

LES DROITS UTILISATEURS SOUS LINUX

1) Notion de permissions sous Linux

1) Introduction

Sur un système d'exploitation moderne, la plupart des fichiers qui sont sur un ordinateur n'appartiennent pas à l'utilisateur qui travaille actuellement sur cet ordinateur, mais appartiennent plutôt au système d'exploitation, aux différents logiciels installés ou aux autres utilisateurs de l'ordinateur. Il est donc prudent que chaque utilisateur de l'ordinateur ne puisse modifier que les fichiers qui le concernent. Les systèmes d'exploitation gèrent donc pour chaque fichier et chaque dossier de l'ordinateur quels utilisateurs ont la « permission » de créer, modifier, lire, renommer, supprimer... ces fichiers.

A noter que ces permissions ne sont pas attribuées à des personnes mais à des sessions. Si un utilisateur se connecte à un ordinateur avec la session « toto », non seulement il pourra modifier tous les fichiers pour lesquels cette session a les droits de modification, mais tous les logiciels qui tournent sur cette session ont aussi ces mêmes droits (et notamment les virus!). C'est pour cela qu'il est vivement conseillé de toujours travailler avec une session qui a des droits limités pour notamment éviter qu'un virus (ou un pirate) ne puissent faire trop de dégâts.

2) Vocabulaire

- Utilisateur : Session créée sur l'ordinateur. La liste des utilisateurs (c'est à dire des sessions) est disponible dans le fichier « /etc/passwd »
- Groupe : Groupe d'utilisateurs (de sessions) ayant les mêmes droits sur un ensemble de fichiers. La liste des groupes est disponible dans le fichier « /etc/group »
- root : Les systèmes Linux ont un utilisateur spécial appelé « root » qui est le super-administrateur du système. Il possède tous les droits et peut modifier, créer ou supprimer n'importe quel fichier ou paramètre. Il est utilisé par l'OS pour faire son travail et il va de soi que l'on ne se connecte jamais avec la session root !

II) Droits d'un fichier ou d'un dossier

1) Visualiser les droits

Sous Linux, on distingue pour chaque fichier ou dossier :

- L'utilisateur propriétaire qui est en général celui qui a créé le fichier et qui a souvent tous les droits sur le fichier.
- Le groupe propriétaire qui contient une liste d'utilisateurs auxquels on veut donner des droits spécifiques sur le fichier.
- Les autres utilisateurs qui ont en général peu de droits sur le fichier.

Pour visualiser les droits d'une série de fichiers, on peut utiliser la commande « **ls -l** »

```
~$ ls -l
drwxr-xr-x 2 thibaud thibaud 4096 juil. 8 17:41 Images
-rw-rw-r-- 1 thibaud smp 45825959 juil. 8 11:22 'Fonds de plan.pdf'
-rw-rw-r-- 1 karl smp 140 juil. 20 11:34 'Ajouter installation.txt'
-rw-r--r-- 1 karl smp 78136664 mai 10 10:48 'Montagne 1.m4a'
-rwxrw-r-- 1 thibaud smp 77668 juil. 20 11:33 script.py
```

droits utilisateur groupe nom du fichier

Cette commande présente les droits de chaque fichier ou dossier sous la forme d'une liste de 10 caractères. Prenons l'exemple du dernier fichier « script.py » : **- rwx rw- r--**

- Le **premier caractère** « - » désigne la **nature de l'objet** : « - » pour un fichier et « d » pour un dossier.
- Les **3 caractères suivants** « **rwx** » désignent les droits de **l'utilisateur propriétaire** du fichier qui est ici « thibaud » : Ces droits sont **r** comme « read » (lecture), **w** comme « write » (écriture) et **x** comme « eXecute » (exécution)
- Les **3 caractères suivants** « **rw-** » désignent les droits du **groupe propriétaire** qui est ici « smp ». Ce groupe a ici le droit de lecture et d'écriture mais pas d'exécution à cause du - final.
- Les **3 derniers caractères** « **r--** » désignent les droits des **autres utilisateurs** : ni « thibaud », ni aucun des utilisateurs du groupe « smp ». Ces utilisateurs n'ont que le droit de lecture.

A faire : Observer et comprendre les droits des autres fichiers et dossiers de la liste ci-dessus.

Attention : Ces droits ont des sens différents selon qu'ils sont appliqués à des fichiers ou des dossiers !

Pour les fichiers :

- Lecture : on peut par exemple lire le fichier avec un logiciel.
- Écriture : on peut modifier le fichier et le vider de son contenu.
- Exécution : on peut exécuter le fichier s'il est prévu pour, c'est-à-dire si c'est un fichier exécutable (script, programme).

Pour les dossiers :

- Lecture : on peut afficher contenu du répertoire (avec la commande **ls**).
- Écriture : on peut créer, supprimer, renommer les fichiers qu'il contient.
- Exécution : on peut entrer dedans (avec la commande **cd**) et accéder aux sous-dossiers.

2) Changer les droits

Chaque fichier reçoit des permissions par défaut au moment de sa création. Les OS étant bien conçus, la plupart des utilisateurs dans la plupart des utilisations n'ont en général pas besoin de modifier ces permissions. Toutefois, il existe des cas où on a besoin de modifier les permissions par défaut : pour rendre un script exécutable, pour partager un dossier avec plusieurs personnes,...

Seuls root et le propriétaire d'un fichier ou d'un dossier peuvent changer ses permissions d'accès.

L'utilisateur propriétaire sera noté « u », le groupe propriétaire noté « g » et les autres utilisateurs notés « o » (pour others).

Pour changer les droits d'un fichier ou d'un dossier, on utilise la commande **chmod** avec les attributs u g o pour « qui », r w x pour « quoi » et le symbole + ou - pour ajouter ou ôter des droits.

Exemples :

- Pour ajouter le droit de lecture aux autres utilisateurs : **chmod a+r fichier**
- Pour retirer le droit de modification au groupe propriétaire : **chmod g-w fichier**
- Pour ajouter le droit d'exécution à l'utilisateur propriétaire : **chmod u+x fichier**

A faire : Que fait la commande suivante ? **chmod go+rw fichier**

3) Changer l'utilisateur propriétaire ou le groupe propriétaire

Pour changer l'utilisateur propriétaire d'un fichier : **chown utilisateur fichier**

Pour changer le groupe propriétaire : **chgrp groupe fichier**