TD COLD #3 - Partie 1

DROITS

SYSTEME MULTI-UTILISATEUR

Le système Unix (et donc Linux) a été concu dès le début pour etre un système multi-utilisateurs, avec un système efficace de gestion des droits.
Même en étant installé et configuré pour n'avoir qu'un utilisateur (humain) unique, un système Linux possède de nombreux comptes. Certains de ces comptes utilisateurs sont présents dès l'installation et sont utilisés par le système pour gérer différentes taches ou services.
Il est donc primordial de bien savoir gérer ses droits même sur un système à utilisateur unique, et à fortiori lorsqu'on est sur un système partagé.

Les droits unix sont principalement construits suivant 2 axes orthogonaux : **qui** a le droit et **quelles actions** le droit concerne-t-il.

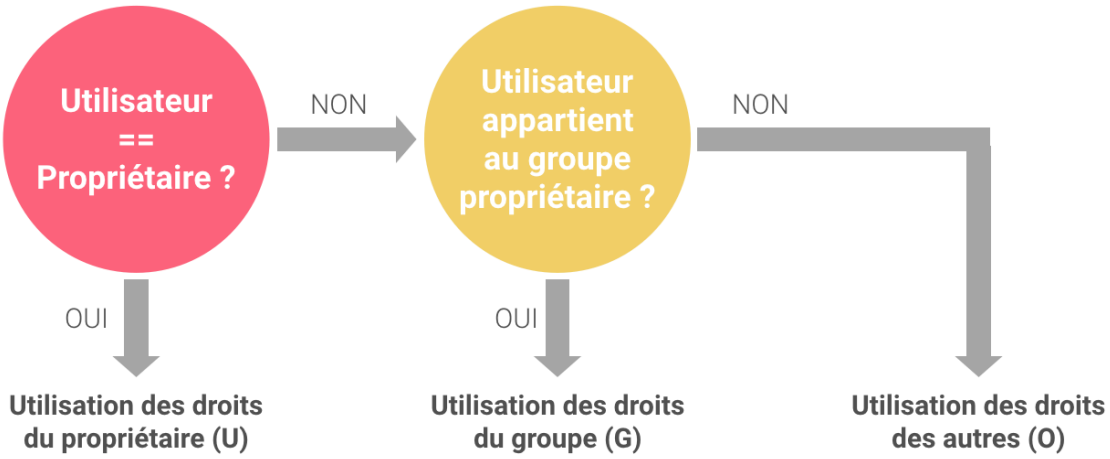
Qui

Sur Linux, un compte utilisateur est défini par un nom et un uid, et il appartient à au moins un groupe (mais peut appartenir à plusieurs).

Un fichier ou un répertoire appartient forcément à un utilisateur et à un groupe (groupe qui peut être différent de ceux auxquels appartient l'utilisateur).

Un droit peut s'appliquer sur 3 catégories de personnes :
- sur le **propriétaire** (**U**ser) du fichier, qui est un utilisateur unique ;
- sur le **groupe** (**G**roup) propriétaire du fichier, qui peut contenir plusieurs utilisateurs ;
- sur toute **autre** (**O**ther) personne n'appartenant pas aux deux catégories précédentes.

Chacune de ces catégories peut avoir des droits différents. Pour vérifier si une action est permise, le système utilise l'algorithme suivant :



Il est tout à fait possible que le propriétaire ai moins de droits que les autres personnes.

Quoi

3 catégories d'actions sont définissables pour un droit :
- le droit de **lecture** (**R**ead) ;
- le droit d'**écriture** (**W**rite) ;
- le droit d'**execution** (e**X**ecute).

Pour un fichier :
- le droit *R* correspond à l'action de voir le contenu du fichier ;
- le droit *W* correspond à l'action de modifier le contenu du fichier ;
- le droit *X* correspond à l'action d'executer le fichier comme s'il s'agissait d'une commande ou d'un programme.

Pour un répertoire :
- le droit *R* correspond à l'action de voir le contenu du répertoire, donc de lister le nom des fichiers ou répertoires contenus ;
- le droit *W* correspond à l'action de modifier le contenu du répertoire, c'est à dire ajouter, supprimer ou renommer un fichier ou un répertoire ;
- le droit *X* correspond à l'action de se déplacer dans un répertoire (avec la commande *cd* par exemple).

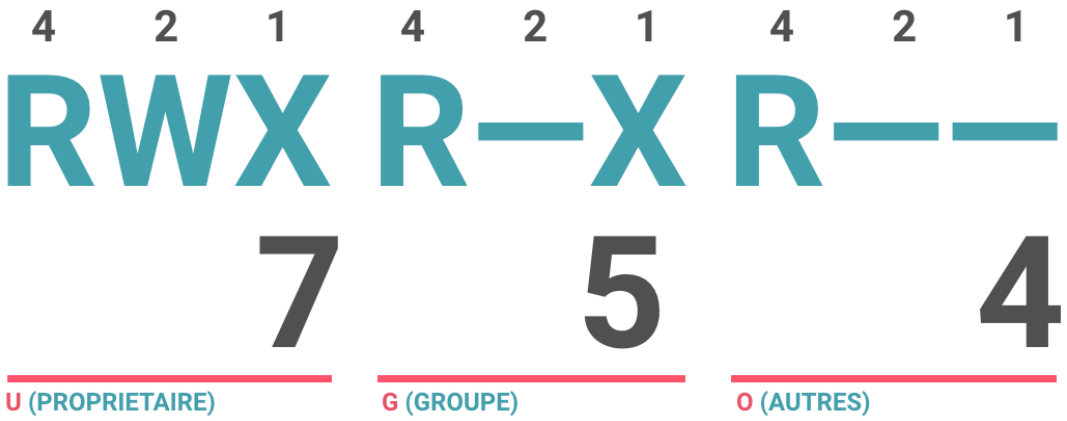
Il est possible de supprimer un fichier sur lequel on n'a pas de droit *W*, en ayant les droits *W* sur le répertoire.
Il est aussi possible d'avoir des droits *X* sur un répertoire sans avoir les droits *R*, ce qui fait que l'on peut se déplacer dans un répertoire sans connaitre le contenu (par exemple en ayant le chemin complet).

Expression

Les droits sur un fichier ou un répertoire peuvent s'exprimer sous deux formes :

- soit sous la forme d'un triplet de triplets de lettres ou de tiret ;

- soit sous la forme d'un triplet de nombres en octal.



COMMANDES

Voici une liste des commandes que vous devez connaitre.

whoami

Retourne le nom de l'utilisateur.

groups

Retourne la liste des groupes auxquels appartient l'utilisateur.

ls -l <répertoire>

Liste le contenu d'un répertoire en affichant différentes caractéristiques, notamment les droits sous la forme d'un triplet de triplet de lettres. Le « ***d*** » juste avant les droits indique qu'il s'agit d'un répertoire (**d**irectory). Sans le paramètre du répertoire, liste le répertoire courant.

chmod <droits> <fichier/répertoire>

Permet de modifier les droits du fichier ou répertoire passé en paramètre. L'action n'est permise qu'avec les droits *W* sur les items affectés. L'option « -R » permet de changer des droits sur le répertoire et de manière récursive sur tout son contenu.
Le passage de droits peut se faire de deux facons :

- soit en passant directement les droits sous forme d'un triplet de nombres en octal ;
- soit en passant une chaine de caractère construite de la manière suivante :
  - une ou plusieurs lettres pour ***qui*** : U, G, O, ou A (All) ;
  - le signe « + » pour ajouter des droits, le signe « - » pour en retirer ;
  - une ou plusieurs lettres pour ***quoi*** : R, W, X

Exemple : ug-w, a+rwx, …

chown <user>.<group> <fichier/répertoire>

Permet de changer le propriétaire ou le groupe propriétaire d'un fichier ou d'un répertoire. L'action n'est permise qu'avec les droits *W* sur les items affectés. L'option « -r » permet de changer des droits sur le répertoire et de manière récursive sur tout son contenu.
ATTENTION : si vous « donnez » un fichier à quelqu'un d'autre et que vous n'avez plus de droits dessus, il n'est plus possible de revenir en arrière (sauf en étant administrateur).

sudo <commande>

Permet d’executer une commande en tant que root, le superutilisateur (ou administrateur) qui a tous les droits (la vérification des droits ne s’applique pas pour lui).
A MANIER AVEC UNE EXTREME PRECAUTION !