

## CHAPITRE 3 : Gestion des Utilisateurs

**Mohammed SABER**

Département Électronique, Informatique et Télécommunications  
École Nationale des Sciences Appliquées "ENSA"  
Université Mohammed Premier OUJDA

Année Universitaire : 2018-2019

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions

## Introduction



- Tout objet du système de fichiers doit avoir :
  - Un compte utilisateur propriétaire
  - Un groupe propriétaire
- Savoir créer des utilisateurs.
- Savoir gérer les groupes et la participation des utilisateurs dans différents groupes.
- Connaître les fichiers de configuration.
- Modifier les comptes des utilisateurs et les informations de configuration par défaut.

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions

## Compte administrateur (SuperUser - root)

- Le nom de l'administrateur d'un système Linux est « **root** ».
- Pour avoir les privilèges de « **root** » il faut se connecter en tant que « **root** ». Quel que soit le shell de connexion de l'administrateur, l'invite est le symbole « **#** ».

```
login : root
password :*****
rootNom_machine :#
```

- Quand on est déjà connecté en tant qu'utilisateur simple, il est possible de prendre temporairement l'identité de l'administrateur grâce à la commande "**su**" qui veut dire "**Super User**".

```
userNom_machine :$ su
password :*****
rootNom_machine :#
rootNom_machine :# exit
userNom_machine :$
```

```
userNom_machine :$ sudo su
password :*****
rootNom_machine :#
rootNom_machine :# exit
userNom_machine :$
```

## Hierarchie des comptes

### Root : Super utilisateur

- Les permissions d'accès ne sont pas appliquées sur lui.
- Il peut faire tous.
- Compte pour l'administrateur du système.

### Comptes ordinaires : Utilisateur simple

- Compte pour une session sur le système.
- Les permissions d'accès sont appliquées sur lui.
- Il peut faire tous simplement sur leurs propres objets dans un espace limité (Changement de graphique, Création et modification sur les fichiers).

### Comptes Applications : SSH, FTP, HTTP, ...

Compte pour une session sur l'application et non sur le système.

### bin, daemon, ...

- Comptes utilisateur utilisés par différentes applications et démons.
- Ne peuvent pas (on doit pas) être utiliser comme login.

## Comptes Utilisateurs ordinaires

### Un compte utilisateur

- Définition de son identification pour le système ;
- Mais aussi définition d'un environnement utilisateur :
  - Home directory ;
  - Shell ;
  - Fichiers d'initialisation du shell ;
  - Environnement graphique ;
  - Quotas ;
  - etc.

### Opérations courantes sur un compte d'utilisateur

- Création d'un compte ;
- Modifications d'un compte ;
- Destruction d'un compte ;
- Archivage d'un compte ;

## Comptes Utilisateurs ordinaires

- Chaque utilisateur qui utilise le système doit être connu de celui-ci par un nom et éventuellement un mot de passe.
- Un utilisateur doit appartenir à un ou plusieurs groupes d'utilisateurs pour être autorisé à utiliser le système.
- Il existe plusieurs méthodes d'identification et de contrôle des utilisateurs, nous ne parlerons ici que de la méthode la plus simple mettant en œuvre les fichiers `/etc/passwd` et `/etc/group`.
- Les utilisateurs et les groupes sont repérés dans le système par des numéros : `UID` pour le numéro d'utilisateur (User Identifier) et `GID` pour le numéro de groupe (Group Identifier).
- Le numéro est unique pour un utilisateur ou un groupe donné. L'identification d'un utilisateur s'effectue dans le fichier `/etc/passwd`.

## Structure du fichier `/etc/passwd`

- Le fichier «`/etc/passwd`» existe sur tous les Linux (UNIX) !
- Le fichier `/etc/passwd` est un fichier de type texte dont chaque ligne définit un compte utilisateur.
- Attention : ajouter un compte dans le fichier texte ne fait rien d'autre : il faut compléter la création du compte pour qu'il soit fonctionnel
- Utilisateur dans «`/etc/passwd`» = une ligne.
- La ligne est composée par plusieurs champs.
- Le séparateur de champs est le symbole «`:`».



## Structure du fichier `/etc/passwd`

- **Nom de connexion** : le nom de connexion est saisi lors de la demande de connexion.

Login (Nom de Connexion) `etu:x:1000:1000:etudiant,,:/home/etu:/bin/bash`

- **Mot de passe** : le mot de passe est présent dans le fichier mais crypté. Le mot de passe crypté est déporté dans un fichier accessible seulement à l'administrateur «`/etc/shadow`».

Mot de passe `etu:x:1000:1000:etudiant,,:/home/etu:/bin/bash`

### Remarques

- Le fichier `/etc/passwd` est public (toute personne qui a un compte sur la machine peut le lire).
- Pour éviter cette faille, certains systèmes ont introduit le fichier `/etc/shadow`.
  - Lisible uniquement par **root**.
  - Contient les mots de passe des utilisateurs, qui disparaissent alors de `/etc/passwd`.
  - Si on ajoute un utilisateur à la main, cela implique d'éditer les 2 fichiers.

## Structure du fichier `/etc/passwd`

### • UID (User Identifier) :

- Une valeur entière positive généralement comprise entre 0 et 65535 permettant d'identifier un utilisateur de manière unique.
- L'administrateur attribue ce numéro à chaque utilisateur.
- Ce numéro, l'UID "User Identification" est mémorisé dans les descripteurs de fichiers pour en identifier le propriétaire. C'est donc l'information pertinente utilisée par Linux pour identifier un utilisateur.

`etu:x:1000:1000:etudiant,,:/home/etu:/bin/bash`  
**Identifiant numérique utilisateur (UID)**

### • GID (Group Identifier) :

- Indique le groupe de connexion d'un utilisateur.
- Un entier entre 0 et 65535 qui trouve sa correspondance dans le fichier `/etc/group`. L'administrateur identifie le groupe de connexion d'un utilisateur grâce à ce champ "Group Identification".
- Le fichier `/etc/group` associe un nom de groupe à ce **GID** et définit les groupes supplémentaires de l'utilisateur.

`etu:x:1000:1000:etudiant,,:/home/etu:/bin/bash`  
**Identifiant numérique groupe (GID)**

## Structure du fichier /etc/passwd

- **Commentaire** : la zone est utilisée librement par l'administrateur pour commenter le compte (Nom complet de l'utilisateur).

```
etu:x:1000:1000:etudiant,,,:/home/etu:/bin/bash
```

Commentaire

- **Répertoire de connexion** : Chemin complet de directory attribuée à l'utilisateur (conventionnellement /home/nom\_utilisateur pour l'utilisateur «nom\_utilisateur» . Ce répertoire contient les fichiers de configuration de l'utilisateur).

```
etu:x:1000:1000:etudiant,,,:/home/etu:/bin/bash
```

Répertoire de connexion

- **Shell de connexion** : ce champ précise le chemin d'accès absolu de la commande à exécuter lors de la connexion. C'est généralement un Shell.

```
etu:x:1000:1000:etudiant,,,:/home/etu:/bin/bash
```

Commande de connexion

## Les commandes de gestion des utilisateurs

Les commandes de gestion des comptes d'utilisateurs et de groupes sont nombreuses, les commandes qui seront mentionnées se décomposent en deux catégories :

### Les commandes d'administration

useradd, adduser, usermod, groupadd, addgroup, groupmod mais aussi userdel et groupdel pour respectivement supprimer un utilisateur ou un groupe. Les commandes pwck (vérifie la cohérence de /etc/passwd) et grpck (vérifie la cohérence de /etc/group) peuvent être utiles quand elles sont intégrées à un script.

### Les commandes d'information

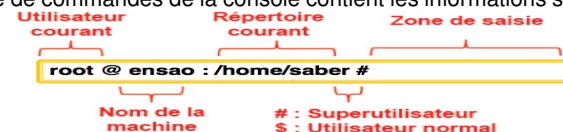
finger, passwd, su, id, vipw (éditer /etc/passwd) et vigr (éditer /etc/group).

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions

## La commande su

- L'invite de commandes de la console contient les informations suivantes :



- Commande fournie avec le paquet login ;
- La commande su permet de changer l'identité de l'utilisateur courant ;
  - Utilisateur est l'utilisateur dont on veut prendre l'identité ;
  - Accès à un autre compte utilisateur (demande mot de passe) ;

```
user1@Nom_machine :~$ su user2
password :*****
user2@Nom_machine :~$
```

```
user@Nom_machine :~$ su
password :*****
root@Nom_machine :~#
```

- Si aucun utilisateur n'est spécifié, le changement se fait vers l'utilisateur root ;
- Accès à un autre compte utilisateur à partir du compte root (pas de mot de passe).

```
root@Nom_machine :~# su user
user@Nom_machine :~$
```

## Créer un compte/session pour un nouvel utilisateur

- La commande `useradd` permet de créer un compte utilisateur.
- Sa syntaxe est simple dès lors que l'on connaît la structure des fichiers `/etc/passwd`, `/etc/group`. (voir `man useradd`)

### Syntaxe

`useradd [-c commentaire] [-d répertoire] [-e expiration] [-f inactive] [-g groupe] [-G groupes] [-u uid [-o]] [-s shell] utilisateur`

- `-c commentaire` : Le champ commentaire du fichier `/etc/passwd`.
- `-d répertoire` : Le répertoire de connexion. Cette option n'est nécessaire que s'il est différent de `/repertoire_base/utilisateur`, `/home/med` pour l'user `med`.
- `-e expiration` : La date d'expiration du compte.
- `-f inactive` : Le nombre de jours d'inactivité au bout duquel le compte devient invalide.
- `-g groupe` : Le groupe principal de l'utilisateur. Le groupe doit exister préalablement à la création du compte.
- `-G groupes` : Les groupes supplémentaires de l'utilisateur.
- `-u uid` : L'UID de l'utilisateur.

## Modifier le compte d'un utilisateur par `usermod`

- La commande `usermod` permet de modifier un compte utilisateur.
- **Syntaxe** : `usermod [options] nom_login`. (voir `man usermod`)
- Les options sont les mêmes que `useradd`.

### Syntaxe

`usermod [-c commentaire] [-d répertoire] [-e expiration] [-f inactive] [-g groupe] [-G groupes] [-u uid [-o]] [-s shell] utilisateur`

- `-c commentaire` : Le champ commentaire du fichier `/etc/passwd`.
- `-d répertoire` : Le répertoire de connexion. Cette option n'est nécessaire que s'il est différent de `/repertoire_base/utilisateur`, `/home/med` pour l'user `med`.
- `-e expiration` : La date d'expiration du compte.
- `-f inactive` : Le nombre de jours d'inactivité au bout duquel le compte devient invalide.
- `-g groupe` : Le groupe principal de l'utilisateur. Le groupe doit exister préalablement à la création du compte.
- `-G groupes` : Les groupes supplémentaires de l'utilisateur.
- `-u uid` : L'UID de l'utilisateur.

## Gestion des mots de passes par la commande `passwd`

- Nous allons compléter la présentation de la commande `passwd`, déjà connue, pour permettre à l'administrateur de gérer les mots de passe des utilisateurs.
- **Syntaxe** : `passwd [options] nom_login`. (voir `man passwd`)
  - Modifier le mot de passe d'un utilisateur : `passwd Nom_user` ;
  - Supprimer le mot de passe d'un utilisateur : `passwd -d Nom_user` ;
  - Verrouiller le compte d'un utilisateur (Empêcher sa connexion) : `passwd -l Nom_user` ;
  - Déverrouiller le compte d'un utilisateur : `passwd -u Nom_user` ;
  - Forcer le changement de mot de passe à la prochaine connexion : `passwd -f Nom_user` ;

### Remarques

Pour les administrateurs :

- Il ne faut jamais supprimer le mot de passe d'un utilisateur en éditant directement le fichier qui le contient,
- `/etc/passwd` dans un système non sécurisé.
- Cela risque fort de générer des incohérences dans les fichiers de données.

## Autres commandes

### Supprimer le compte d'un utilisateur par `userdel`

- **Syntaxe** : `userdel [-r] nom_login`
- L'option `-r` supprime aussi le répertoire personnel de l'utilisateur ;
- La commande supprime toute trace de l'utilisateur dans le fichier de configuration : `/etc/passwd` y compris dans les groupes d'utilisateurs.

### Connaître l'UID et le GID d'un utilisateur courant par `id`

Connaître l'UID et le GID d'un utilisateur.

```
Fichier Édition Affichage Terminal Aide
root@l213:/home/lpro# id alpha
uid=2001(alpha) gid=3001(groupe1) groupes=3001(groupe1),3002(groupe2)
root@l213:/home/lpro# id beta
uid=2002(beta) gid=3002(groupe2) groupes=3002(groupe2),3001(groupe1)
root@l213:/home/lpro#
```

### Information sur les utilisateurs connectés par (`who`, `finger`)

Donne des informations sur un utilisateur.

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes**
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions

## Structure du fichier `/etc/group`

- Le fichier `/etc/group` est un fichier de type texte dont chaque ligne définit un groupe d'utilisateurs.
- La ligne est composée de champs.
- Le séparateur de champs est le symbole " :".

Nom du groupe	:	Mot de passe	:	GID	:	Liste des utilisateurs membre du groupe
---------------	---	--------------	---	-----	---	---

### Nom du groupe

Le nom du groupe est celui utilisé dans les commandes de gestion des groupes, ou par exemple, celui affiché par la commande `ls`.

### Mot de passe

Ce champ contient le mot de passe crypté. Le mot de passe était demandé à un utilisateur qui voulait se connecter à un groupe dont il n'était pas membre.

### Liste des utilisateurs

La liste des utilisateurs qui sont membres du groupe.

## Les comptes des groupes

- Un groupe est un ensemble d'utilisateurs.
- Chaque utilisateur doit faire partie au moins d'un groupe.
- 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.
- La liste des groupes est donnée par le fichier `/etc/group`.

## Comment faire partie d'un groupe ?

Il y'a trois possibilités pour appartenir à un groupe :

- Le groupe est votre groupe initial défini dans `/etc/passwd`.
- Le groupe est un de vos groupes supplémentaires définis dans `/etc/group`.
- Vous connaissez le mot de passe associé au groupe et vous vous connectez à ce groupe grâce à la commande `newgrp`.

### Remarques

- Lors de la connexion, le groupe courant est le groupe initial.
- La commande `newgrp` permet de modifier le groupe courant.
- Le groupe courant détermine le groupe des fichiers que vous créez.
- La commande `id -a` permet de connaître votre groupe courant (GID) et les groupes dont on est membre (`groups`).

## Les commandes de gestion des groupes

- Pour lister tous les groupes d'un utilisateur : `groups nom_login` ;
- Pour créer un nouveau groupe : `groupadd nom_groupe` ;
- Supprimer un groupe : `groupdel nom_groupe` (le groupe est supprimé du fichier `/etc/group`) ;
- modifier un groupe : `groupmod -n nouveau_nom nom_groupe` ;
- Pour ajouter un utilisateur à un groupe. Le plus simple est d'éditer le fichier `/etc/group` et d'ajouter une liste d'utilisateurs (séparés par des virgules) sur la ligne du groupe.

## Le dialogue avec les utilisateurs

- L'administrateur dispose de nombreux moyens pour informer les utilisateurs et dialoguer avec eux.
- Certaines commandes sont déjà connues par les utilisateurs et ne sont mentionnées qu'à titre de rappel :
  - `mail` : La commande envoie un courrier déposé dans la boîte aux lettres de l'utilisateur.
  - `write` : La commande affiche un message sur l'écran de l'utilisateur connecté s'il a accepté qu'on lui écrive par `write`.
  - `wall` : La commande (`wall` : Write All) envoie le message fourni par l'administrateur sur l'entrée standard à tous les utilisateurs.
  - `talk` : La commande permet un dialogue en temps réel.

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs**
- 6 Surveillance des connexions

## Plan de chapitre

- 1 Introduction
- 2 Les comptes des utilisateurs
- 3 Les commandes de gestion des utilisateurs
- 4 Les comptes des groupes
- 5 Le dialogue avec les utilisateurs
- 6 Surveillance des connexions**

## Surveillance des connexions

- Le système Linux conserve une grande partie de ces informations dans des fichiers journaux (fichiers log), ce qui permet après coup de retracer l'activité du système.
- Donc possible de détecter les comportements anormaux, comme par exemple un grand nombre de tentatives de connexions ayant échouées pour le compte root.
- Ces fichiers se trouvent généralement dans `/var/log`.
- Contrôle régulier des connexions impératif !
  - Liste des utilisateurs connectés  $\Rightarrow$  `w` ;

```
etu@vm:~$ w
02:28:11 up 0 min, 1 user, load average: 0,17, 0,05, 0,02
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
etu       pts/0    192.0.2.1     02:28    0.00s  0.11s  0.00s  w
```

- Journalisation des connexion  $\Rightarrow$  `/var/log/auth.log` (selon la distribution Linux utilisée) ;

```
vm.sshd[1966]: Server listening on :: port 22.
vm.sshd[2004]: Accepted password for etu from 192.0.2.1 port 42096 ssh2
vm.sshd[2004]: pam_unix(sshd:session): session opened for user etu by (uid=0)
```

- Historique des connexions (Comptes système utilisés).

```
# lastlog
Utilisateur  Port  Venant de  Dernière
root        tty1          jeu. mai 17 11:01:50 +0200 2012
daemon              **Jamais connecté**
bin              **Jamais connecté**
sys              **Jamais connecté**
svnc              **Jamais connecté**
saber       pts/0    192.0.2.1   jeu. juin 6 12:28:10 +0200 2012
```

## QUESTIONS ?