

R1.04 - Systèmes - TP 10

Etape 3 : Droits Unix

Vérifications et Conclusions

Introduction

Cette partie fait suite à ce qu'on vous a demandé d'observer dans le document **Etape 1 : Droits Unix - Expérimentations**.

Reprenez vos notes et notamment les grilles que vous avez remplies à cette **Étape 1**.

Analyse des résultats

La seconde phase du travail consiste à vérifier que les protections sont bien appliquées par le système Linux. On va voir s'il y a correspondance entre les actions qu'on a pu faire et ce qui est réellement défini dans les droits.

Remplir les trois premières colonnes du tableau suivant en recopiant une partie de ce qu'affiche la commande.

Ce qu'affiche la commande : <code>ls -l f*</code>					
Nom	Droits ¹	Propriétaire ²	Groupe	UGO ³	Conclusion
f1					
f2					
f3					
f4					
f5					

¹ Le détail des 3 blocs de droits

² Qui est propriétaire et groupe propriétaire ?

³ UGO : quel bloc vous concerne ?

Ce qu'affiche la commande : ls -ld d*					
Nom	Droits	Propriétaire	Groupe	UGO	Conclusion
d1					
d2					
d3					
d4					
d5					

Relisez la partie de cours sur les droits et protections des fichiers.

Souvenez-vous que tout utilisateur sur Linux possède un nom de compte et un groupe, également un mot de passe, un répertoire d'origine, etc.

La commande **groups** affiche le (ou les groupes) au(x)quel(s) vous appartenez ; c'est l'administrateur qui vous a placé dans ces groupes lors de la création de votre compte.

La commande **id** peut aussi servir à la place de **groups**.

A l'aide de la commande **groups** (ou **id**), notez le nom du groupe auquel vous appartenez.

Analysons maintenant les résultats du tableau.

D'après le propriétaire et le groupe de chaque ressource (fichier ou dossier) :

- Déduisez dans quelle catégorie **U**, **G** ou **O**, vous vous trouvez par rapport à cette ressource.
- Ecrivez **U**, **G** ou **O** dans la colonne **UGO**,
- Entourez les droits que cette catégorie possède pour cette ressource.

Pour finir, pour chaque ressource (fichier ou dossier) :

- Relisez les observations (**oui/non**) que vous avez notées dans les tableaux du paragraphe **Manipulations et observations**,
- Observez les droits que vous avez entourés dans le tableau précédent,
- Concluez : est-ce que l'observation coïncide bien avec les droits ? Si oui, écrivez **OK** dans la case **Conclusion**, sinon, réfléchissez encore avant d'écrire **NOK** dans la case conclusion.

Voyez-vous des "anomalies" ?

Avez-vous compris complètement comment sont gérées les protections ?

Manipulations en solo

Revenez dans votre compte, (sans doute **systeme/td10**). Créez un dossier appelé **dossier**, descendez dedans et créez-y un fichier appelé **fichier**. Puis faites les tests suivants. Répondez aux questions, notez vos observations et vos conclusions.

- 1) Retirez tous les droits sur **fichier** :

```
chmod u-rwx fichier
```

et retirez seulement **W** sur **dossier** :

```
chmod u-w .
```

ou

```
chmod u=rx .
```

 (ce qui laisse uniquement **R** et **X** sur **dossier**)

tentez d'afficher **fichier** à l'écran, tentez de le renommer, tentez de le supprimer (recréez-le s'il est supprimé). Quels sont les droits qui sont sollicités dans chaque cas ?

- 2) Rajoutez tous les droits sur **fichier** :

```
chmod u=rwx fichier
```

mais toujours sans **W** sur **dossier**, vérifiez que vous pouvez l'afficher. Tentez de le renommer, tentez de le supprimer, quels sont les droits nécessaires et qui manquent pour pouvoir le faire ? Rajoutez le droit **W** sur **dossier** et tentez de renommer **fichier** puis de le supprimer (recréez-le s'il disparaît).

- 3) Vérifiez qu'il y a les droits **RWX** sur **dossier**. Enlevez le droit **W** sur **fichier** puis tentez de faire :

```
echo suite >> fichier
```

puis

```
echo vide > fichier
```

qu'est-ce que c'est censé faire et que se passe-t-il? Essayez :

```
echo truc > autre
```

puis enlevez le droit **W** sur le répertoire courant puis faites :

```
echo trac >> autre
```

Est-ce normal ? Remettez **W** sur **dossier**.

- 4) Enlevez le droit **X** sur le répertoire courant puis tentez d'afficher **fichier**, tentez de lister le dossier courant. Remettez le droit **X** sur le répertoire (vous devrez remonter au dessus car vous n'avez plus le droit de rien faire dans le dossier courant) et retentez les opérations. Que peut-on en conclure ?

- 5) Enlevez seulement le droit **R** sur **fichier** :

```
chmod u-r fichier
```

en laissant **RWX** sur **dossier**, tentez de copier **fichier** :

```
cp fichier copie
```

Tentez de renommer **fichier** :

```
mv fichier chifrier
```

Remettez alors le droit **R** sur **chifrier** et retentez la copie. Conclusion ?

- 6) Enlevez le droit **W** sur le répertoire courant et tentez de copier **fichier** comme précédemment, tentez maintenant de copier **fichier** dans le repertoire parent :

```
cp fichier ..
```

Enfin tentez de renommer **fichier** comme précédemment. Qu'est-ce qui empêche de copier le fichier ?

Manipulations en binôme

L'idée de ces exercices est de tester avec votre voisin (ou binôme) les protections que vous pouvez mettre sur vos fichiers. Pour travailler, placez-vous tous deux dans le répertoire **/FILER/ano*/SYS2017/temp**, c'est un répertoire où vous pouvez créer des fichiers pour ce TP.

Dans ce répertoire **temp**, créez un dossier portant votre nom de compte, on l'appellera **votre_login** par la suite dans ce TP. Évidemment vous remplacerez **votre_login**, dans les exemples ci-après, par le vrai nom du dossier que vous avez créé.

ATTENTION : avant de commencer, en étant dans le répertoire **temp**, vous devez impérativement taper la commande :

```
chmod -s votre_login
```

où **votre_login** est le dossier que vous venez de créer à votre nom ou plus exactement votre nom de login. Nous expliquerons plus tard la raison de cette commande.

Dans le dossier **votre_login**, créez deux fichiers, l'un appelé **tintin**, l'autre **milou**. Le binôme fait pareil de son côté.

Dessinez une partie de l'arborescence depuis le dossier **SYS2017** : vous indiquerez le dossier **temp**, celui que vous avez créé à votre nom, celui du binôme ainsi que le contenu de ces 2 derniers.

Les manipulations suivantes se font en modifiant les droits sur le répertoire **votre_login** et sur les deux fichiers. Commencez par lister les droits qui sont en place chez vous et chez le binôme (analysez l'affichage afin de déterminer dans quelle catégorie **UGO** sont les utilisateurs concernés).

- 1) Modifiez et testez les droits pour permettre au binôme de lister votre répertoire et d'afficher vos fichiers **tintin** et **milou** mais pour empêcher qu'il puisse modifier quoi que ce soit.
- 2) Modifiez et testez les droits pour que le binôme puisse toujours afficher le contenu de **tintin** mais pas celui de **milou**.
- 3) Idem que la précédente mais en plus, le binôme ne peut plus lister votre répertoire (seulement afficher **tintin** en connaissant son nom). Amusez-vous à changer le nom de **tintin**, le binôme peut-il l'afficher sans connaître son nom ?

- 4) Faites en sorte que le binôme puisse éditer **milou** mais pas **tintin**.
- 5) Créez un fichier appelé **haddock** chez vous, tandis que le binôme crée **tournesol**. Faites en sorte de pouvoir faire une copie de l'un vers l'autre (son **tournesol** copié chez vous tandis que le voisin vient copier votre **haddock**).
- 6) Même question, mais avec déplacement des fichiers au lieu d'une copie pour réaliser un échange. Vérifiez qui est propriétaire des fichiers que vous avez déplacés. Quel droit faut-il enlever pour empêcher ce déplacement? Vérifiez effectivement que ça marche.
- 7) Faites en sorte que le binôme puisse renommer **tintin** (avec un nom quelconque).
- 8) Peut-on empêcher de supprimer **tintin** tout en autorisant la suppression de **milou**. Qu'en pensez-vous ? Proposez une solution : par exemple, en créant des sous-répertoires ; quoi mettre dans chacun d'eux ? Quels droits assigner à chacune des ressources (dossier ou fichier) ?
- 9) Faites en sorte que le binôme puisse créer et éditer un nouveau fichier, par exemple **dupontd**.

Attention à bien vérifier que les protections mises en place jouent pleinement le rôle demandé. Ne vous contentez pas d'approximations.

Quand vous avez tout fini, effacez les répertoires et leur contenu (commande : **rm -r votre_login**).