Chapitre1 Parite B. Gestion des utilisateurs et des groupes d'utilisateurs

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.
Points importants	Le système de gestion des utilisateurs sous Linux est simple mais efficace. Cependant, il a quelques limitations.
Mots clés	/bin/false, /etc/default/useradd, /etc/group, /etc/gshadow, /etc/passwd, /etc/shadow, /etc/skel, groupadd, groupdel, groupe, groups, grpconv, grpunconv, id, newgrp, passwd, pwconv, pwunconv, useradd, userdel, usermod, utilisateur

A. Les utilisateurs

Pour la création d'un utilisateur, on utilise la commande `/usr/sbin/useradd`, ou son alias `/usr/sbin/adduser` qui est un lien symbolique vers la commande précédente pour des raisons de compatibilité historique.

Syntaxe :

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

Quelques options utiles :

- `-c` : commentaire ;

- `-g` : groupe ;
- `-s` : shell.

Pour ajouter un utilisateur « mejdi » dans le groupe « chefs » avec le shell « tcsh » :

```
/usr/sbin/adduser -c 'Mejdi le chef' -g 'chefs' -s '/bin/tcsh'
mejdi
```

Les options par défaut se trouvent dans le fichier /etc/default/useradd, ou bien sont listées par l'option `-D` de la commande `useradd`.

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
```

Chaque utilisateur possède un identifiant ou UID (*user identifier*), numéro généré automatiquement et compris entre 500 et 60 000. Un autre intervalle de valeurs peut si nécessaire être imposé. Il doit dans ce cas être spécifié dans le fichier `/etc/login.defs`.

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

Syntaxe :

```
/usr/bin/passwd nom-utilisateur
```

Exemple :

```
/usr/bin/passwd mejdi
```

Cette commande permet également à l'utilisateur de changer lui-même son mot de passe.

B. Les groupes

Un utilisateur appartient toujours au moins à un groupe dit **groupe primaire** (*primary group*).

Si le groupe n'est pas spécifié au moment de la création du compte deux stratégies générales sont employées pour assigner un groupe par défaut :

- le groupe par défaut est le même pour tous. Il s'appelle par exemple « **users** » ;
- la distribution Red Hat a introduit la notion de groupe privé par utilisateur ou **UPG** (*User Private Group*). Le nom du groupe est identique à celui du login.

Selon la stratégie employée, le masque par défaut (*umask*) de création est initialisé à 022 dans le premier cas (classique) et à 002 dans le deuxième cas (UPG).

Si un utilisateur crée un fichier, celui-ci appartiendra par défaut au groupe primaire de l'utilisateur.

Un utilisateur peut appartenir à d'autres groupes, ce sont les groupes secondaires.

Pour connaître la liste des groupes auxquels l'utilisateur appartient, on utilise la commande `id`.

Dans l'exemple qui suit, l'utilisateur « moi » appartient au groupe primaire « normal » et aux groupes secondaires « compta » et « chefs ».

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

La commande `newgrp` permet de changer temporairement de groupe primaire, à condition que le nouveau groupe soit un groupe secondaire de l'utilisateur ou que l'utilisateur en connaisse le mot de passe.

```
newgrp chefs
```

La commande `id` donne alors :

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

La commange `groups` permet elle aussi d'afficher les groupes auxquels appartient un utilisateur.

```
groups
normal compta chefs
```

Pour ajouter un groupe, on utilise la commande `groupadd` :

```
groupadd forcats
```

Pour supprimer un groupe, on utilise la commande `groupdel` :

```
groupdel forcats
```

Ces commandes mettent à jour le fichier /etc/group.

Pour gérer les utilisateurs d'un groupe, on utilise la commande `gpasswd`.

Les options sont les suivantes :

- `-a` : ajout d'un utilisateur ;
- `-d` : retrait d'un utilisateur ;
- `-A` : affectation d'un administrateur au groupe.

```
gpasswd -a nicolas forcats
```

La commande était prévue à l'origine pour ajouter un mot de passe commun au groupe et permettre aux utilisateurs appartenant à un même groupe de se connecter avec le même mot de passe, ce qui explique le nom de la commande. Cette possibilité n'existe plus pour des raisons de sécurité évidentes.

C. Les fichiers de configuration

a) Gestion des utilisateurs

Le fichier /etc/passwd contient les informations sur les utilisateurs, structurées en sept champs :

- login ;
- UID ;
- GID ;
- mot de passe ou « x » s'il existe un fichier /etc/shadow ;
- description de l'utilisateur ;
- répertoire par défaut de l'utilisateur ;
- shell.

Les sept champs sont présentés sur une ligne et séparés par le caractère « : ».

Exemple de ligne extraite d'un fichier /etc/passwd avec utilisation d'un fichier /etc/shadow :

```
nicolas:x:502:502:Nicolas L:/home/nicolas:/bin/tcsh
```

Depuis quasiment l'origine, la majorité des distributions Linux utilise un fichier /etc/shadow pour stocker les mots de passe. La sécurité est bien meilleure car il est protégé en lecture. Le fichier /etc/passwd est, lui, lisible par toutes les applications.

Pour créer un fichier « /etc/shadow » à partir d'un fichier « /etc/passwd » on utilise la commande /usr/sbin/pwconv.

Pour revenir à la configuration précédente (*i.e.* stockage des mots de passe dans le fichier /etc/passwd), on utilise la commande /usr/sbin/pwunconv.

Attention à fixer correctement les droits sur ces fichiers : 600 ou même 400 pour /etc/shadow et 644 pour /etc/passwd.

Ne pas oublier de vérifier, lors de l'utilisation de la commande pwunconv, de remettre les mêmes droits sur le fichier /etc/passwd.

b) Gestion des groupes

Le fichier /etc/group contient les informations sur les groupes, structurées en quatre champs :

- nom du groupe ;
- mot de passe du groupe ou « x » s'il existe un fichier /etc/gshadow ;
- GID ;
- liste des utilisateurs du groupe.

Les quatre champs sont présentés sur une ligne et séparés par le caractère « : ».

Ligne de fichier /etc/group avec utilisation d'un fichier /etc/gshadow :

```
normal:x:555:niry,andrei,kader,nicolas
```

De même que pour le fichier /etc/passwd, pour créer un fichier /etc/gshadow à partir d'un fichier /etc/group on utilise la commande :

```
/usr/sbin/grpconv
```

Pour revenir à la configuration précédente (i.e. stockage des mots de passe dans le fichier /etc/group et destruction de /etc/gshadow) :

```
/usr/sbin/grpunconv
```

c) Fichiers de configuration par défaut

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 maximum de jours d'utilisation d'un mot de passe ;
- PASS_MIN_DAYS : nombre minimum de jours 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.

D. Gestion des comptes et des options de création par défaut

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.

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

- `-n` : nouveau nom du groupe ;
- `-g` : identifiant du groupe (GID).

a) Comment bloquer un compte

Un moyen simple est 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 :

```
passwd -d
```

Enfin, on peut affecter à un utilisateur le shell par défaut `/bin/false`, ce qui l'empêche de se connecter.

b) Gestion des informations d'expiration du compte

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

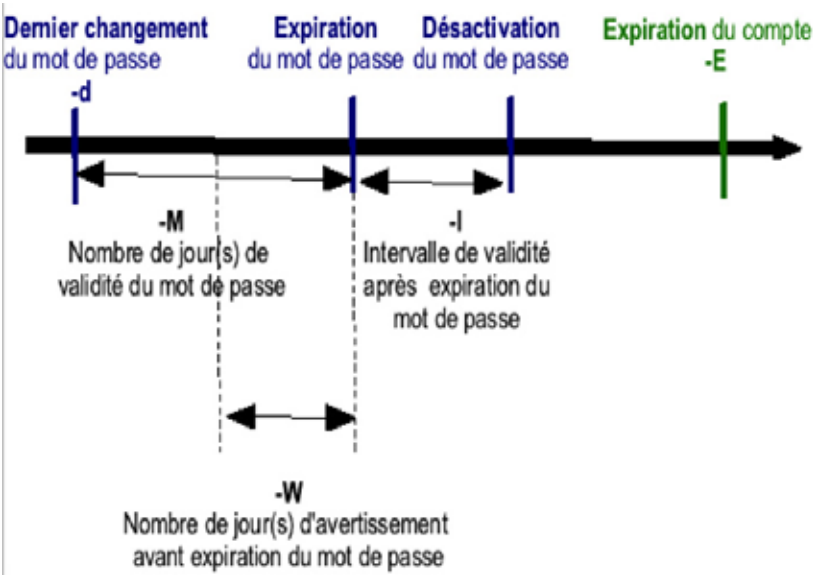
```
chage [ -l ] [ -m min_days ] [ -M max_days ] [ -W warn ] [ -I
inactive ] [ -E expire ] [ -d last_day ] user
```

Options :

- `-l` donne les valeurs actuelles du compte ;
- `-E` permet de fixer une date d'expiration sous la forme Unix standard ou sous la forme YYYY/MM/DD ;
- `-M` permet de changer la valeur de PASS_MAX_DAYS contenue dans le fichier /etc/login.defs ;
- `-m` permet de changer la valeur de PASS_MIN_DAYS contenue dans le fichier /etc/login.defs ;
- `-w` permet de changer la valeur de PASS_WARN_AGE contenue dans le fichier /etc/login.defs ;
- `-d` permet de changer la date de dernier changement de mot de passe sous la forme Unix standard ou sous la forme YYYY/MM/DD.

La *figure 4* récapitule les différentes informations associées à la « vie » du compte.

Figure 4. Informations d'expiration d'un compte associées à la commande en ligne



c) Destruction d'un compte

On utilise la commande `/usr/sbin/userdel`. L'option `-r` permet de détruire également le contenu du répertoire home.

```
/usr/sbin/userdel -r mejdi
```

E. Exercices

1. **Quelle est la commande Unix qui permet de créer un utilisateur user1 qui appartient au groupe auf ?**
   - ❑ useradd -m -g user1 auf
   - ❑ useradd -m user1 -group auf
   - ❑ add -m -g auf user1
   - ❑ useradd -m -g auf user1

2. **L'utilisateur mejdi a été déplacé dans le département BECO. Vous voulez changer son groupe principal en beco. Quelle est la commande la plus simple pour réaliser cela ?**