#### Droits d'accès sur les fichiers ou répertoires (Chmod)

Le système de permis de Linux est basé sur un modèle d'utilisateurs / groupes qui sont devenus la base principale de la sécurité sous Linux, les utilisateurs et les groupes bénéficient de droits à des fichiers et des répertoires.

C'est l'une des fonctions qui font que Linux soi presque immunisé aux Virus d'ordinateur, les virus doivent être capables d'écrire sur des fichiers pour pouvoir les infecter et être exécuté d'une certaine manière pour pouvoir infecter d'autres fichiers, avec le système de permis de Linux les virus ne peuvent pas se copier à toutes les fichiers, si l'utilisateur qui exécute le virus manque d'autorisations sur le reste du système, le virus ne pourra pas se reproduire.

En Linux nous avons trois différents droits de fichier :

- r : read (lecture) : Quand l'autorisation de lecture sera actif sur un répertoire il signifie qu'on pourra énumérer les fichiers stockés dans ce répertoire, si elle est assignée à des fichiers on pourra lire son contenu.
- w: write (écriture): Lorsque l'écriture est activée sur un répertoire, vous pouvez créer et supprimer des fichiers dans le répertoire, s'il est activé pour les fichiers il signifie qu'on pourra modifier son contenu.
- x : execute (exécution) : Si la permission d'exécution est activé sur un répertoire, signifie que l'utilisateur peut exercer d'autres fonctions dans le répertoire et s'il est actif sur les fichiers, signifie que le fichier pourra être exécute depuis la ligne de commandes.

Pour afficher les autorisations de fichiers et de répertoires, il est nécessaire d'exécuter la commande suivante :

```
ls -1
```

Cette commande nous donnera un résultat similaire à:

Les droits sont assignés en groupes de trois et correspondent à :

- **Propriétaire** (owner) : Propriétaire de des fichiers ou répertoires.
- **Groupe** (group) : groupe auquel appartient le propriétaire du fichier.
- Autres (others) : les utilisateurs d'autres groupes.

#### Commandes

Linux dispose de 3 commandes pour modifier les autorisations, le propriétaire et le groupe d'un fichier ou un répertoire, respectivement:

• chmod : Permet de changer les permissions du fichier ou du répertoire.

```
$ chmod [autorisations] [fichier / répertoire] [options]
```

• **chown** : Est utilisée pour changer le propriétaire du fichier ou de répertoire.

```
chown [nouveau propriétaire] [fichier / répertoire] [options]
```

• chgrp : Pour changer le groupe de fichiers ou de répertoires.

```
chgrp [groupe] [fichier / répertoire] [options]
```

## Changer les permissions en utilisant des caractères.

```
Symbole Description

Identités u C'est le propriétaire du fichier ou le répertoire.
g C'est le groupe du fichier ou du répertoire.
o D'autres utilisateurs, le reste du monde.
a Tout le monde - propriétaire, groupe et autres.

Permis r Accès de lecture.
w Accès en écriture.
x Accès d'exécution.

Actions + Ajouter permis.
- Élimine les permis.
- Le seul permis.
```

## Exemples

1 sur 2

Commande	Description	Résultats
chmod u+rwx photol.png	Ajouter toutes les autorisations pour le propriétaire.	rwx
chmod g+x photol.png	Ajouter la permission d'exécution pour le groupe.	rwx-x
chmod o+r photol.png	Ajouter la permission de lecture pour les autres utilisateurs.	rwx-xr
chmod u-rw photol.png	Supprimer les permissions de lecture et écriture pour le propriétaire.	x-xr
chmod a=r photol.png	Nous établissons lecture comme seule autorisation pour les 3 groupes.	rrr
chmod u+rx,o+x photol.png	Nous ajoutons les autorisations lecture et exécution pour le propriétaire et exécution pour les autres.	

# Changer les permissions en utilisant des chiffres.

Chaque autorisation ont assigné une valeur, même quand l'autorisation ne sera pas active. Pour pouvoir utiliser les chiffres nous devrons tenir compte le tableau suivant avec leurs valeurs respectives :

Valeur	Permis	Description
0		Zéro signifie que pas de permis ont été attribués.
1	x	On a seulement assigné celui d'exécution.
2	-w-	Seulement autorisation d'écriture.
3	-wx	Autorisations écriture et exécution.
4	r	Seulement autorisation de lecture.
5	r-x	Autorisations lecture et exécution.
6	rw-	Autorisations lecture et écriture.
7	rwx	Autorisations de lecture, écriture et exécution.

Les autorisations par chiffres sont assignées dans des groupes de 3 (propriétaire, groupe, autres), il n'est pas possible d'assigner seulement pour un ou deux d'entre eux.

### Exemples

Commande	Résultats	Description
chmod 600 photol.png chmod 644 photol.png chmod 700 photol.png chmod 751 photol.png chmod 711 photol.png chmod 666 photol.png chmod 777 photol.png	rw-rr rwx rwxr-xr-x rwxxx rw-rw-rw-	Seul le propriétaire a la permission de lire et d'écrire mais le groupe et les autres ne peuvent que lire. Seul le propriétaire a le droit de lire, d'écrire et d'exécuter le fichier. Le propriétaire a le droit de lire, d'écrire et d'exécuter, le groupe peut lire et exécuter et les autres ne peuvent que exécuter.

 $droits\_d\_acces\_sur\_les\_fichiers\_ou\_repertoires.txt \cdot Dernière\ modification:\ 2011/11/25\ 15:40\ (modification\ externe)$ 

2 sur 2 05/02/2013 13:04