SYSTÈMES ET RÉSEAUX

Aix*Marseille université

Licence MIAGE

Configuration et gestion d'un serveur

Labo 7 : Gestion des droits

Objectifs :

Sécuriser son système Linux en maîtrisant au mieux les droits d'accès aux différents nœuds.
Connaître les commandes système de gestion des droits.

Plan :

Ressources :

pages de manuel Internet : man page of
tout sur .htaccess

Pour rappel, on appelle nœud tout objet défini dans le système de fichier, qu'il s'agisse de fichier ou dossier.

1. Les trois niveaux de droits.

Trois niveaux de droits d'accès sont définis pour chaque nœud :
- le compte propriétaire du nœud,
- le groupe propriétaire du nœud,
- tous les autres utilisateurs.

Il est donc possible de définir les trois droits pour chacun de ces niveaux, pour chaque nœud.
Il est important de bien comprendre et gérer les droits pour éviter les failles de sécurités.

En affichant les informations détaillées sur le contenu d'un dossier, il est possible d voir apparaître les trois niveaux de droits :

```
$ ls -l
```

L'option `-l` permet d'obtenir plus de détails sur les nœuds affichés.

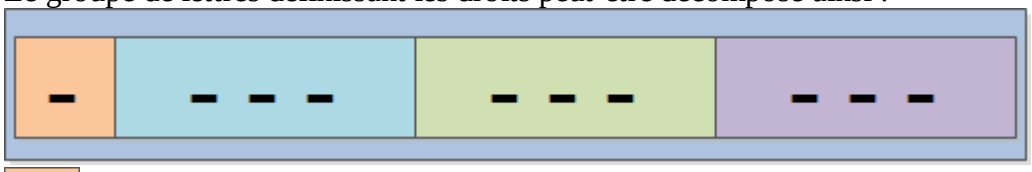
On obtient quelque chose qui ressemble à cela (en dehors des noms des nœuds) :

```
drwxr-xr-x 2 jack   jack   4096 févr.  7 22:38 jack
drwxr-xr-x 2 julien julien 4096 févr.  7 23:31 julien
drwxr-xr-x 3 paul   paul   4096 févr.  7 23:07 paul
drwxr-xr-x 2 pierre pierre 4096 févr.  7 22:38 pierre
```

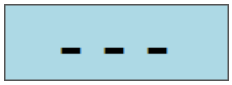
Les champs obtenus par cette commande sont les suivants :

* nombre de sous-noeuds

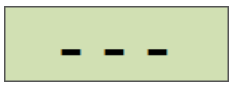
Le groupe de lettres définissant les droits peut-être décomposé ainsi :



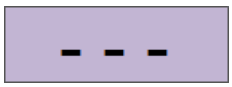
le nœud est-il un dossier (valeur d) ou un fichier (valeur -)



droits associés au propriétaire du nœud.



droits associés au groupe propriétaire du nœud.

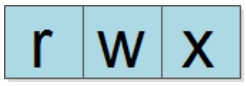


droits associés aux autres utilisateurs.

Les droits associés à chaque niveau sont détaillés dans le paragraphe 2.

2. Les trois droits.

Chaque noeud possède trois droits, pour chacun des trois niveaux expliqués précédemment :



read : droit de lecture du contenu du nœud.

write : droit d'écriture/modification du contenu du nœud.

eXecute : droit de lister le contenu du dossier ou d'exécuter le programme.

3. Changer les droits.

La commande permettant de modifier les droits est la suivante.
Elle s'exécute dans la limite des droits : vous devez être le propriétaire du nœud ou avoir les super pouvoirs pour changer les droits.

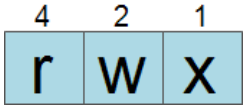
```
$ chmod [-R] <droits> <noeud>
```

L'option `-R` permet d'appliquer les droits de façon récursive, c'est-à-dire également aux nœuds inclus dans celui indiqué.

`<droits>` représente une expression des droits, de façon calculée ou lettrées, telle que détaillée ci-après.

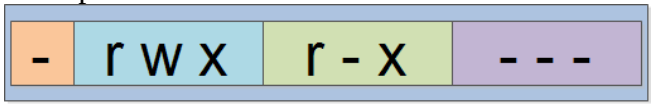
3.1. Les droits calculés.

Une valeur est associée à chacun des trois droits :



Il suffit alors de calculer le total des droits désirés.
Il faut déterminer cette valeur pour chacun des trois niveaux de droits.

Exemple :

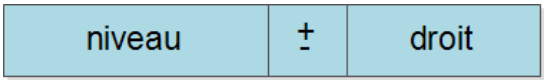


donne comme droits calculs : 4+2+1 4+1 0, soit 750

d'où :
`$ chmod [-r] 750 <noeud>`

3.2. Les droits lettrés.

Il est également possible d'ajouter ou supprimer un seul droit, à un niveau ou à l'ensemble.
La modification de droits sera alors exprimée ainsi :



niveau	permet d'identifier le niveau de droit sur lequel appliquer le droit : `u` = user, propriétaire du nœud. `g` = group, groupe propriétaire du nœud `o` = other, tous les autres utilisateurs du système `a` = all, tout le monde
±	`+` permet d'ajouter un droit, `-` permet de supprimer un droit.
droit	`r` pour le droit de lecture `w` pour le droit d'écriture `x` pour le droit de listage des dossier ou d'exécution des programmes.

Exemples :

`$ chmod a+r /home/commun/partiel2.pdf`
donne à tout le monde le droit de lire le fichier partiel2.pdf

`$ chmod o-r /home/commun/correctionPartiel2.pdf`
retire au autres utilisateurs (non propriétaires, non groupe propriétaire) le droit de lire le fichier.

`$ chmod a+x ~/sauvAutoBD.sh`
ajouter le droit d'exécution sur ce script de sauvegarde de base de données en bash.

4. Les propriétaires d'un nœud.

Le propriétaire et le groupe propriétaire d'un nœud peuvent être modifiés, si vous êtes déjà le propriétaire ou si vous avez les super-pouvoirs.

Pour changer les propriétaires d'un nœud, il faut utiliser la commande :

```
$ chown [-R] <login>[:<nomGroupe>] <noeud>
```

L'option `-R` permet d'appliquer les droits de façon récursive, c'est-à-dire également aux nœuds inclus dans celui indiqué.

exemples :

`$ sudo chown -R julien:miw2019 /home/paul`
julien devient propriétaire et *miw2019* groupe propriétaire du dossier personnel de Paul (?).

`$ sudo chown -R root /var/www/html/test`
root devient propriétaire du sous dossier web *test*. Le groupe propriétaire reste inchangé.

`$ sudo chown -R :devweb /var/www/html`
le groupe *devweb* devient groupe propriétaire du dossier web et de tout ce qu'il contient. Les propriétaires des différents nœuds concernés ne sont pas modifiés.

5. Le droit spécial setGId.

On vient de voir qu'un groupe était systématiquement propriétaire d'un nœud.
Mais lorsqu'un utilisateur créé un nœud (fichier ou dossier), dans la limite des droits qui lui sont accordés, le nœud a comme groupe propriétaire le groupe de l'utilisateur . Pour mémoire, chaque utilisateur possède un groupe à son nom.

Cela peut contrarier les droits définis, notamment sur un serveur Web.

Le droit spécial setGId, lorsqu'il est positionné sur un dossier, assure que tout élément créé dans le dossier aura le groupe propriétaire du dossier. C'est l'héritage de groupe.
Pour affecter ce droit spécial, il faut précéder le triplet de droits du chiffre 2 ;
par exemple : `chmod 2750 dossierExamen`.

Mise en œuvre pour le dossier web :

julien est propriétaire du dossier web, le groupe www-data le groupe propriétaire :
```
$ sudo chown -R julien:www-data /var/www/
```

affecter les droits au dossier web
```
$ sudo chmod -R 2750 /var/www
```

Ici, apache (www-data) aura toujours le droit de lecture sur le répertoire web.

Toute la complexité des droits sur le serveur web réside dans le droit d'écriture donné à apache, via son utilisateur www-data ou son groupe www-data.
Le droit d'écriture est une faille de sécurité. Mais il faut le mettre au moins pour le répertoire de upload.

Dans ce cas, une injection html sera imparable, à moins de bien profiler le fichier .htaccess.