



Université Abdelhamid Mehri – Constantine 2

Systèmes d'Exploitation 1

– TP –

Chapitre III : Gestion des utilisateurs & protection des fichiers



| Staff pédagogique | | | |
|-------------------|-------|------------------------|--------------------------------------|
| Nom | Grade | Faculté/Institut | Adresse e-mail |
| Mohamed SANDELI | MCB | Nouvelles Technologies | mohamed.sandeli@univ-constantine2.dz |

| Etudiants concernés | | | |
|------------------------|-------------|-----------|--------------|
| Faculté/Institut | Département | Année | Spécialité |
| Nouvelles Technologies | MI | Licence 2 | Tronc commun |

Objectifs du TP 3

A l'issue de ce TP, vous serez en mesure de :

- Personnaliser la définition de votre compte utilisateur.
- Modifier les droits d'accès aux fichiers et aux répertoires afin d'assurer la confidentialité des données stockées sur les systèmes de fichiers linux.

1. Introduction

- Linux est un système multi-utilisateurs;
- Plusieurs personnes peuvent travailler simultanément sur le même OS;
- Sous Linux il existe un ensemble de règles qui disent qui a le droit de faire quoi.
- Ces droits concernent généralement la lecture, l'écriture et l'exécution d'un fichier.

2. Concepts de comptes utilisateur

1- Les types des comptes utilisateurs

- Les comptes utilisateur ne sont pas tous égaux sur Linux. On distingue trois types:
 - Super-utilisateur (root)
 - Comptes systèmes
 - Comptes ordinaires
- Exécuter en tant que Administrateur
 - ✓ La commande sudo (Substitute User **DO**) permet à un utilisateur d'exécuter des commandes qui ne peuvent être utilisées que par le super-utilisateur.

\$ sudo commande

- ✓ La substitution d'utilisateur par sudo c'est une manière de vous dire et de vous rappeler : Est-ce que vous êtes sûr que vous voulez faire ceci?!

useradd [option] login

adduser [option] login

- Exemple :

sudo useradd tarzan --uid 1010 --home /home/acteur/ --create-home --groups jungle,animaux --gid jungle --shell /bin/bash

- Explication des options :
 - Nom d'utilisateur : tarzan
 - ID de l'utilisateur (UID) : 1010
 - Dossier personnel de l'utilisateur : /home/acteur/
 - Ce dossier personnel est créé par useradd
 - L'utilisateur est ajouté aux deux groupes suivants : jungle et animaux
 - Groupe principal de l'utilisateur : jungle
 - Chemin du shell pour les commandes du terminal : /bin/bash
- Pour terminer, on fait l'*activation du compte* en lui attribuant un mot de passe grâce à la commande passwd.
sudo passwd tarzan

2- Modifier les propriétés d'un compte :

usermod [option] login

- Exemple :

- **usermod -aG toto machin**
Ajoute l'utilisateur machin au groupe toto sans supprimer machin de ses groupes d'origine.
- **usermod -g group1 user1**
Défini pour l'utilisateur user1 le groupe group1 comme groupe primaire

3- Changer de mot de passe utilisateur

passwd login

```
ubuntu@ubuntu-VirtualBox:~$ sudo passwd user1
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
```

4- la suppression d'un utilisateur:

userdel [option] login

Exemple :

- **userdel -r user1**
Supprime l'utilisateur user1 ainsi que son répertoire personnel.
- Les fichiers de user1 qui se trouvent en dehors du répertoire personnel. La commande suivante permet de les trouver et de les supprimer à partir du UID de l'utilisateur

**Find ./ -type f -uid 1002 -print exec rm {} **

3. Concepts de groupes utilisateur

- Un groupe est un ensemble d'utilisateurs qui partagent les mêmes fichiers et répertoires.
- Chaque utilisateur doit faire partie au moins d'un groupe, son *groupe primaire*. Celui-ci est défini au moment de la création du compte, et *par défaut*, l'utilisateur appartient à un nouveau groupe créé, portant son nom.
- Ainsi, dans **/etc/passwd** chaque utilisateur possède un groupe par défaut, précisé par son identifiant **gid** dans ce fichier.
- L'appartenance au groupe primaire n'étant pas exclusive, tout utilisateur peut faire partie de plusieurs autres groupes, appelés ses *groupes secondaires*.
- Les commandes de gestion des Groupes utilisateurs :

Pour lister tous les groupes (primaire et secondaires) d'un utilisateur :

groups stagex

Pour créer un nouveau groupe

groupadd stagiaire

Supprimer un groupe, au hasard .. encore totox.

groupdel totox

(Le groupe est supprimé du fichier **/etc/group**).

La commande **groupmod** permet de modifier un groupe.

groupmod --new-name nouveau-nom ancien-nom

L'option **--new-name**, **gpasswd** ajoute un utilisateur à un groupe.

NB: les fichiers ne changent pas de gid à l'attribution du nouveau numéro de gid. Ils doivent, par conséquent, être changé manuellement.

Les 4 principaux fichiers des comptes:

- **passwd** : comptes utilisateurs
- **shadow** : mots de passe et sécurité
- **group** : les groupes utilisateurs
- **gshadow**

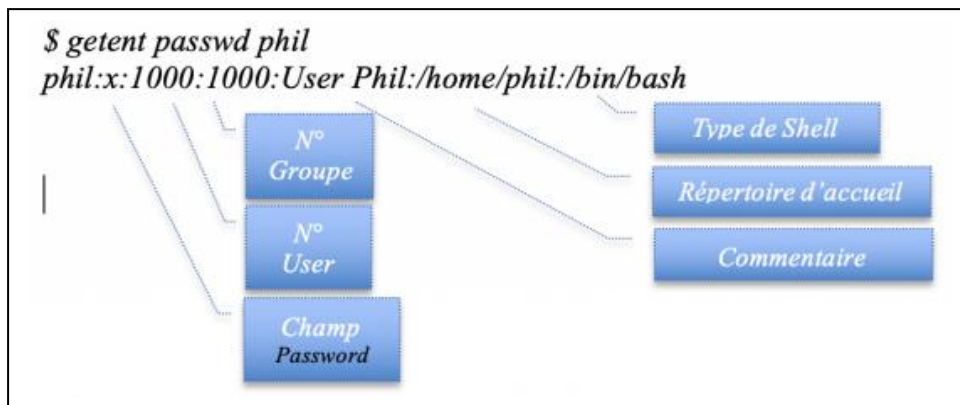
```

atrchoum@localhost:~$ ls -l /etc/passwd /etc/group /etc/shadow /etc/gshadow
-rw-r--r-- 1 root root 1141 fév 25 15:22 /etc/group
-r----- 1 root root 981 fév 25 15:22 /etc/gshadow
-rw-r--r-- 1 root root 2827 fév 25 15:22 /etc/passwd
-rw----- 1 root root 2005 mar 4 10:17 /etc/shadow
atrchoum@localhost ~]$

```

/etc/passwd

- Le Fichier **/etc/passwd** définit tous les utilisateurs qui existent sur le système Linux.
- Ce fichier texte peut être visualisé par tous les utilisateurs grâce à la commande **cat /etc/passwd**



Comandes utile

- La commande **id** permet de connaître le User Identifier d'un utilisateur
- la commande **passwd** permet de valider ou modifier un mot de passe
 - **passwd -l** : (lock) verrouille le compte de l'utilisateur, ex: **passwd -l annie**
 - **passwd -u** : (unlock) : déverrouille le compte
 - **passwd -d** : (delete) : supprime le mot de passe

/etc/shadow

- Ce fichier généralement associé à **/etc/passwd** contient des informations d'encryptage des mots de passe pour chaque utilisateur.

- La structure de ce fichier texte est identique à celle de **/etc/passwd** : chaque ligne est relative au mot de passe d'un utilisateur ;

| Champ n° 1 | Compte utilisateur |
|---------------|--|
| 2 | Mot de passe encrypté : si ce champs est vide, pas de mot de passe nécessaire! |
| 3 | Date à laquelle le mot de passe a été modifié la dernière fois (en jours depuis le 1/1/70) |
| 4 | Nombre de jours avant que le mot de passe puisse être changé (0 = n'importe quand) |
| 5 | Nombre de jours avant que le système ne force l'utilisateur à changer son mot de passe (- 1 = jamais) |
| 6 | Nombre de jours avant l'expiration du mot de passe pour prévenir l'utilisateur (-1 = pas d'avertissement) |
| 7 | Nombre de jours après que le mot de passe ait expiré pour verrouiller ce compte (-1 = jamais verrouiller) |
| 8 | Nombre de jours depuis lequel ce compte est invalidé (-1 = toujours actif) |
| 9 | Usage futur |

/etc/group

- Ce fichier décrit tous les groupes disponibles sous votre système Linux
 - contient la liste des groupes, un par ligne
 - pour chaque groupe, le numéro du groupe (**GID**)
 - les membres du groupe
- Le format de ce fichier est indiqué dans la page de manuel du fichier de configuration group (section 5) :

\$ man 5 group

...

- nom du groupe
- mot de passe chiffré du groupe. Si ce champ est vide, aucun mot de passe n'est nécessaire
- GID : identifiant numérique du groupe
- tous les noms des membres du groupe, séparés par des virgules

/etc/gshadow

- Contient les informations cachées sur les groupes.
- Il contient des lignes avec les champs suivant séparés par des deux-points :
 - nom du groupe
 - mot de passe chiffré
 - liste d' administrateur du groupe séparés par des virgules
 - liste des membres du groupe séparés par des virgules

4. Les droits d'accès sous Linux

- Les permission d'accès aux fichiers déterminent les actions que peuvent entreprendre les utilisateurs.

- Les droits d'accès sous Linux sont définis pour:
 - Un compte utilisateur: propriétaire du fichier, c'est en principe l'utilisateur qui a créé celui-ci.
 - Un groupe: ce groupe est généralement le groupe principal du propriétaire du fichier mais peut être modifié par ce dernier et prendre la valeur d'un de ses groupes secondaires.
 - Les autres: cette entité représente toute personne autre que le propriétaire et qui n'est pas membre du groupe cité précédemment.
- Les droits, l'utilisateur et le groupe propriétaires d'un fichier sont affichés avec la commande :

ls -l

smi@ubuntu: ~/Documents

```
smi@ubuntu:~/Documents$ ls -l
total 4
-rw-rw-r-- 1 smi smi 0 Oct 31 07:33 mon_fichier.txt
drwxrwxr-x 2 smi smi 4096 Oct 31 07:36 mon_repertoire
smi@ubuntu:~/Documents$
```

Avec:

| | |
|---|--------------------|
| - | Fichier ordinaire |
| d | Fichier répertoire |
| r | Read (lecture) |
| w | Write (Ecriture) |
| x | Exécution |

Type de fichier | Droits pour le propriétaire | Droits pour le groupe | Droits pour les autres

Voyons maintenant le sens de ces permissions. Le sens des termes « *droit d'écrire, droit d'exécuter* » diffère selon qu'ils s'appliquent à un fichier simple ou à un répertoire.

fichier

- **r : read** Permet la lecture du contenu du fichier.
- **w : write** Permet l'écriture, c'est-à-dire la modification, du fichier.
- **x : execute** Permet d'exécuter le fichier.

répertoire

- **r : read** Permet de lister le contenu du répertoire.
- **w : write** Permet de créer, d'effacer ou de renommer les fichiers du répertoire.
- **x : execute** Permet d'entrer dans le répertoire.

5. Gestion des droits

Changement des droits d'accès -chmod-

1- Mode symbolique

| Opérateur chmod | Signification | Exemple | Résultat |
|--------------------|--|-----------------------------|---|
| + | Ajouter les droits désignés à un fichier ou répertoire | chmod o+wx test.txt | Ajout des droits de modification et d'exécution au autres utilisateurs |
| - | Supprimer les droits désignés à un fichier ou répertoire | chmod u-x test.txt | Supprime le droit d'exécution ce fichier pour le propriétaire |
| = | Attribuer exactement ces droits | chmod g=r-x test.txt | Donne exactement les droits de lire et d'exécuter pour les utilisateurs du groupe |

2- Mode absolu

Exemple - r w x r w - r - -

1 1 1 1 1 0 1 0 0

7 6 4

Pour affecter ces droits en mode absolu

chmod 764 test.txt