# TP1-2 d'administration Unix

F. Butelle M. Mayero

2015

**Conseil** : rédiger un compte-rendu de TP.
Se "loguer" en tant qu'*etudiant*. Expliquez pourquoi on vous demande de vous connecter en tant qu'*etudiant* et non en tant que *root*.

## 1 Commandes de base d'Unix

Grâce à la commande `man`, décrivez en une phrase ce que font les commandes suivantes (essayez les, elles serviront pour la suite !) :
`tar, compress, gzip, bzip2, find, su, head, pwd, grep, cmp, du, df, diff, cat, info, useradd, usermod, userdel, groups, groupadd, groupmod, groupdel, chmod, chown, chgrp, chroot, newgrp, passwd`

## 2 Système de fichier

Pensez à noter les commandes que vous utiliserez pour les questions suivantes :

1. Combien y a-t-il de systèmes de fichier montés sur le système ? A quoi correspondent-ils ?
2. Quel espace disque occupe votre répertoire de connexion ?
3. Quel est le numéro d'inode de votre répertoire de connexion ?
4. Créer un répertoire nommé rep. Combien y a-t-il de liens sur rep ? A quoi correspondent-ils ?
5. Dans rep, créer un sous-répertoire nommé ssrep. Combien y a-t-il de liens sur rep ? Pourquoi ?
6. Créer un fichier `titi` dans ssrep. Quel est son numéro d'inode ?
7. Changer le nom du fichier en `tata` ; le numéro d'inode change-t-il ?
8. Créer un lien physique `liendur` vers le fichier `tata`. Vérifier que le compteur de références de tata et de `liendur` est bien 2 et que les inodes sont identiques.
9. Créer maintenant un lien symbolique `liensymbo` vers tata. Que constatez-vous au niveau du compteur de références ?
10. Déplacer les fichiers `liendur` et `liensymbo` dans un autre répertoire. Les liens sont-ils encore valides ? Essayez avec un répertoire d'un autre volume (SGF) que celui de `tata`, par exemple /tmp.
11. Même question si l'on supprime le fichier `tata`
12. Dans le répertoire ssrep, créer un lien sur le répertoire rep. Que se passe-t-il si on utilise la commande `ls -Ral rep` ?

## 3 Gestion des utilisateurs

1. Etudiez `/etc/passwd` : combien d'utilisateurs sont définis localement sur votre système ? Dire les types d'utilisateurs (humains ou pas).
2. Quel est le shell de `root` ?
3. Étudier plus en détail `/etc/passwd, /etc/shadow, /etc/group`
4. Créer deux nouveaux utilisateurs guest1 et guest2 : chaque utilisateur doit avoir son propre groupe (gpguest1 et gpguest2) ; leur répertoire de connexion doit être dans `/home`.
5. Donner un mot de passe aux nouveaux utilisateurs.
6. Vérifier les contenus des fichiers `/etc/passwd, /etc/shadow, /etc/group` avant et après ces créations.
7. Consulter le fichier d'audit grâce à la commande `journalctl`.

8. Allez dans le répertoire de connexion de guest1, listez tous ses fichiers et répertoires avec les détails et les fichiers et répertoires "cachés".

   Ajoutez lui gpguest2 comme groupe secondaire de guest1 (en utilisant `usermod`).

9. Loguez vous en tant que guest1 ; créez quelques fichiers dont un de nom pgm1, dans lequel vous mettrez les commandes suivantes :

   ```
   echo "debut"
   sleep 500
   echo "fin"
   ```

   Changez les droits pour le rendre exécutable puis lancez le. Puis observez la table des processus avec `ps -el`.

10. Vérifier votre situation actuelle avec la commande `id`.
11. Passez dans le groupe de gpguest2 avec newgrp. A nouveau vérifier avec la commande `id`.
12. Lancez le même pgm1 et observez la table des processus. Changez le groupe du fichier pgm1 et ôtez les droits d'exécutions aux "autres".
13. Quittez la session de l'utilisateur guest1 et logez vous comme guest2, vérifiez que vous avez bien le droit de lancer pgm1. Regardez à nouveau la table des processus.
14. Quittez la session de guest2. Supprimez maintenant l'utilisateur guest2 (userdel sans l'option -r). Allez voir les fichiers dans `/home/guest2`. Tapez `journalctl -f` consultez les fichiers `/etc/passwd, /etc/shadow, /etc/group`.
15. L'utilisateur guest1 veut changer de login : tout en gardant ses fichiers, il désire être guest0, avec comme répertoire de connexion `/home/guest0`.
    Que faut-il faire ? Vérifier en se loguant sur le compte de guest0 et en tapant `ls -l`. Consultez le fichier d'audit.

# 4 Partitions — montage

1. Consultez la table des partitions du disque dur (commande `fdisk`).
   Combien y a-t-il de cylindres ? Listez les types de partition connus.
   Affichez la table des partitions. .
2. Multipliez (commande `bc` dans une autre console pour avoir une calculatrice en ligne) le nombre de têtes par le nombre de secteurs/piste, par le nombre de cylindres et par la taille d'un secteur (512 octets en général). Vous devez retrouver la taille du disque dur.
3. Passez en mode expert et affichez la table des partitions avec la même commande p.
4. Quittez le mode expert et notez le fichier spécial (notons-le ici `/dev/sdaN`) associé à la partition de swap.
5. Quittez fdisk. Nous allons sauver la table de partitions avant de la modifier.
   D'abord consultons ces fichiers spéciaux liés au disque dur : `ls -l /dev/sda*`. Si ce sont des liens vers `ide/host0/bus0/target0/lun0/...` c'est que vous êtes sur un système avec une gestion plus complexe mais plus complète des périphériques. Il faut alors aller voir ces fichiers et non ceux de `/dev/sda*`.
   Ce sont des périphériques en mode bloc et `/dev/sda` (ou sa forme `/dev/ide/host0/bus0/target0/lun0/disc`) représente l'ensemble du disque et non une partition. C'est ce que nous allons utiliser :
   `dd if=/dev/sda of=/sauvetable bs=512 count=1`
   (même si `/dev/sda` est un lien il n'y a pas de problème).
   `bs` signifie block size, `count` signifie nombre de blocs à lire et écrire.
   La fin du fichier /sauvetable devrait être analysable en hexadécimal :
   `od --format=x1 -j 446 /sauvetable`
   Vous devez pouvoir voir sur la quatrième colonne les types de partitions des quatre premières partitions.
6. Nous allons supprimer la partition de swap et jouer avec mais avant il faut éviter que le système ne l'utilise.
   (a) Consultez l'état de la mémoire avec `cat /proc/meminfo`
   (b) Quelle est la capacité mémoire de votre machine ? Le swap ("zone d'échange") est-il utilisé ?
   (c) Signalons au système qu'il ne peut plus utiliser la zone de swap : `swapoff`
7. Vérifions le nouvel état mémoire avec `cat /proc/meminfo`
8. Avec fdisk changez le type de la partition `/dev/sdaN` en type FAT32 Win95(LBA). Quittez fdisk en sauvant la nouvelle table avec w.
9. Il est possible que le système signale la nécessité de redémarrer la machine pour prendre en compte la nouvelle table de partition, cela dépends du BIOS. En cas de besoin, faites le, mais avant il faut mettre en commentaire la ligne correspondant à la partition swap dans `/etc/fstab`.
10. Une fois le système redémarré, il faut encore créer un SGF (Système de Gestion de Fichiers) sur `/dev/sdaN` : `mkfs -t vfat /dev/sdaN`
    puis monter ce SGF, par la commande `mount -v /dev/sdaN /mnt/disk` ; puis vérifier avec la commande `df`.
11. Créer un fichier dans le répertoire `/mnt/disk`. Le fichier doit contenir des chaînes de caractères particulièrement identifiables par exemple `password=toto`.
12. Démonter le SGF, puis le remonter sur un autre répertoire. Vérifier que le fichier est toujours présent. Pour vérifier qu'il s'agit bien d'un SGF de type vfat, il suffit d'essayer de créer un autre fichier de même nom que le premier mais utilisant des majuscules au lieu des minuscules... Que constatez-vous ?
13. Supprimez ce fichier. Démontez la partition et lancer la commande suivante :
    `dd if=/dev/sdaN count=10000 | strings | grep password=`
    Expliquez le résultat obtenu. Donnez une solution à ce problème.
14. Changer le type de la partition avec fdisk. Relancer la commande `dd` précédente, a-t-on presque toujours le même résultat et pourquoi ? Essayez de monter à nouveau la partition... Ça marche ! Pourquoi ?
15. Remettre tout en état pour que le système voit bien à nouveau `/dev/sdaN` comme une zone de swap... Pensez à rectifier `/etc/fstab` au besoin...
16. Dans quel système de gestion de fichiers (SGF) se trouve le répertoire `/home` ? Comment faire si cette partition devient pleine ? On a acheté et installé un nouveau disque dur `/dev/sdb`. On veut que les utilisateurs ne s'aperçoivent de rien. Comment faire ?