AGENCE UNIVERSITAIRE DE LA FRANCOPHONIE

CHAPITRE 5

Gestion des utilisateurs et des groupes d'utilisateurs

CNF Rabat **Mohammed RIDOUANI**

Novembre 2010

Objectifs

- 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.

Gestion des utilisateurs et des groupes d'utilisateurs

SOMMAIRE

- Principe de base
- Les fichiers de configuration
  - /etc/group
  - /etc/passwd
  - /etc/shadow
- Création d'un compte utilisateur
- Destruction de compte
- Gestion de groupe
- Gestion des comptes
- Exercices et TPs

PRINCIPE: COMPTE UTILISATEUR

Espace de travail pour un utilisateur donné :

Accessible selon **les droits** fixés par:

- Le propriétaire de cet espace
- Le super utilisateur

Accessible par :

- Un **login**
- Un **mot de passe** (jamais vide).

Matérialisé par **un répertoire** et un ou plusieurs fichiers de configuration (selon la version du système).

PRINCIPE: COMPTE UTILISATEUR

Le super utilisateur

Il a **seul** le pouvoir de **créer un compte utilisateur** à l ’aide des différents outils suivants :

Les **commandes en ligne**

Les **logiciels d'administration**
(yast sous suse, kuser sous Red Had)

D'autres utilitaires

PRINCIPE: COMPTE UTILISATEUR

L'utilisateur dispose des attributs de base suivants :

- un nom de connexion appelé le login
- un mot de passe
- un UID
- un GID correspondant à son groupe principal
- un descriptif
- un répertoire de connexion
- une commande de connexion

PRINCIPE: GROUPE

Chaque utilisateur fait partie d'au moins un groupe. Un groupe regroupe des utilisateurs. Comme pour les logins, le GID du groupe accompagne toujours l'utilisateur pour le contrôle de ses droits.

Le groupe primaire est celui qui est toujours appliqué à la création d'un fichier.

PRINCIPE: MOTS DE PASSE

Les mots de passe permettent d'authentifier les utilisateurs.

Les mots de passe sont cryptés (MD5)

LES FICHIERS DE CONFIGURATION

Ils sont regroupés dans **deux** répertoires:
/etc et ***/bin***.

Les principaux fichiers sont :

Nom du fichier	Description
/etc/group	Définition des groupes (système + utilisateurs)
/etc/passwd	Définition des comptes (système + utilisateurs)
/etc/shadow	Définition des mots de passe (complète */etc/passwd*)
/bin/passwd	Modification du mot de passe

LE FICHIER /etc/passwd

Rôle

-Définit les comptes utilisateurs et système.
- Chaque ligne définit un compte utilisateur.
- Une ligne comporte **sept champs**, séparés par deux points (:).
Login:password:UID:GID:comment:homedir:shell

Les droits du fichier */etc/passwd* sont :
rw-r--r--

LE FICHIER /etc/passwd

Les différents champs

1) Nom de login :
Nom sous lequel l'utilisateur se connecte au système.

2) Mot de passe :
sur les vieilles versions, le mot de passe crypté. Si un x est présent, le mot de passe est placé dans /etc/shadow. Si c'est un point d'exclamation le compte est verrouillé.

3) UID(User IDentifier)
Entier unique compris entre 0 et 65535.

4) GID (Group IDentifier)
- Entier unique compris entre 0 et 65535.
- Il est partagé par tous utilisateurs d'un même groupe.

LE FICHIER /etc/passwd

Les différents champs

5) Commentaires :
- Champ réservé à l'administrateur.
- Contient éventuellement une chaîne servant de commentaire.

6) Répertoire d'accueil du compte :
le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte.

7) Shell de démarrage :
- Indique le programme à exécuter au moment de la connexion.
- Ce champ contient le nom d'un shell, par exemple Bourne shell (*/bin/bash*), le C-Shell (*/bin/csh*) et le Korn Shell (*/bin/ksh*).

LE FICHIER /etc/shadow

Rôle

- Il contient les informations relatives à la sécurité du compte utilisateur.
- Chaque ligne correspond à un compte utilisateur.

said:
$2a$10$AjADxPEfE5iUJcltzYA4wOZO.f2UZ0qP/8EnOFY

Les droits du fichier */etc/shadow* sont :

r--------

Conséquence :

Seul le root peut visualiser ce fichier.

LE FICHIER /etc/shadow

Les différents champs

1) Nom de login :
- Idem à */etc/passwd*.

2) Mot de passe :
crypté

3) Dernière modification
Date de la dernière modification du mot de passe:
- en nombre de jours
- depuis le 1 janvier 1970.

Il est mis à jour par le système lorsqu'on change de mot de passe.

LE FICHIER /etc/shadow

Les différents champs

4) Durée min :
- Durée s'écoulant entre deux modifications du mot de passe.
- Exprimé en nombre de jours.

5) Durée max :
- Durée maximale de validité du mot de passe.
- Exprimé en nombre de jours

6) Période avertissement :
Nombre de jours précédant la date d'expiration du mot de passe à partir duquel l'utilisateur doit être averti par le système.

LE FICHIER /etc/shadow

Les différents champs

7) Durée inactivité :
Nombre de jours maximum d'inactivité autorisée avant le verrouillage du compte.

8) Durée expiration :
Date d'expiration à partir de laquelle le compte sera verrouillé

9) Réservé :
Non encore affecté

LE FICHIER /etc/group

-Définit les groupes d'utilisateurs
- Chaque ligne définit un groupe
- Permet de faire le lien entre :
    Le numéro de groupe (GID)
    La liste des utilisateurs de ce groupe
- Une ligne contient quatre champs, séparés par deux points (:)

Group:password:GID:user1,user2,...

Les droits du fichier /etc/group

rw-r--r--

LE FICHIER /etc/group

Les différents champs

1) Nom du groupe

2) Mot de passe

3) Numéro du groupe (GID)

4) Les membres

- Chaque groupe comprend une liste des membres, séparés chacun par une virgule.

CONVERSION DES FICHIERS

pwunconv:convertir les fichiers /etc/shadow et /etc/passwd en un seul et unique /etc/passwd

```
# pwunconv
# grep said /etc/passwd
said:
$2a$10$dwbUGrC75bs3l52V5DHxZefkZyB6VTHsLH5ndjsNe/v
F/HAzHOcR2:1001:100:toto:/home/bean:/bin/bash
# ls -l /etc/shadow
ls: ne peut accéder /etc/shadow: Aucun fichier ou
répertoire de ce type
```

CONVERSION DES FICHIERS

La commande **pwconv** fait l'inverse

```
# grep said /etc/passwd
said:x:1001:100:toto:/home/bean:/bin/bash
p64p17bicb3:/home/seb
# grep said /etc/shadow
said:
$2a$10$dwbUGrC75bs3l52V5DHxZefkZyB6VTHsLH5ndjsNe/v
F/HAzHOcR2:13984:0:99999:7:::0
```

Les commandes **grpconv** et **grpunconv** font la même chose pour les groupes

FICHIER DE CONFIGURATION PAR DEFAUT

Le fichier **/etc/login.defs** contient les informations par défaut sur la validité des comptes et des mots de passe des utilisateurs. Ces informations sont stockées dans le fichier **/etc/shadow** lors de la création du compte

```
! MAIL_DIR : répertoire mail par défaut (e.g. /var/spool/mail) ;
! PASS_MAX_DAYS, PASS_MIN_DAYS, PASS_MIN_LEN, PASS_WARN_AGE : informations
concernant la validité du mot de passe ;
! UID_MIN, UID_MAX : plage des numéros identifiant des utilisateurs (UID)
lors de l'utilisation de useradd ;
! GID_MIN, GID_MAX : plage des numéros identifiants des groupes (GID) lors
de l'utilisation de groupadd ;
! CREATE_HOME : création automatique du répertoire home lors de
l'utilisation de useradd ;
! PASS_MAX_DAYS : nombre de jours maximum d'utilisation d'un mot
de passe ;
! PASS_MIN_DAYS : nombre de jours minimum entre deux changements
de mot de passe ;
! PASS_MIN_LEN : taille minimum d'un mot de passe ;
! PASS_WARN_AGE : nombre de jours d'envoi d'un avertissement avant
que le mot de passe n'expire.
```

CRÉATION D'UN COMPTE UTILISATEUR

Les méthodes

1 - Manuellement

2 - A l'aide d'un utilitaire en ligne de commande

3 - A l ’aide d’un utilitaire graphique

CRÉATION D'UN COMPTE UTILISATEUR

Les méthodes : Manuellement

La création d'un utilisateur consiste à :

- rajouter une ligne dans **/etc/passwd**,
- rajouter d'une ligne dans **/etc/shadow**,
- rajouter d'éventuelles informations dans **/etc/group**,
- créer le répertoire personnel et mettre à jour son contenu avec **/etc/skel**,
- changer les permissions et le propriétaire du répertoire personnel(***chown et chgrp***),
- changer le mot de passe (**passwd**).

CRÉATION D'UN COMPTE UTILISATEUR

Les méthodes : *Utilitaire en ligne de commande*

Commande useradd ou adduser

Permet d ’ajouter un utilisateur

/usr/sbin/useradd [options] nom-utilisateur

Les principales options **:**

-c	commentaire
-d	répertoire de base
-e	date limite(MM/DD/YY).
-f	délai d’inactivité.
-g	groupe primaire
-s	shell
-u	uid.

CRÉATION D'UN COMPTE UTILISATEUR

Les méthodes : *Utilitaire en ligne de commande*

Commande useradd ou adduser

Exemple

useradd –u 100 –s /bin/bash –c “ gérant de l’entreprise”
–d /home/said –g user said

Les options par défaut se trouvent dans le fichier **/etc/default/useradd** (ou sont listées par l'option **-D** de la commande **useradd**)

Pour activer le compte, l'administrateur doit définir un mot de passe pour le compte par la commande **/usr/bin/passwd**

/usr/bin/passwd said

DESTRUCTION D ’UN COMPTE UTILISATEUR

Les méthodes : *Utilitaire en ligne de commande*

Commande **userdel**

Permet de supprimer un utilisateur

Suppression d’un utilisateur et son répertoire de base :

L ’option **-r** de **userdel**

CRÉATION D'UN COMPTE UTILISATEUR

Les méthodes : Utilitaire graphique

Kuser	pour Redhat
Yast	pour Suse
Linuxconf	pour Redhat
users-admin	Pour Débian

GESTION DE GROUPE

Création, destruction et administration de groupes

Pour créer un groupe on utilise la commande :
groupadd nom _du_group

Pour supprimer un groupe on utilise la commande :
groupdel nom_du_groupe

gpasswd –a said stagiaire : pour ajouter l'utilisateur said dans le groupe stagiaire.
gpasswd –d said stagiaire : pour supprimer gaye dans le groupe stagiaire
gpasswd -A said stagiaire : pour nommer said administrateur du groupe stagiaire.

GESTION DE GROUPE

Administrer un groupe

Pour connaître la liste des groupes que l'on peut joindre, on utilise la commande **id**

```
id
uid=1421(moi) gid=1664(normal) groupes=1664(normal),2010
(compta),2008(chefs)
```

Pour rejoindre un autre groupe, on utilise la commande **newgrp**

```
newgrp chefs
```

Pour connaître la liste des groupes disponibles, on utilise la commande **groups**

```
groups
normal compta chefs
```

GESTION DES COMPTES ET DES OPTIONS DE CREATION PAR DEFAUT

Les options de configuration d'un compte peuvent être modifiées par la commande **usermod**

-l nouveau nom d'utilisateur
-c commentaire
-g groupe (il doit exister au préalable)
-s shell
-d chemin du répertoire 'home'
-u identifiant utilisateur (UID)
-p mot de passe à entrer en format md5
-e informations d'expiration du compte

GESTION DES COMPTES ET DES OPTIONS DE CREATION PAR DEFAUT

Les options de configuration d'un groupe peuvent être modifiées par la commande **groupmod**

-n nouveau nom du groupe

-g identifiant du groupe

GESTION DES COMPTES ET DES OPTIONS DE CREATION PAR DEFAUT

Bloquer un compte

Un moyen simple et de faire précéder le mot de passe par un **'!'** dans les fichiers de configuration. Lors de l'utilisation d'un fichier **/etc/shadow**, on peut remplacer également le **'x'** dans le fichier **/etc/passwd** par un **'*'**

Une autre méthode consiste à utiliser les commandes **'passwd' et 'usermod'.**

```
passwd -l
usermod -L
```

Pour débloquer le compte en utilisant les mêmes commandes

```
passwd -u
usermod -U
```

On peut aussi détruire le mot de passe par la commande

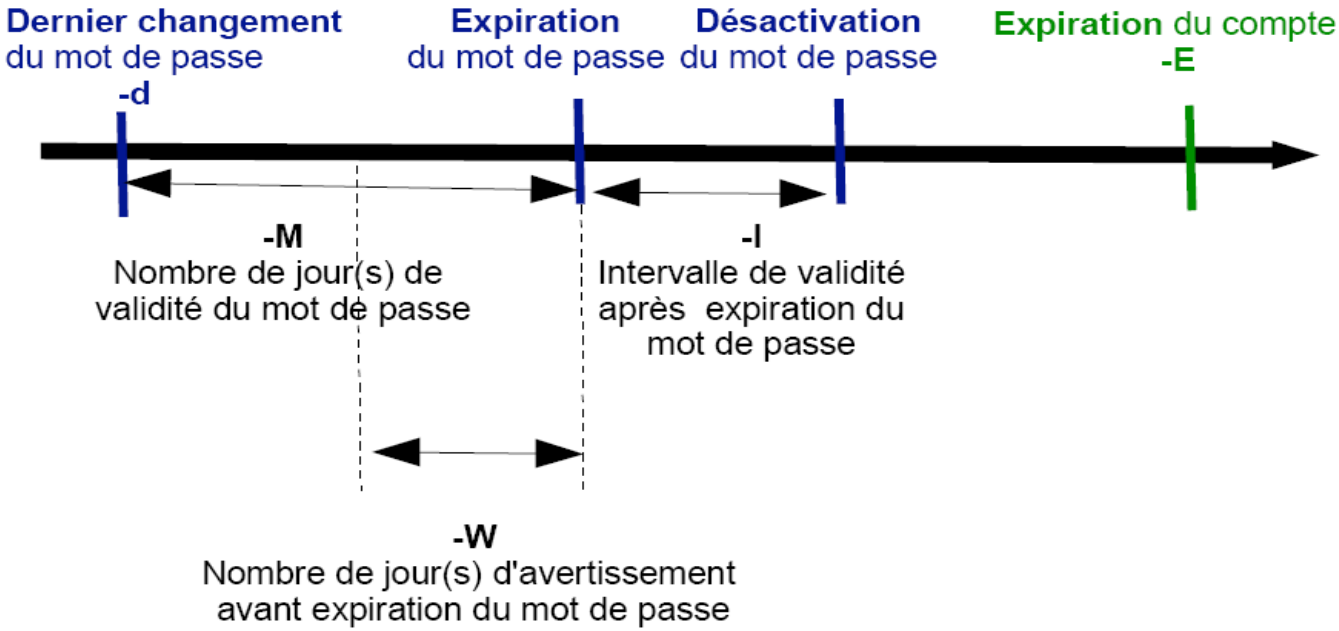
```
passwd -d
```

GESTION DES COMPTES ET DES OPTIONS DE CREATION PAR DEFAUT

Gestion des informations d'expiration du compte

Pour modifier les informations mises par défaut (**/etc/login.defs**) et les informations d'expiration, on utilise la commande **/usr/bin/chage**

chage [-l] [-m min_days] [-M max_days] [-W warn] [-I inactive] [-E expire] [-d last_day] user



EXERCICES

1) Par quelle méthode un utilisateur est-il authentifié sous Linux ?

- A - Par son login.
- B - Par son UID.
- C - Par son mot de passe.
- D - Par une clé secrète.

2) Quelle commande permet de connaître les UID et GID d'un utilisateur ?

3) Quel est le chemin complet du fichier contenant les mots de passe cryptés ?

4) Est-ce que root peut connaître le mot de passe d'un utilisateur?

5) L'utilisateur **mounir** a été licencié de l'entreprise. Comment verrouiller son compte ?

EXERCICES

6) Quelle commande saisir pour forcer l'utilisateur **mounir** à changer son mot de passe tous les 30 jours ?

7) La ligne **useradd -m -u 100 -g users -G vidéo -c test –s /bin/false**:

- A - Ne marche pas.
- B - Ajoute un utilisateur test d'UID 100.
- C - Ajoute un utilisateur vidéo mais qui n'a pas le droit de se connecter.
- D - Crée un utilisateur de groupe secondaire vidéo.

8) Quelle variable du fichier /etc/login.defs devez-vous modifier pour que tous les UID des utilisateurs démarrent à 1500 ?

9) **mounir** avait des documents importants dans son répertoire personnel. Comment supprimer son compte sans supprimer son dossier personnel ?

TPs

But : créer un utilisateur et appliquer une politique de sécurité.

1) Créez un utilisateur **fouad** ayant comme UID **1000**, comme groupe **lpi**, comme commentaire **Formation LPI 102** et comme shell **/bin/bash.**

2) Activez le compte de **fouad**

3) Ajoutez un groupe **CNF** et un groupe **AUF** avec le GID **800**

4) Ajoutez **fouad** dans le groupe **CNF** (en utilisant une commande) et dans **AUF** (en éditant le fichier /etc/group).

5) Modifiez les informations de changement de mot de passe de **fouad** avec la commande chage. Le mot de passe ne peut pas être changé avant 10 jours et il est obligatoire de le changer tous les 50 jours.

6) Blouquez, deblouquez, et après supprimez le compte de **fouad**