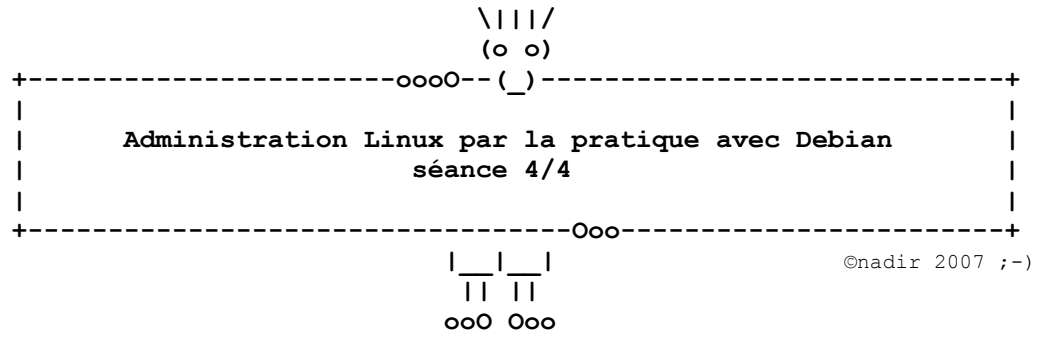


**ci-dessous un rappel de ce que nous avons vu en TD/TP.**

**Sommaire**



# 1. les montages

montage et filesystems

Si on veut accéder à une partition du disque, il faut la « monter » (la commande mount). Mount permet d'affecter tout disque extérieur (partition, cdrom, usb, partage réseau ...) à un répertoire créé pour cela dans l'arborescence.

il y a toujours un montage minimal, celui du root: le « / »

sur ce schema, l'utilisation de disques extérieurs (disques, disquettes, cd ..) s'effectue par **intégration** de ces disques (ou partitions) dans le système fondamental *"racine"*.

Ce mécanisme d'intégration (de montage) est souple mais possible tant que le type de système de fichiers est connu du noyau( ext2, Fat32, ntfs,...).

monter/demonter

l'opération de montage consiste à rattacher :

- un fichier de périphérique situé dans /dev (qui représente la communication physique avec le périphérique)

– à un répertoire (le point de montage) qui doit exister et etre accessible

commande:

mount <dev> <rep>

ex: mount /dev/hda1 /mnt/win

commande longue:

mount -t fstype -o options <dev> <rep>

ex: mount -t fat32 -o rw /dev/hda1 /mnt/win

pour les options et les type de fs possibles: man mount

TP:
trouver la commande pour démonter.
Que faut-il lui passer en paramètre?

montages standards (fstab)

il s'agit des montages qui sont réalisé automatiquement au démarrage de Linux.
Il y a toujours au moins le root « / » !

/etc/fstab -> liste des FS à monter au démarrage

format:

```
[dev]       [mount point] [type] [option]
/dev/hda    /             ext2    ro      (exemple)
```

3e colonne: les FS types principaux sont ext2 et ext3,swap, FAT16 ou FAT32, nfs, ntfs

4e colonne: options de montage séparés par des virgules.
Options de montage principales:

| | |
|---|---|
| user | permettre aux users normaux de monter la partition |
| exec | autorise l'exécution de programme |
| noauto | ne pas la monter au démarrage (ni « mount -a ») |
| ro | read only |
| rw | écriture possible |
| defaults | équivalent de rw, suid, dev, exec, auto, nouser |

5e colonne: booleen autorisant dump a écrire: toujours à 0

6e colonne: ordre de priorité de fsck
- 1 partition racine
- 2 autres partitions
- 0 pas de fsck

en règle générale on essaie de monter "à la main" un systèmes de fichiers avec la commande mount et ses options avant de le figer dans le fstab.

Utilisation de la commande mount

mount (tout court) affiche les montages en cours (actifs)
à noter qu'on peut aussi aller voir le fichier /etc/mtab qui reflete les montages à tout moment
mount -a monter toutes les entrées définies dans /etc/fstab

TP:
1/demonter la partition windows. Essayer d'y accéder depuis X-windows.

2/remonter la partition windows dans le répertoire /media/windows.
quels problèmes cela pose t'il?

3/ si la partition est en ntfs, essayer de la monter en r/w. cela marche t'il?

4/ monter la partition de votre colocataire en lecture seule.

Solution (à voir en version électronique/masqué pour l'impression):

Partages réseaux à la mode Unix(NFS)
On peut partager des répertoires sur une machines, cela fait appel au protocole NFS.
NFS est à considérer comme un système de fichiers distant.

/etc/exports -> liste des répertoires en partage sur le serveur (NFS)
format:
<repertoire> qui(options)
où
- le répertoire est obligatoire
- « qui » peut être: une machine (nom ou IP),un réseau, ou * (tous)
- options peut etre ro/rw/rootsquash le plus souvent
  rootsquash: rendre le root distant simple user sur le partage

par exemple:
/home hostname1(rw,sync) hostname2(ro,sync)

commandes associées:
- exportfs : à utiliser à chaque modif du fichier d'exports
- showmount: afficher les partages publiés sur un serveur NFS. par défaut le sien, on peur préciser un IP pour avoir les partages d'un autre serveur

TP:
1/installer un serveur NFS. Quelle package faut il?

2/partager à tous le réseau votre répertoire /tmp et y placer un fichier qui porte votre prénom

3/ monter la partition d'un de vos collègues, et vérifier bien que lorsque qu'un fichier est créé, vous le voyez simultanément

4/ vérifier le fonctionnement de l'option « rootsquash »

Solution (à voir en version électronique/masqué pour l'impression):

# 2. Utilisateurs et droits

## config Utilisateurs

```
adduser    script         -->    /etc/passwd + group + shadow
useradd    bin
```

Quelles sont les propriétés minimales d'un user ?
uid gid home shell

TP
cat /etc/passwd et /etc/group et /etc/shadow
ajouter user toto
vérifier l'ajout de ligne dans /etc/passwd

format du fichier /etc/passwd :

```
      nom/pass/uid/gid/full name/home/shell
           |        |
           |       Gid=groupe par defaut
           |
           Pass=x dans shadow
           Pass=* user non loggable
```

groupes
- 1 ou plusieurs
- en commun des fichiers
- /etc/groups

Droits et fichiers
un fichier possède toujours
- un propriétaire
- des droits

TP
1/
Avec la commande ls -l, vérifier que les répertoires ont un caractère particulier sur la 1e colonne : essayer avec le répertoire / et le répertoire /etc
(le 1er caractère indique le type: "-" normal, "d" un répertoire, "l" un lien.)

2/vérifier que chaque ligne affiche bien le userid du propriétaire et le groupe

3/trouver un fichier lien

4/Essayer : cd / puis file * et comparer avec ls -l

Commandes de manipulation des propriétaires / groupes / droits
- chmod droits fichier
- chown  user[:group] fichier
- chgrp group  fichier

| **droits chmod**<br>mode numérique (complet) ou alphabetique (partiel) | | |
|---|---|---|
| mode numérique :<br><br>U G O<br>rwxrwxrwx<br><br>une série de 3 chiffres de 0 à 7 symbolisant rwx (en bit 0 ou 1) pour user,group,others<br>-> r=lecture/w=écriture /x=exécution<br><br>exemple<br>lecture pour tous<br>rwx rwx rwx<br>100 100 100<br>→ chmod 444 fichier | Rappel<br>notation binaire<br>rwx = (en décimal)<br>000 = 0<br>001 = 1<br>010 = 2<br>011 = 3<br>100 = 4<br>101 = 5<br>110 = 6<br>111 = 7 | Mode alphabétique :<br><br>dest(+-=)droits<br>ugoa rwx<br><br>exemple<br>lecture pour tous<br><br>→ chmod a+r fichier<br>ou<br>→ chmod ugo+r fichier |

TP
1/
cp /etc/shadow (backup)

2/création en ligne de commande
(root)#useradd minnie
*Dans une autre console, pouvez-vous vous connecter comme minnie ?*
*Voir l'effet dans /etc/passwd, dans /etc/group, dans /etc/shadow*

3/(root)#passwd minnie (Donner le mot de passe)
*Voir l'effet dans /etc/passwd, dans /etc/group, dans /etc/shadow*

*Connectez-vous alors comme minnie*
*Avez vous un rép. personnel (tapez pwd) ?*

*4/Restez loggé-Passer dans la console root et tenter de supprimer le compte minnie*
userdel minnie (normalement echec)
*Faites en sorte d'effectuer la suppression (il faut delogger minnie)*
*Voir l'effet dans /etc/passwd, dans /etc/group, dans /etc/shadow*

*5/Création interactive*
*# adduser minnie*
*Voir l'effet dans /etc/passwd, dans /etc/group, dans /etc/shadow*
*le répertoire personnel /home/minnie existe-t-il ?*

6/vous etes maintenant à meme de dire la Différence entre adduser et useradd?
*(utiliser la commande file par exemple)*

*7/Comparer /home/minnie et /etc/*skel (ls -al)
Créer un repertoire nommé « voila » dans /etc/skel
Créez un utiliateur avec adduser. Verifier que tout est copié dans son home (« voila »)

8/Suspension d'un compte
passwd -l minnie
*Essayer de connecter minnie*

passwd -u minnie
*Remet en service ce compte*

9/Forcer le changement d'un mot de passe
passwd -e minnie
*Essayer de se reconnecter en minnie*

10/Suppression d'un compte
userdel -r minnie
*verifiez l'effet de l'option -r : suppression aussi du rép. Perso*

11/Gestions des groupes
(ajouter 2 utilisateurs : mickey, donald)
groupadd rugbyman  (ajout d'un groupe)
*Vérifiez dans /etc/group*

(ajouter l'utilisateur chabal)
adduser chabal rugbyman  (ajoute chabal au groupe rugbyman)
*Quel effet dans /etc/group? Ajouter dans rugbyman l'utilisateur donald (verifier /etc/group)*

deluser chabal rugbyman
groupdel rugbyman

13/ dans /etc/shadow, Copier le password d'un user quelconque (mickey) sur celui de root ou dupliquer la ligne de mickey puis remplacer le debut de ligne « mickey: » par « root: ». Vérifier que vous pouvez vous logger en root avec le pass de mickey.

14/usurpation d'identité
En tant que root, changer le uid d'un user quelconque (donald) à 0.
Puis se logguer avec le user/password de donald
Faire un id/whoami : vous devez etre root.

15/Créer un user donald et créer un repertoire /home/rep
Attribuer r.x (other) à ce répertoire

Essayer d'y accéder avec le user mickey
- ls marche t'il ?
- cd marche t'il ?
- mkdir marche t'il ? (créer un rep mickey sur rep)

faire la même chose avec ..x à ce rep
faire la même chose avec rwx à ce rep
-quels sont les différences ?

16/
Si on modifie USERGROUPS à no dans /etc/adduser.conf, quel sera l'effet ?

Afficher toutes les infos sur un fichier
La commande stat permet d'obtenir une information plus poussée sur un fichier.
Exemple : stat /etc/passwd

TP
Comparer la commande file et la commande stat

## Cas particuler de root

Le "super-utilisateur" root n'est pas soumis aux restrictions des permissions.

TP
-Vérifier que /etc/shadow est inaccessible même en lecture aux utilisateurs
-Vérifier que ses permissions sont rw-r-----, seul le propriétaire root peut écrire
- Root se supprime ce droit de lecture : chmod ug-rw /etc/shadow
- Vérifier /etc/shadow
- vérifier que Root peut le lire, le copier et le modifier quand même.

root peut donc retrouver des fichiers appartenant à des utilisateurs ayant perdu leurs droits d'accès.

TP

```
1/
- (mickey)cp ~/.bashrc ./test.txt
- (mickey)chmod ugo=  ./test.txt    aucune permission sur le fichier
- (mickey)cat ./test.txt            il est totalement protégé en lecture
- (root) cat ~mickey/test.txt       mais pas pour root

2/
retablir un droit rw sur test.txt en tant que root fonctionne toujours
rétablir un droit rw sur test.txt en tant que mickey. Possible ?
```

## Droits sur les répertoires

Pour les répertoiresla signification des attributs est différente de celle des fichiers.

- **r** : lire le contenu, la liste des fichiers (avec ls)
- **w** : modifier le contenu : droits de créer et de supprimer des fichiers dans le répertoire (avec cp, mv, rm). Si on attribue **w**, il faut attribuer aussi **x** sur le répertoire.
- **x** : permet d'accéder aux fichiers du répertoire et de s'y déplacer (avec cd).

```
TP

1/Essayer les diverses possibilités pour user, groupe, other

2/Un utilisateur mickey peut-il créer des rép. un peu partout ?
La commande est mkdir nom-rep
Essayer par exemple dans /etc ou dans /usr

3/ remplir le tableau ci-dessous quand l'utilisateur est donald
(root)mkdir /picsou
(root)chown mickey:mickey /picsou
(mickey)touch /picsou/test.txt
```

| Droits pour other Rwx (sur /picsou) | (donald) ls /picsou | (donald) cd /picsou | (donald) rm /picsou/test.txt |
|---|---|---|---|
| 000 | | | |
| 001 | | | |
| 010 | | | |
| 011 | | | |
| 100 | | | |
| 101 | | | |
| 110 | | | |
| 111 | | | |

## Droit Suid

Sa présence permet à un fichier exécutable de s'exécuter sous l'identité et donc les droits de son propriétaire.

```
TP
Observez :
1/
ls -al /etc/shadow
-rw-r-----  root root  shadow

2/
ls -l /usr/bin/passwd
-r-Sr-xr-x root bin passwd
Vérifier la presence du bit suid.
Comme le droit x est accordé à tous, chacun peut donc exécuter la commande passwd.
```

```
3/
(root)cp /usr/bin/passwd /bin/mdp
(root)chmod -s /bin/mdp
(mickey)mdp (donner le mdp actuel)
      --> echec, mdp execute en tant que mickey ne peut acceder à /etc/passwd
(root)chmod +s /bin/mdp
(mickey)mdp
      --> succes

4/
(root) cp /bin/bash /tmp/sh
(mickey) /tmp/sh → on se trouve sur un nouveau shell marqué par le # ci-dessous
(mickey)   # touch /etc/passwd → erreur renvoyé par la commande touch
(rout) chmod +s /tmp/sh
(mickey) réssayer le /tmp/sh + touch  → fonctionne
```

Note : il existe un droit SGID non couvert

## droit "sticky bit"

Ce droit spécial, traduit en "bit collant", à un rôle important surtout pour les répertoires.
Il réglemente le droit w sur le répertoire, en interdisant à un utilisateur quelconque de supprimer un fichier dont il n'est pas le propriétaire

```
TP
1/
vérifier que le sticky bit est présent sur le rép. /tmp
Pour quelle raison ?

2/
(root)mkdir /tempo
(root)chmod 777 /tempo
(mickey)touch /tempo/mickey.txt
(donald)touch /tempo/donald.txt
(donald)rm /tempo/mickey.txt
      --> ca marche, donald peut supprimer (à cause du w sur le repertoire)
(root)chmod +t /tempo
(mickey)touch /tempo/mickey.txt
(donald)rm /tempo/mickey.txt
      --> ERRREUR, ca ne marche pas, donald n'a pas le droit à cause du sticky bit)
```

## (bonus) Droits et propriété par défaut : umask

Lors de la création d'un fichier/répertoire, voici les règles qui s'appliquent :

- le **propriétaire** est l'utilisateur qui l'a créé
- le **groupe** est le groupe *principal* de l'utilisateur qui l'a créé
- les droits d'accès *initiaux* vont dépendre de la commande umask

pourquoi « **umask** » ?
Umask signifie « user file creation mode mask », masque de création de fichier utilisateur. Car ce qui est appliqué est un masque binaire du droit total avec la valeur de umask (un « and not » binaire). On peut aussi dire que umask est un masque de protection (du droit total).
Le droit total est 0666 pour les fichiers et 0777 pour les répertoires (pas de x pour les fichiers).

Utilisation :
- **umask** affiche le masque de l'utilisateur actif
- **umask -S** affiche les permissions correspondantes au masque sous forme symbolique.
- **umask *masque*** Où ***masque*** est un nombre exprimé sous forme octale.

La valeur par défaut typique pour l'umask est 022 en octal, ce qui signifie u=rwx,g=rx,o=rx.

Exemple de droits effectifs après création par un utilisateur dont umask=**027 :**

```
  777 = 111 111 111 permissions maxi pour un répertoire      = rwx rwx rwx
- 027 = 000 010 111 masque de protection
= 750 = 111 101 000 permissions effectives =                 = rwx r-x ---

  666 = 110 110 110 permissions maxi pour un fichier         = rw- rw- rw-
- 027 = 000 010 111 masque de protection
= 640 = 110 100 000 permissions effectives                   = rwx r-x ---
```

TP
1/configurer le umask pour root, afin que les droits par defaut soientt u=rwx,g=,o=
2/essayer umask 022 puis 027 en créant un fichier puis un répertoire
3/comment rendre permanentes les modifs de umask ?

Solution (à voir en version électronique/masqué pour l'impression):