur 'toor' existe déjà
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: ~#_
```

Connexion au compte d'utilisateur toor :

Remarques : cet utilisateur sert de compte de secours dans le cas où l'on perd le mot de passe de root. L'option -u permet de fixer l'uid, mais on ne peut pas utiliser un uid existant… sauf si l'on utilise l'option -o.

```
Debian GNU/Linux 12 DEB12Server tty2

DEB12Server login: toor
Password:
Linux DEB12Server 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) 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: Sat Dec 21 10:15:35 CET 2024 on tty1
root@DEB12Server: ~#_
```

La commande adduser palpatine permet de créer l'utilisateur palpatine avec un processus interactif (par des questions)

La commande id palpatine permet d'afficher l'uid, le gid et les groupes de palpatine.

```
root@DEB12Server: ~#adduser palpatine
Ajout de l'utilisateur « palpatine » ...
Ajout du nouveau groupe « palpatine » (1005) ...
Ajout du nouvel utilisateur « palpatine » (1005) avec le groupe « palpatine » (1005) ...
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 []: palpatine
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]o
Ajout du nouvel utilisateur « palpatine » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « palpatine » au groupe « users » ...
root@DEB12Server: ~#is palpatine
-bash: is : commande introuvable
root@DEB12Server: ~#id palpatine
uid=1005(palpatine) gid=1005(palpatine) groupes=1005(palpatine),100(users)
root@DEB12Server: ~#
```

La commande grep luke /etc/passwd recherche les informations de l'utilisateur luke dans le fichier /etc/passwd.

La commande grep rebelles /etc/group vérifie les membres du groupe rebelles.

L'utilisateur luke appartient au groupe secondaire 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
root@DEB12Server: ~#_
```

2. La gestion des droits

La commande mkdir /home/etoilenoire permet de créer le répertoire /home/etoilenoir

La commande cd /home/etoilenoire permet de se déplacer au répertoire /home/etoilenoire.

La commande echo “voici les plans” > plans permet de créer un fichier plans contenant "voici les plans".

La commande echo “c’est ouvert” > entree_secrete permet de créer un fichier entree_secrete contenant "c’est ouvert".

```
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#
```

La commande cd permet de retourner au répertoire personnel.

La commande ls -ld /home/etoilenoire permet d’afficher le contenue du répertoire /home/etoilenoire.

La commande chown luke /home/etoilenoire permet de définir luke comme propriétaire du répertoire /home/etoilenoire.

La commande chgrp jedi /home/etoilenoire permet de définir le groupe jedi comme groupe du répertoire /home/etoilenoire.

La commande chmod 750 /home/etoilenoire attribue les permissions au répertoire, propriétaire : lecture, écriture, exécution (rwx), groupe : lecture, exécution (r-x) et les autres aucun accès.

La commande ls -ld /ho permet de créer le répertoire /home/etoilenoire

```
root@DEB12Server: /home/etoilenoire#cd
root@DEB12Server: ~#ls -ld /home/etoilenoire
drwxr-xr-x 2 luke jedi 4096 21 déc.  10:47 /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 21 déc.  10:47 /home/etoilenoire
root@DEB12Server: ~#
```

La commande chmod g=r, o=- /home/etoilenoire/* attribue les permissions suivantes aux fichiers du répertoire, groupe lecture uniquement et les autres aucun accès.

La commande chmod –help permet d'afficher l'aide pour la commande chmod

```
root@DEB12Server: ~#chmod g=r, o=- /home/etoilenoire/*
chmod: mode incorrect : « g=r, »
Saisissez « chmod --help » pour plus d'informations.
root@DEB12Server: ~#chmod --help
Utilisation : chmod [OPTION]... MODE[,MODE]... FICHIER...
         ou : chmod [OPTION]... MODE_OCTAL FICHIER...
         ou : chmod [OPTION]... --reference=FICHIER_R FICHIER...
Modifier le mode de chaque FICHIER en MODE.
Avec --reference, modifier le mode de chaque FICHIER à celui de FICHIER_R.

  -c, --changes          comme --verbose, mais seulement en cas de modification
  -f, --silent, --quiet  supprimer la plupart des messages d'erreur
  -v, --verbose          afficher un diagnostic pour chaque fichier traité
      --no-preserve-root ne pas traiter « / » de manière spéciale (par défaut)
      --preserve-root    bloquer le traitement récursif sur « / »
      --reference=FICHIER_R  utiliser le mode de FICHIER_R au lieu de la valeur MODE
  -R, --recursive        modifier récursivement les fichiers et répertoires
      --help        afficher l'aide et quitter
      --version     afficher des informations de version et quitter

Chaque MODE a la forme « [ugoa]*([-+=]([rwxXst]*|[ugo]))+|[-+=][0-7]+ ».

Aide en ligne de GNU coreutils : <https://www.gnu.org/software/coreutils/>
Signalez les problèmes de traduction à : <traduc@traduc.org>
Documentation complète <https://www.gnu.org/software/coreutils/chmod>
ou disponible localement via: info '(coreutils) chmod invocation'
root@DEB12Server: ~#chmod g=r,o=- /home/etoilenoire/*
```

La commande chgrp jedi /home/etoilenoire/plans permet de changer le groupe propriétaire du fichier plans en jedi.

La commande chgrp rebelles /home/etoilenoire/entree_secrete permet de changer le groupe propriétaire du fichier entree_secrete en rebelles.

La commande ls -l /home/etoilenoire/ permet d'afficher les permissions et les informations des fichiers dans /home/etoilenoire.

```
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 21 déc.  10:47 entree_secrete
-rw-r----- 1 root jedi     16 21 déc.  10:46 plans
root@DEB12Server: ~#_
```

Connexion au compte d'utilisateur luke :
La commande ls /home/etoilenoire/ permet de lister les fichiers et répertoires présents dans /home/etoilenoire

La commande cat /home/etoilenoire/plans permet d'afficher le contenu du fichier plans situé dans le répertoire /home/etoilenoire

La commande cat /home/etoilenoire/entree_secrete permet d'afficher le contenu du fichier entree_secrete situé dans /home/etoilenoire

La commande cal > /home/etoilenoire/fichier permet de crée un fichier nommé fichier dans le répertoire /home/etoilenoire et y insère le calendrier du mois courant.

La commande ls /home//etoilenoire/ vérifie que le fichier fichier a été correctement créé en listant le contenu de /home/etoilenoire

La commande rm /home/etoilenoire/fichier permet de supprimer le fichier fichier dans le répertoire /home/etoilenoire

La commande ls /home/etoilenoire/ vérifie que le fichier fichier a été supprimé en listant le contenu de /home/etoilenoire

La commande echo "====" >> /home/etoilenoire/plans ajoute la ligne ==== à la fin du fichier plans sans écraser son contenu.

Remarque : l'administrateur root n'a pas besoin de mot de passe quand il se connecte sous un compte avec la commande su.

```
root@DEB12Server:~#su - luke
luke@DEB12Server:~$ ls /home/etoilenoire/
entree_secrete  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:~$ _
```

Connexion au compte d'utilisateur vador :
La commande ls /home/etoilenoire permet de lister le contenu du répertoire /home/etoilenoire

La commande rm /home/etoilenoire/plans permet de supprimer le fichier plans dans le répertoire /home/etoilenoire

La commande cal > /home/etoilenoire/plans génère un calendrier pour le mois actuel avec la commande cal et redirige la sortie pour créer ou remplacer le fichier plans dans /home/etoilenoire

La commande cat /etoilenoire/plans permet d'afficher le contenu du fichier plans situé dans le répertoire /etoilenoire.

La commande cat /etoilenoire/entree_secrete permet d'afficher le contenu du fichier entree_secrete situé dans /etoilenoire.

La commande echo "====" >> /home/etoilenoire/plans ajoute quatre symboles ==== à la fin du fichier plans sans supprimer son contenu existant.

```
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/plans
-sh: 3: cannot create /home/etoilenoire/plans: 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
root@DEB12Server: ~#
```

Connexion au compte d'utilisateur solo :
La commande ls /home/etoilenoire permet de lister le contenu du répertoire /home/etoilenoire

La commande cal > /home/etoilenoire/fichier permet de créer ou remplace le fichier fichier avec le calendrier du mois actuel.

La commande rm -f /home/etoilenoire/entree_secrete permet la suppression du fichier entree_secrete sans demander de confirmation, même s'il est protégé en écriture.

La commande cat /home/etoilenoire/entree_secrete permet d'afficher le contenu du fichier entree_secrete

La commande exit permet de terminer la session de l'utilisateur.

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

La commande whereis uptime recherche l'emplacement du fichier binaire, du manuel et des fichiers associés à la commande uptime

La commande whatis uptime permet d'afficher une description de la commande uptime

La commande uptime permet d'afficher depuis combien de temps le système fonctionne, ainsi que le nombre d'utilisateurs connectés et la charge système.

La commande ls -l /usr/bin/uptime permet d'afficher les permissions, le propriétaire, le groupe et d'autres métadonnées pour le fichier binaire uptime

La commande chmod o-x /usr/bin/uptime retire le droit d'exécution pour les "autres" utilisateurs sur la commande uptime

La commande ls -l /usr/bin/uptime vérifie les permissions modifiées du fichier uptime

```
root@DEB12Server: ~#whereis uptime
^[[Auptime: /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
 11:51:45 up  1:39,  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: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 14648 19 déc.   2022 /usr/bin/uptime
root@DEB12Server: ~#
```

Connexion au compte d'utilisateur solo :

La commande uptime permet d'afficher depuis combien de temps le système fonctionne, ainsi que le nombre d'utilisateurs connectés et la charge système.

```
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
luke@DEB12Server:~$ exit_
```

Connexion au compte d'utilisateur luke :

La commande uptime permet d'afficher le temps de fonctionnement du système

La commande exit permet de terminer la session de l'utilisateur.

```
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ uptime
 11:55:42 up  1:43,  2 users,  load average: 0,00, 0,00, 0,00
luke@DEB12Server:~$ exit
```

3. La gestion des droits, compléments

La commande chmod 3770 /home/etoilenoire/ définit les permissions du répertoire /home/etoilenoire avec les droits SGID (droit de groupe partagé) et empêche les suppressions par d'autres utilisateurs (sticky bit)

La command ls -ld /home/etoilenoire/ permet d'afficher les détails des permissions du répertoire /home/etoilenoire

La commande echo "fichier un" > /home/etoilenoire/f1 permet de créer un fichier f1 contenant le texte "fichier un".

```
root@DEB12Server: ~#chmod 3770 /home/etoilenoire/
root@DEB12Server: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 21 déc.  11:21 /home/etoilenoire/
root@DEB12Server: ~#echo "fichier un" > /home/etoilenoire/f1
root@DEB12Server: ~#
```

Connexion au compte d'utilisateur luke :

La commande echo "Bonjour" > /home/etoilenoire/f2 permet de créer ou remplacer le fichier f3 avec le texte "Bonjour"

La commande exit permet de terminer la session de l'utilisateur.

```
root@DEB12Server: ~#su - luke
luke@DEB12Server:~$ echo "Bonjour" > /home/etoilenoire/f2
luke@DEB12Server:~$ exit_
```

Connexion au compte d'utilisateur vador :

La commande echo "Bonjour" > /home/etoilenoire/f3

La commande exit permet de terminer la session de l'utilisateur.

```
root@DEB12Server: ~#su - vador
$ echo "Bonjour" > /home/etoilenoire/f3
$ exit
```

La commande ls -l /home/etoilenoire/f ? Lister avec des détails tous les fichiers ou répertoires situés dans /home/etoilenoire dont le nom correspond au motif f

Remarque : du fait du droit SGID, l'ensemble des fichiers sont affiliés au groupe jedi c'est à dire le groupe du répertoire etoilenoire

```
root@DEB12Server: ~#ls -l /home/etoilenoire//f?
-rw-r--r-- 1 root  jedi 11 21 déc.  11:57 /home/etoilenoire//f1
-rw-r--r-- 1 luke  jedi  8 21 déc.  11:58 /home/etoilenoire//f2
-rw-r--r-- 1 vador jedi  8 21 déc.  12:00 /home/etoilenoire//f3
root@DEB12Server: ~#
```

Connexion au compte d'utilisateur vador :

La commande rm /home/etoilenoire/f2 permet de supprimer le fichier f2 dans /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
rm: impossible de supprimer '/home/etoilenoire/f2': Opération non permise
$ exit_
```

La commande chmod -t /home/etoilenoire/ permet de retirer le sticky bit du répertoire, ce qui permet à tout utilisateur ayant les permissions nécessaires de supprimer les fichiers dans ce répertoire.

Connexion au compte d'utilisateur vador :

La commande ls -l /home/etoilenoire/f2
Remarque : dans tous les cas, luke peut détruire le fichier de **vador** puisqu'il est propriétaire du répertoire

```
root@DEB12Server: ~#chmod -t /home/etoilenoire/
root@DEB12Server: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 21 déc.  12:00 /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
```

La commande ls -l /dev/sda1 permet d'afficher les permissions et les métadonnées de la partition /dev/sda1

Remarque : Les périphériques (comme /dev/sda1) se comportent comme des fichiers spéciaux dans un système Linux/Unix. Ils sont représentés sous forme de fichiers dans le répertoire **/dev** et possèdent, comme les fichiers ordinaires, des **droits d'accès**.

Qui peut formater la partition /dev/sda1 ? Seuls les utilisateurs ayant les permissions nécessaires peuvent formater une partition

```
root@DEB12Server: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 21 déc.  10:11 /dev/sda1
root@DEB12Server: ~#
```

La commande cp -p /home/etoilenoire/* /tmp permet de copier les fichiers du répertoire /home/etoilenoire vers /tmp tout en conservant leurs propriétés

La commande ls -l /tmp/plans /tmp/entree_secrete perrmet d'afficher les permissions et les métadonnées des fichiers copiés.

Remarque : Normalement, quand on copie un fichier, la copie appartient à celui qui copie. Ici, rebelles et jedi restent les groupes auxquels sont affiliés respectivement les fichiers entree_secrete et plans. Sans l'option -p, le groupe root serait le groupe propriétaire.

```
root@DEB12Server: ~#cp -p /home/etoilenoire/* /tmp
root@DEB12Server: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 21 déc.  10:47 /tmp/entree_secrete
-rw-r----- 1 root jedi     16 21 déc.  10:46 /tmp/plans
root@DEB12Server: ~#
```

La commande chown luke /tmp/entree_secrete permet de changer le propriétaire du fichier entree_secrete pour l'utilisateur luke

La commande ls -l /tmp/entree_secrete permet d'afficher les détails du fichier entree_secrete notamment les droits d'accès, le propriétaire, le groupe, la taille et la date de modification.

```
root@DEB12Server: ~#chown luke /tmp/entree_secrete
root@DEB12Server: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke rebelles 13 21 déc.  10:47 /tmp/entree_secrete
root@DEB12Server: ~#
```

Connexion au compte d'utilisateur vador :
La commande cat /tmp/entree_secrete permet d'afficher le contenu actuel du fichier entree_secrete

La commande echo "======" >> /tmp/entree_secrete permet d'ajouter (sans écraser) une chaîne de caractères à la fin du fichier entree_secrete

La commande cat /tmp/entree_secrete permet de vérifier si le contenu ajouté apparaît dans le fichier en le relisant et en l'affichant

La commande /tmp/entree_secrete permet d'exécuter le fichier entree_secrete comme un programme ou un script à condition qu'il dispose des droits d'exécution.

```
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:~$ _
```

Connexion au compte d'utilisateur solo :
La commande cat /tmp/entree_secrete permet d'afficher le contenu du fichier entree_secrete

La commande echo "++++++" >> /tmp/entree_secrete permet d'ajouter une chaîne de caractères à la fin du fichier entree_secrete sans modifier son contenu existant.

```
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
```

La commande cat /tmp/entree_secrete permet d'afficher le contenu du fichier entree_secrete

La commande echo "+=+=+=+=" >> /tmp/entree_secrete permet d'ajouter une chaîne de caractères à la fin du fichier entree_secrete

La commande sudo echo "+=+=+=+=" >> /tmp/entree_secrete permet d'ajouter une chaîne de caractères à la fin du fichier entree_secrete en utilisant les privilèges d'administrateur

La commande cd /tmp permet de se déplacer dans le répertoire /tmp

La commande sudo echo "+=+=+=+=" >> /entree_secrete permet d'ajouter une chaîne de caractères à la fin du fichier entree_secrete en utilisant les privilèges d'administrateur

La commande echo "+=+=+=+=" >> /entree_secrete permet d'ajouter une chaîne de caractères à la fin du fichier entree_secrete

La commande cat /tmp/entree_secrete permet d'afficher le contenu du fichier entree_secrete

La commande /tmp/entree_secrete permet d'exécuter le fichier entree_secrete comme un script ou un programme.

```
root@DEB12Server: ~#cat /tmp/entree_secrete
c'est ouvert
======
root@DEB12Server: ~#echo "+=+=+=+=" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#sudo echo "+=+=+=+=" >> /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#cd /tmp
root@DEB12Server: /tmp#sudo echo "+=+=+=+=" >> /entree_secrete
-bash: sudo : commande introuvable
root@DEB12Server: /tmp#echo "+=+=+=+=" >> /entree_secrete
root@DEB12Server: /tmp#cd
root@DEB12Server: ~#cat /tmp/entree_secrete
c'est ouvert
======
root@DEB12Server: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#_
```

La commande chown root /tmp/entree_secrete permet de changer le propriétaire du fichier entree_secrete pour qu'il soit root

La commande ls -l /tmp/entree_secrete permet d'afficher les détails du fichier entree_secrete, y compris son propriétaire, son groupe, ses droits et sa taille.

La commande cat /tmp/entree_secrete permet d'affichee le contenu du fichier pour vérifier les modifications apportées.

La commande echo “+=+=+=+=” >> /tmp/entree_secrete permet d’ajouter la chaîne de caractères à la fin du fichier entree_secrete

La commande /tmp/entree_secrete permet d'exécuter le fichier entree_secrete comme un programme ou un script car le root dispose des droits d’exécution.

Remarque : les droits des utilisateurs ne s’appliquent pas à l’administrateur. Seule restriction, comme tout le monde, root a besoin du droit d’exécution pour activer une commande.

```
root@DEB12Server: ~#chown root /tmp/entree_secrete
root@DEB12Server: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 root rebelles 20 21 déc.  12:09 /tmp/entree_secrete
root@DEB12Server: ~#cat /tmp/entree_secrete
c'est ouvert
======
root@DEB12Server: ~#echo "+=+=+=+=" >> /tmp/entree_secrete
root@DEB12Server: ~#cat /tmp/entree_secrete
c'est ouvert
======
+=+=+=+=
root@DEB12Server: ~#/tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
root@DEB12Server: ~#_
```

La commande chmod -t /tmp permet de supprimer le bit sticky du répertoire /tmp

```
root@DEB12Server: ~#chmod -t /tmp
root@DEB12Server: ~#
```

```
OPTIONS
       Changer le mode d'appartenance de chaque FICHIER en MODE. Avec l'option --reference, modifier le mode de chaque fichier en celui de FICHIER-R.

       -c, --changes
              utiliser le mode bavard en ne signalant que les modifications

       -f, --silent, --quiet
              supprimer la plupart des messages d'erreur

       -v, --verbose
              afficher un diagnostic pour chaque fichier traité

       --no-preserve-root
              ne pas traiter « / » de manière spéciale (par défaut)

       --preserve-root
              ne pas opérer récursivement sur « / »

       --reference=FICHIER-R
              utiliser le mode du FICHIER-R au lieu des valeurs MODE

       -R, --recursive
              modifier récursivement les fichiers et les répertoires

       --help afficher l'aide-mémoire et quitter.

       --version
              afficher les informations de version et quitter.

       Chaque MODE est de la forme « [ugoa]*([-+=]([rwxXst]*|[ugo]))+|[-+=][0-7]+ ».

AUTEUR
       Écrit par David MacKenzie et Jim Meyering.

SIGNALER DES BOGUES
 Manual page chmod(1) line 50 (press h for help or q to quit)_
```

La commande ls -l /etc/shadow permet d’afficher les permissions du fichier contenant les mots de passe système

La commande ls -l /usr/bin/passwd permet d’afficher les droits d'accès au programme permettant de modifier les mots de passe des utilisateurs

Remarque : tout le monde a le droit d'exécuter la commande **passwd**. Avec son droit SUID, un utilisateur endosse les droits de **root**, ce qui lui permet d'accéder au fichier **shadow**.

```
root@DEB12Server: ~#ls -l /etc/shadow
-rw-r----- 1 root shadow 1281 21 déc.  10:39 /etc/shadow
root@DEB12Server: ~#ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 68248 23 mars   2023 /usr/bin/passwd
root@DEB12Server: ~#_
```