EC2LT
ECOLE CENTRALE DES LOGICIELS LIBRES
ET DE TELECOMMUNICATIONS

Deuxième ACTIVITE

Gestion des Droits des fichiers

Consignes :

Lisez attentivement la première partie avant d'attaquer les exercices.

Chacun doit rendre un rapport qui est composé d'une introduction qui décrit le rôle d'administrateur système. Le corps du rapport sera les captures des résultats des commandes, de vos remarques et vos constats. Vous terminerez le rapport avec une conclusion.

Aly TIRERA, ingénieur Télécoms et Réseaux, Certifié Linux LPIC-1 & LPIC-2

1. Objectif de l'activité

Un administrateur systèmes et réseaux doit être capable d'organiser les utilisateurs sous forme de groupe et leur attribuer les permissions sur des fichiers.

A l'issue de cette activité l'apprenant sera capable de :

- Savoir les différents types d'utilisateurs (**utilisateur propriétaire**, **groupe propriétaire** et les **autres**) ;
- Savoir les différents droits qui existent : de **lecture**, d'**écriture** et d'**exécution** ou d'**accès** ;
- Connaitre les droits spéciaux qui sont : **set-uid**, **set-gid** et **stick bit**
- Gérer (ajouter/retirer) les droits sur des fichiers en mode **caractère** et mode **décimale** ;

Linux est un système multi-utilisateur et chacun de ces utilisateurs peut se connecter à n'importe quel moment pour travailler dans son espace de travail.

Linux étant multi-utilisateurs il est important de pouvoir contrôler leurs droits sur les différents fichiers du système.

Le système Linux ne fait pas de différence entre un fichier et un répertoire ils sont tous (fichiers, répertoires) considérés comme un **fichier.**

Le terme **fichier** désigne à la fois un fichier ordinaire et les répertoires

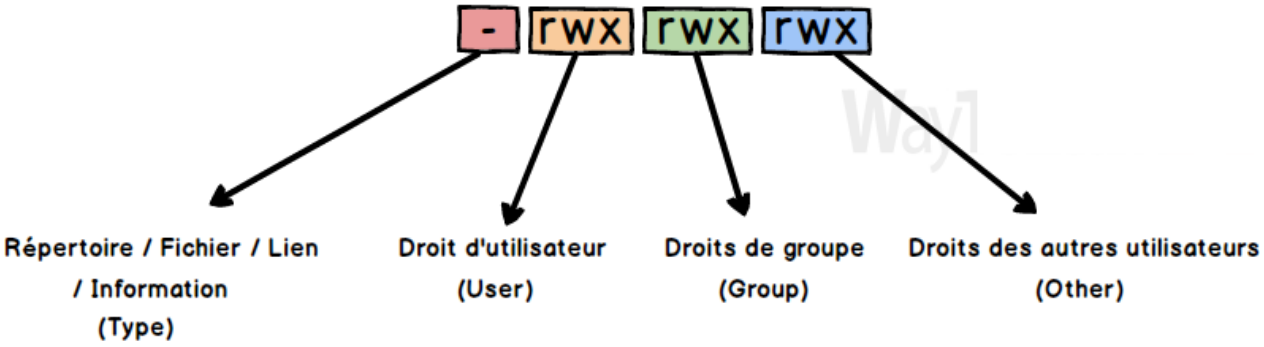
Les types utilisateurs Unix sont

- Les droits du propriétaire du fichier (**u**ser) ;
- Les droits des utilisateurs appartenant au même groupe que le propriétaire : **g**roupe
- Les droits des autres ceux qui sont ni propriétaire et ni membre du groupe propriétaire. Ils sont représentés par la lettre (**o**thers).

Les droits Unix sont :

- droit de Lecture
- droit d'Ecriture
- droit d'exécution : on parle de droit d'exécution s'il s'agit d'un fichier et droit d'accès ou de traverser s'il s'agit d'un répertoire

La figure ci-dessous vous montre comment les droits sont représentés sur un fichier :

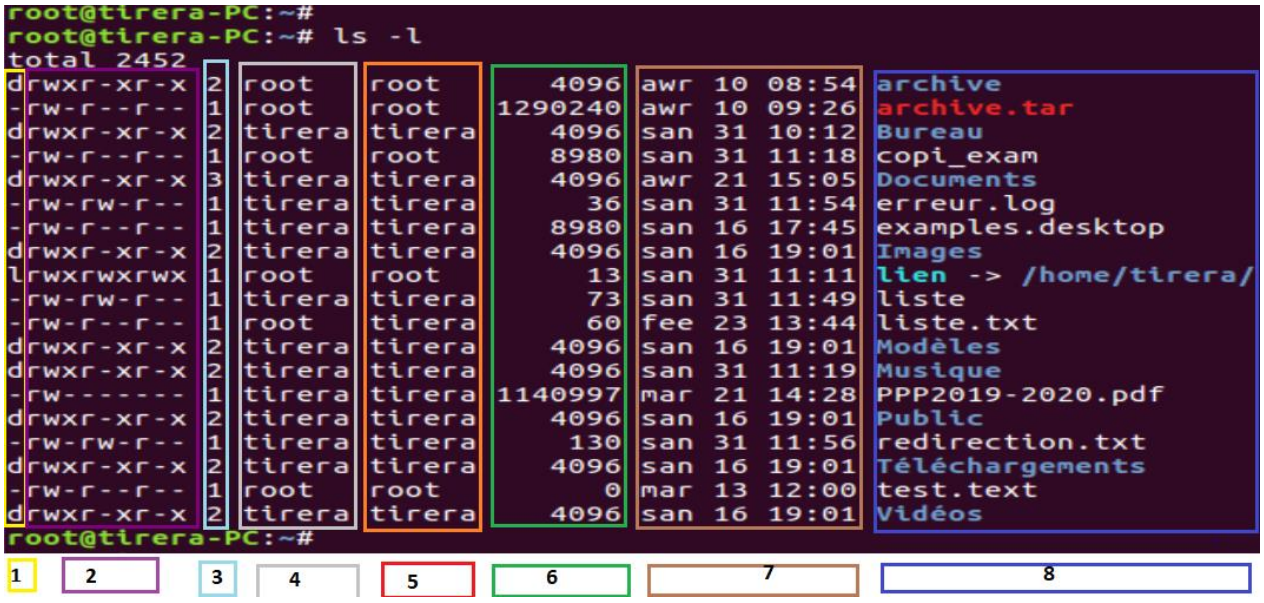


1. La case qui est colorée en **rouge** peut prendre les valeurs suivantes :
   - **-** (tiret) : cela montre que le fichier est un **fichier ordinaire**
   - **d** : cela montre que le fichier est un répertoire
   - **l :** cela montre que le fichier est un **lien** (Linux) ou un **raccourci** (Windows)
2. La case colorée en **orange** représente les droits ou permissions de l'utilisateur propriétaire
3. La case colorée en **vert** représente les droits ou permissions des utilisateurs membre du groupe propriétaire
4. La case colorée en **bleu** représente les droits ou permissions des autres utilisateurs

Voyons un exemple comme le montre la figure ci-dessous :

```
root@tirera-PC:~#
root@tirera-PC:~# ls -l
total 2452
drwxr-xr-x 2 root   root       4096 awr 10 08:54 archive
-rw-r--r-- 1 root   root    1290240 awr 10 09:26 archive.tar
drwxr-xr-x 2 tirera tirera     4096 san 31 10:12 Bureau
-rw-r--r-- 1 root   root       8980 san 31 11:18 copi_exam
drwxr-xr-x 3 tirera tirera     4096 awr 21 15:05 Documents
-rw-rw-r-- 1 tirera tirera       36 san 31 11:54 erreur.log
-rw-r--r-- 1 tirera tirera     8980 san 16 17:45 examples.desktop
drwxr-xr-x 2 tirera tirera     4096 san 16 19:01 Images
lrwxrwxrwx 1 root   root         13 san 31 11:11 lien -> /home/tirera/
-rw-rw-r-- 1 tirera tirera       73 san 31 11:49 liste
-rw-r--r-- 1 root   tirera       60 fee 23 13:44 liste.txt
drwxr-xr-x 2 tirera tirera     4096 san 16 19:01 Modèles
drwxr-xr-x 2 tirera tirera     4096 san 31 11:19 Musique
-rw------- 1 tirera tirera  1140997 mar 21 14:28 PPP2019-2020.pdf
drwxr-xr-x 2 tirera tirera     4096 san 16 19:01 Public
-rw-rw-r-- 1 tirera tirera      130 san 31 11:56 redirection.txt
drwxr-xr-x 2 tirera tirera     4096 san 16 19:01 Téléchargements
-rw-r--r-- 1 root   root          0 mar 13 12:00 test.text
drwxr-xr-x 2 tirera tirera     4096 san 16 19:01 Vidéos
root@tirera-PC:~#
```

Description de la figure ci-dessous :



1	Colonne 1 nous donne le type du fichier (fichier ordinaire, répertoire, lien)
2	Colonne 2 nous donne les droits positionnés sur un fichier des différents types utilisateurs
3	Colonne 3 nous donne le nombre de lien
4	Colonne 4 nous donne le propriétaire du fichier
5	Colonne 5 nous donne le le groupe propriétaire du fichier
6	Colonne 6 nous donne la taille du fichier (fichier ordinaire, répertoire, lien)
7	Colonne 7 nous donne la date et l'heure de la création du fichier (fichier, répertoire,lien)
8	Colonne 8 nous donne le nom du fichier (fichier ordinaire, répertoire, lien)

Les modes d'attribution des droits :

Il existe deux pour attribuer des droits ou permissions aux différents types d'utilisateurs :

- **Le mode caractère :**
  - Le droit de **lecture (read)** est représenté par la lettre **r (lecture = r)**
  - Le droit d'**écriture** (**write**) est représenté par la lettre **w (écriture = w)**
  - Le droit d'**exécution (execute)** est représenté par la lettre **x (exécution =x)**
- **Le mode décimal :**
  - Le droit de **lecture** est représenté par la lettre **r (lecture = 4)**
  - Le droit d'**écriture** est représenté par la lettre **w (écriture = 2)**
  - Le droit d'**exécution** est représenté par la lettre **x (exécution = 1)s**

La commande **chmod** est utilisée pour exprimer les droits sur des fichiers avec la syntaxe suivante :

chmod [u g o a] [+ - =] [droits] nom_du_fichier

Opérateurs : + (ajouter), - (enlever), = (attribuer seulement ces droits)

Exemple 1 : Comment fixer de nouveaux droits sans tenir compte des anciens droits comme suit :

```
root@tirera-PC:~#
root@tirera-PC:~# touch essai.text
root@tirera-PC:~# chmod u=rwx,g=rw,o=r essai.text
root@tirera-PC:~#
```

Exemple 2 : Comment ajouter ou retirer ou enlever des droits à un utilisateur comme suit :

```
root@tirera-PC:~#
root@tirera-PC:~# ls -l essai.text
-rwxrw-r-- 1 root root 0 awr 21 16:33 essai.text
root@tirera-PC:~#
root@tirera-PC:~# chmod u-x,g-w,o+w essai.text
root@tirera-PC:~#
root@tirera-PC:~# ls -l essai.text
-rw-r--rw- 1 root root 0 awr 21 16:33 essai.text
root@tirera-PC:~#
```

Exemple 3 : Comment fixer les droits en mode octal ou décimal comme suit :

```
root@tirera-PC:~#
root@tirera-PC:~# chmod 764 essai.text
root@tirera-PC:~# ls -l essai.text
-rwxrw-r-- 1 root root 0 awr 21 16:33 essai.text
root@tirera-PC:~#
```

Sous Linux, les fichiers nouvellement créés ont les droits : **-rw-r--r--** ce qui vaut à 644 en mode décimal. On constate que lors de la création du fichier il y a des droits que le système retire

aux différents types d'utilisateurs (user, group, other) appelé **valeur de masque de création de fichier par defaut**.

Cette valeur s'obtient en exécutant la commande suivante **umask** et la valeur **022.**

NB : La valeur de masque de création de fichier par défaut s'applique aussi aux répertoires

Pour constater cela créer un répertoire avec **esnr** par la commande **mkdir esnr** et remarquer que ses droits sont : **rwxr-xr-x**

Exercice 1 :

Q1. Créer un utilisateur nommé banta
Q2. Intégrer banta le groupe sudo
Q3. Connectez-vous avec le compte banta
Q4. Créer un répertoire nommé **droits** dans votre dossier personnel
Q5. Déplacez vous dans le dossier droits et créez un fichier appelé **ec2lt.text**
Q6. Exécuter la commande **ls -l ec2lt.text** et relever toutes les informations concernant ce fichier
Q7. Quelles sont les droits des différents utilisateurs (user, group, other) sur le fichier **ec2lt.text?**
Q8. Utiliser la commande chmod pour donner à l'utilisateur propriétaire tous les droits et ajouter le droit d'écriture au groupe propriétaire
Q9. Quels sont les droits des autres sur le fichier ?
Q10. Créer un nouvel utilisateur nommé raoul
Q11. Créer un nouvel utilisateur nommé papa et intégrer dans le groupe **banta**
Q12. Connectez-vous avec le compte de papa avec la commande : **su - papa**
Q13. Essayer d'écrire dans le fichier **ec2lt.text** avec la commande : **nano ec2lt.text**. papa peut-il écrire dans le fichier ?
Q14. Connectez-vous avec le compte de raoul avec la commande : **su – raoul**
Q15. Essayer d'écrire dans le fichier ec2lt.text avec la commande : nano ec2lt.text. raoul peut-il écrire dans le fichier ?
Q16. Dans quelle catégorie d'utilisateur mettez-vous l'utilisateur raoul ?

Pour permettre à raoul de pouvoir écrire dans **ec2lt.text on peut procéder comme suit :**

1. On intégre raoul au groupe banta comme membre du groupe dans ce cas il bénéficie des droits du groupe et il pourra modifier le contenu du fichier.
2. On peut donner aux autres le droit d'écriture sur le fichier ec2lt.text

Selon vous quelle est la meilleure solution entre les options (1 et 2) justifiez votre réponse ?

Q17. Retire le droit d'exécution de l'utilisateur propriétaire et ajouter aux autres le droit d'écriture
Q18. Utiliser le mode octal pour donner à l'utilisateur propriétaire le droit de lecture et d'écriture, aux membres du groupe le droit de lecture et les autres n'ont aucun droit sur ce fichier
Q19. Afficher la valeur de masque de création de fichier par défaut avec la commande : **umask**
Q20. Interpréter la valeur **umask** que vous avez obtenu ?

Q21. Changer la valeur de umask comme suit : **umask 222**

Q22. Créer dans votre répertoire personnel le test.txt ensuite donner les droits de ce dernier

Q23. Avec cette valeur de umask (222) peut-on lire le fichier et modifier son contenu

Q24. Retirer le droit de lecteur à tous les utilisateurs et donner à tous les utilisateurs le droit d'écriture

Q25. Est-ce que en ayant uniquement le droit d'écriture sur un fichier on peut lire et modifier son contenu ?

Q26. Est-ce que en ayant le droit d'écriture sur un fichier nous donne aussi indirectement le droit de lecture ?

Q27. Redémarrer la machine

Q28. Afficher la valeur de umask avec la commande suivante : **umask** et que constatez-vous ?

Q29. Onnectez-vous avec le compte de banta avec la commande : **su - banta**

Q30. Créer un répertoire sur votre Bureau avec la commande suivante :
mkdir /home/banta/Bureau/covid19

Q31. Quels les droits du répertoire covid19 comme suit : **ls -ld /home/banta/Bureau/covid19**

Q32. Retirez le droit d'accès au répertoire covid19 du groupe propriétaire et aux autres avec la commande suivante : **sudo chmod g-x,o-x /home/banta/Bureau/covid19**

Q33. Quels sont les utilisateurs qui sont membres du groupe banta comme suit : **grep banta /etc/group**

Q34. Donner les nouveaux droits du répertoire ld /home/banta/Bureau/covid19 ?

Q35. Est-ce que selon les membres du groupe ou bien et autres peuvent accéder au répertoire covid19 ? justifiez votre réponse

Q36. Connectez-vous avec le compte de papa avec la commande suivante : **su – papa**

Q37. Accéder au répertoire covid19 avec la commande **cd /home/banta/Bureau/covid19**, que constatez-vous ?

Q38. Connectez-vous avec le compte de banta avec la commande suivante : su – banta

Q39. Accéder au répertoire covid19 avec la commande **cd /home/banta/Bureau/covid19**, que constatez-vous ?

Q40. Pourquoi l'utilisateur banta a accès au répertoire **/home/banta/Bureau/covid19 ?**

Q41. Créer un fichier dans répertoire covid19 comme suit :
touch /home/banta/Bureau/covid19/confinement.text

Q42. En ayant le droit de lecture et sans le droit d'accès peut-on lister le contenu d'un répertoire ?

1. Pour une preuve connecte toi avec le compte de papa et tente de lister **/home/banta/Bureau/covid19**
2. Ensuit déconnecte toi du compte de papa comme suit : **exit**

Q43. Donner le droit d'écriture au groupe propriétaire avec la commande suivante :
sudo chmod g+w /home/banta/Bureau/covid19

Q44. Tentez de créer un sous répertoire test comme suit : **mkdir /home/banta/Bureau/covid19/test**

Q45. Est-ce que sans le droit d'accès peut-on bénéficier des autres droits sur un répertoire (lecture et écriture) ?

Q46. Donner tous les droits au groupe propriétaire et aux autres sur le sous répertoire test comme suit : sudo chmod go+rwx /home/banta/Bureau/covid19/test

Q47. Après avoir donné tous les droits aux différents utilisateurs, connectez-vous avec le compte de papa avec la commande **su – papa** ensuite tentez d'accéder au sous répertoire test avec la commande suivante : **cd /home/banta/Bureau/covid19/test** Que constatez-vous ?

Q48. Déconnecte-toi du compte de papa avec la commande suivante : **exit**

Q49. Malgré qu'on dispose de tous les droits sur le sous répertoire test il faut obligatoirement disposer le droit de traverser le répertoire parent qui est **covid19** pour accéder au répertoire test donc ajoutons au groupe propriétaire et aux autres le droit de traverser le répertoire parent avec la commande suivante : **sudo chmod go+x /home/banta/Bureau/covid19**

Q50. Reconnectez vous avec le compte de papa et créer un répertoire qui porte votre nom complet comme suit : **mkdir /home/banta/Bureau/covid19/test/prenom_nom**

TP2 : les droits spéciaux (set-UID, set-GID, sticky bit)

1. Le droit set-UID

Linux est multi-utilisateurs. Pour cette raison, tout le monde ne peut pas tout faire, à part l'administrateur système (traditionnellement nommé root), qui a le droit de lire et d'écrire tous les fichiers de tous les répertoires.

Lorsqu'un utilisateur exécute un programme ou une commande, celui-ci se lance avec les droits de cet utilisateur. Mais il arrive que l'on souhaite lancer une commande qui entrainera une action (par exemple : écrire dans un fichier ou seul root a droit) dont seul le super utilisateur a droit de le réaliser. Cela signifie que lorsqu'elle est exécutée, elle l'est avec les droits de son propriétaire, et non avec ceux de l'utilisateur qui le lance.

Par exemple, le programme `passwd`, qui permet à un utilisateur de modifier son mot de passe, est setuid root (c'est à dire qu'il est setuid et qu'il appartient à l'utilisateur root) : il doit pouvoir écrire dans le fichier `/etc/passwd` (ou `/etc/shadow`), dans lequel seul root peut écrire.

Q1. Connectez-vous avec le compte de banta comme suit : **su – banta**

Q2. Créez le fichier suivant avec la commande suivante : **touch banta.txt**

Q3. Donnez le droit de lecture et le droit d'écriture à l'utilisateur propriétaire et le droit de lecture au groupe propriétaire et aux autres avec la commande suivante :
sudo chmod u+rw,go+r /home/banta/banta.txt
noter bien que c'est banta qui est propriétaire du fichier et il est seul qui peut écrire dans ce fichier

Q4. Copiez l'éditeur de texte **nano** avec la commande suivante : **cp /bin/nano monediteur**

Q5. Connectez-vous avec le compte de papa comme suit : **su papa**

Q6. Après avoir connecté avec la compte de papa tenter d'écrire dans le fichier banta.txt comme suit : **./monediteur banta.txt** Que constatez-vous ?

Q7. Déconnectez-vous avec le compte de papa comme suit :

Q8. Papa voulant écrire dans le fichier banta.txt à la question précédente (Q6) a utilisé le droit qu'il possède sur le fichier banta.txt alors que le droit de lecture qu'il a sur ce dernier ne lui permet pas d'écrire dans ce fichier. Il faut que papa puisse lancer la commande avec les droits

de l'utilisateur propriétaire banta. Pour cela il faut ajouter le droit **set-uid** à l'utilisateur propriétaire (banta) avec la commande suivante : **sudo chmod u+s monediteur**

Q9. Quels sont les droits de l'utilisateur propriétaire et le reste des utilisateurs

Q10. Reconnectez-vous avec le compte de papa avec la commande suivante : **su papa**

Q11. Tentez d'écrire dans le fichier banta.txt avec la commande suivante :
./monediteur banta.txt Que constatez-vous ?

2. Le droit set-GID

Problème

Sachant, par défaut, qu'un fichier crée par un utilisateur lui appartient et a pour groupe propriétaire le groupe de l'utilisateur. Comment faire en sorte que les fichiers créés par les d'un projet aient comme groupe propriétaire le groupe du projet ?

Pour cela, on va créer un groupe projet et un répertoire nommé **/rep-projet**, et donner le **/rep-projet** au groupe projet et ajouter le droit **s (set-GID)** au groupe propriétaire du **/rep-projet** et enfin intégrer les utilisateurs banta et papa comme membre du groupe projet :

Q1. Ajouter le groupe projet avec la commande suivante : **sudo addgroup projet**

Q2. Créer le répertoire rep-projet avec la commande suivante **: sudo mkdir /rep-projet**

Q3. Donner le répertoire /rep-projet au groupe projet comme suit : **sudo chgrp projet /rep-projet**

Q4. Ajouter le droit s au groupe propriétaire avec la commande suivante :
sudo chmod g+s /rep-projet

Q5. Donner le droit d'écriture au groupe propriétaire avec la commande suivante **:**
sudo chmod g+w /rep-projet

Q6. Ajouter les utilisateurs banta et papa dans le groupe projet avec la commande suivante :
sudo gpasswd -a banta projet
sudo gpasswd -a papa projet

Q7. Connectez-vous avec l'un des utilisateurs et créer des fichiers ou des répertoires comme suit :
su – papa

Q8. Créer le fichier papa.txt dans le répertoire /rep-projet avec la commande suivante :
cd /rep-projet
touch papa.txt

Q9. Afficher les détails du fichier pour vérifier le groupe propriétaire du fichier comme suit :
ls -l papa.txt Que remarquez-vous ?

3. Le droit sticky bit

Le sticky bit sert à *sécuriser* un fichier se trouvant dans un répertoire où tout le monde a les droits en écriture. Par exemple pour un répertoire que vous partagez avec vos camarades ou tout le monde a le droit d'écriture, il serait gênant qu'un autre utilisateur puisse supprimer un de vos fichiers. Pour y remédier, on positionne le droit sticky bit sur ce répertoire, n'autorisant la suppression d'un fichier uniquement à son propriétaire.

Pour se faire :

Q1. Créer un répertoire /partage avec la commande suivante : **mkdir /partage**
Q2. Donner à tous les utilisateurs le d'écriture sur ce répertoire /partage avec la commande suivante : **sudo chmod go+w /partage**
Q3. Positionner le droit sticky bit sur le répertoire /partage comme suit : **sudo chmod +t /partage**
Q4. Connectez-vous avec le compte de banta et créer un fichier dans le répertoire /partage comme suit :
su – banta
touch /partage/banta.txt
Q5. Déconnectez-vous du compte de banta avec la commande suivante : **exit**
Q6. Connectez-vous avec le compte de papa et ensuite tentez de supprimer le fichier banta.txt comme suit :
su – papa
cd /partage
rm banta.txt
Q7. Que remarquez-vous ?
Q8. Déconnectez-vous du compte de papa pour se connecter avec celui banta comme suit :
Q9. **su - banta**
Q10. Tentez de supprimer le fichier banta.txt avec la commande suivante **: rm /partage/banta.txt**
Q11. Que peut-on conclure ?