TD3: Droits d'accès aux fichiers

Les catégories d'utilisateurs

Tout fichier du système appartient à la fois à **un seul utilisateur** (son "propriétaire") et à **un seul groupe**.

Pour chaque fichier il y a **3 catégories d'utilisateurs** :

- **u**, l'utilisateur normal, son propriétaire, souvent celui qui l'a créé.
- **g**, son groupe, ensemble d'utilisateurs ayant parfois des "permissions" particulières.
- **o**, tous les autres (others) .

L'utilisateur propriétaire et le groupe propriétaire du fichier peuvent être indépendants.

Un utilisateur peut être inscrit dans plusieurs groupes

Droits d'accès aux fichiers

Pour chaque catégorie d'utilisateurs, il y a trois types d'accès :

- **r** lecture (read)
- **w** écriture (write) (pour les répertoires: droit de créer et d'effacer des fichiers si **x** ou **t** est positionné)
- **x** exécution (pour les répertoires : droit d'y entrer)

Les droits sont consultables par la commande : *ls –l*
Par exemple :
ls –l /home/toto/.profile
retourne:
-rw-r--r-- 1 toto toto 675 sept 17 2012 .profile

On trouve de gauche à droite

le 1er caractère indique la nature du fichier : "**-**" fichier normal, "**d**" un fichier répertoire, "**l**" un lien.
les droits correspondants aux 3 catégories d'utilisateurs du fichier : **rwx|rwx|rwx**
u g o
nombre de liens sur le fichier: 1 signifie que le fichier n'a aucun lien qui pointe vers lui,
le nom du propriétaire du fichier
le nom du groupe propriétaire
la taille
la date de dernière modification
le nom complet du fichier

stat permet d'obtenir plus d'informations sur un fichier.
Exemple : *stat /etc/passwd*

chmod permet de changer les droits
chgrp permet de changer le groupe propriétaire d'un fichier
chown permet de changer le propriétaire d'un fichier

Exercice 1:

1) Examiner les droits et propriétaires :

- des répertoires qui se trouvent dans */home*
  Réponse :.....
- des fichiers qui se trouvent dans */home/lea*
  Réponse :.....
- des fichiers */etc/passwd* et */etc/shadow*
  Réponse :.....
- du fichier */usr/bin/password*
  Réponse :.....
- du répertoire */tmp*
  Réponse :.....

Exercice 2:

Créer un utilisateur *lulu* avec le mot de passe *lulu* et faisant parti du groupe principal *lulu* et du groupe secondaire *étudiants*

Se connecter sous le nom de *lulu* dans un autre terminal (Alt Ctrl F2…) et :

- créer les répertoires : *perso etudiants et public*
- créer un fichier de test dans chacun de ces répertoires
- examiner les droits et le groupe propriétaire de ces répertoires et fichiers

lulu souhaite que :

- les membres du groupe étudiants aient un accès complet aux fichiers de son répertoire *étudiants*.
- tous les utilisateurs puissent lire et exécuter les fichiers de son répertoire public
- personne n'accède à son répertoire perso (excepté root et lui-même bien sûr)

Que doit faire *lulu* ?

- l'administrateur doit-il intervenir ?
  Réponse :.....
- Vérifier le bon fonctionnement en se connectant avec le nom d'un utilisateur faisant partie du groupe *étudiants* puis d'un autre utilisateur ne faisant pas parti du groupe *étudiants*

Faire valider par l'enseignant lorsque ça fonctionne.

Notation octale des droits d'accès à un fichier

Il existe une autre façon d'indiquer les droits d'accès à un fichier : la numération octale
Voici la table de correspondance entre les 8 chiffres en numérotation octale (base 8) et les 8 valeurs des droits.
Par convention le 1 indique que le droit est accordé et le 0 que le droit est refusé.

Binaire	Droit	Octal
000	---	0
001	--x	1
010	-w-	2
011	-wx	3
100	r--	4
101	r-x	5
110	rw-	6
111	rwx	7

Exemples :
chmod 754 /toto/fichier_test
7 5 4
111 011 100
rwx r-x r-- toto peut tout faire sur le fichier, le groupe peut lire et exécuter, les autres ne peuvent que lire (à condition que l'accès au répertoire *toto* soit possible voir les droits sur le répertoire /home/toto)

Droits par défaut lors de la création « *umask* »

Lors de la création d'un fichier ou d'un répertoire :
- le propriétaire est l'utilisateur qui l'a créé
- le groupe propriétaire est le groupe primaire de ce même utilisateur
- les droits accordés par défaut sont au plus 666 (-rw-rw-rw-) pour un fichier et au plus 777 (-rwxrwxrwx) sur un répertoire.

On peut restreindre les droits accordés par défaut avec la commande *umask*.
umask indique les droits qui ne sont pas accordés
Exemple : *umask 027* 000 010 111 interdit l'écriture au groupe et interdit tout aux autres utilisateurs

Exercice :

- *umask* affiche le masque de l'utilisateur actif.
- Quelles sont les valeurs des masques par défaut de *root* et des autres *utilisateurs* ?
- Changer *umask* de l'utilisateur *toto* pour interdire au groupe et aux autres utilisateurs tous les droits sur les nouveaux répertoires et fichiers crées par *toto*, vérifier.
Attention, le changement ne s'applique qu'à la présente session. On peut le rendre permanent en ajoutant la ligne *umask 077* dans le fichier de configuration *.bash_profile* de l'utilisateur.Utiliser l'éditeur *vi* pour faire la modification.

Les droits étendus

Le droit SUID
-Sa présence permet à un fichier exécutable de s'exécuter sous l'identité et donc les droits de son propriétaire, à la place des droits de l'utilisateur actuel qui l'exécute.
-Ce droit est noté s et se positionne à la place du x du propriétaire (mais sans écraser le droit x) Sa valeur octale est 4000
Le droit SGID
-Pour un fichier exécutable, il fonctionne de la même façon que le SUID, mais transposé aux membres du groupe.
-Positionné sur un répertoire, ce droit modifie le groupe propriétaire d'un fichier créé dans ce répertoire, ce ne sera plus le groupe primaire du propriétaire qui l'a créé (règle habituelle), mais à la place, le groupe propriétaire du répertoire lui-même.
-Notation s, mis à la place du x du groupe, valeur octale 2000
Le "sticky bit"
- Ce droit spécial, traduit en "bit collant", a un rôle important sur les répertoires.
- Il réglemente le droit w sur le répertoire, en interdisant à un utilisateur quelconque de supprimer un fichier dont il n'est pas le propriétaire
- Ce droit noté t , occupe x sur la catégorie other de ce répertoire, mais bien entendu il ne supprime pas le droit d'accès x (s'il est accordé).

- Si ce droit x n'est pas accordé à la catégorie other, la lettre T qui apparaîtra à la place de t.
- Sa valeur octale associée vaut 1000.

Exercice :

- Comparer et justifier les droits du fichier exécutable */usr/bin/passwd*, qui permet de (re)définir un mot de passe et le comparer à ceux du fichier */etc/shadow* qui contient les mots de passe cryptés.
- Pourquoi le sticky bit est-il présent sur le répertoire */tmp*

Exercice 4: Sécuriser le partage d'un répertoire.

-Créer un répertoire */home/rep_lic_pro* partagé par tous les membres du groupe *licencepro* .
- Pourquoi cette tâche relève-t-elle des prérogatives de *root* ?
- Modifier les droits sur le répertoire pour que seuls les membres du groupe *licencepro* puissent y écrire et s'y déplacer.
- Créer les utilisateurs *lea* et *luc* membre du groupe et *joe* extérieur au groupe
- En tant que *luc* vous créez un fichier accessible en **lecture seule** dans le répertoire *rep_lic_pro*.
- Vérifier le bon accès en lecture pour *lea*, membres du groupe
- Vérifier que *joe* ne peut pas accéder aux fichiers du groupe
- *léa* tente de supprimer ce fichier ou de le renommer, y parvient-elle ? Essayez !
- **N'est-ce pas inquiétant ?** Expliquez pourquoi cela est possible.
- Comment "*root*" va-t-il régler le problème ?
- Vérifiez que le problème est réglé et protège le propriétaire des tentatives de suppression ou de changement de nom de ses fichiers par les autres membres du groupe.