Administration système

Gestion des utilisateurs

Tuyêt Trâm DANG NGOC
<dntt@dept-info.u-cergy.fr>

Université de Cergy-Pontoise

2009–2010

Utilisateur

- Tout utilisateur est caractérisé par :
  - un nom (login)
  - un numéro d'utilisateur (UID)
  - un numéro de groupe (GID)
  - un mot de passe
  - un shell
- Les utilisateurs sont définis dans `/etc/passwd` (et `/etc/shadow` ou `/etc/master.passwd`)
- Les groupes d'utilisateur sont définis dans `/etc/group`

Fichier /etc/passwd

Le fichier /etc/passwd centralise toutes les informations relatives aux utilisateurs connus sur le système.

- en format texte (clair et modifiable avec tout éditeur de texte)
- Liste d'utilisateurs (un par ligne), dont chaque ligne contient :
  - le nom (login) : pas de majuscule et pas plus de 8 caractères sur certains systèmes
  - le mot de passe chiffré : lors de la connexion, le mot de passe utilisateur est chiffré et comparé avec cette version
  - le numéro d'utilisateur (UID) : identifiant entre 0 et 32767 **unique** de l'utilisateur
  - le numéro de groupe d'utilisateurs (GID) : groupe par défaut de l'utilisateur. Entre 0 et 32767.
  - le nom complet de l'utilisateur (gecos) : pour information.
  - le répertoire d'accueil (*homedir*) : répertoire par défaut quand on se connecte et à laquelle est initialisée la variable **$HOME**
  - le shell : le shell par défaut. S'il est vide, **/bin/sh** sera pris.

  Ces champs (dans cet ordre) sont séparés par des " :"

  Pas de commentaires possibles

Format du fichier /etc/passwd

```
login :mot-de-passe :UID :GID :gecos :repertoire :shell
```

Exemple

```
root:$1$8ofzSt0:0::Le chef:/root:/bin/sh
daemon:*:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:*:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:$1$4/jh/aXv:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:$4HUcta/uYY:1002:1000:Remy CARD:/users/card:/bin/csh
```

Le fichier /etc/passwd est lisible par tous les utilisateurs, mais n'est modifiable que par root

Groupe d'utilisateurs

- Un utilisateur appartient à :
  - un groupe primaire
  - plusieurs groupes secondaires éventuels
- Les groupes associés à un utilisateur sont utilisés pour les contrôles d'accès
- Changement de groupe courant :
  - automatique sous BSD et System V récent
  - commande **newgrp** sous les vieux System V

Fichier /etc/group

- Définition des groupes et des utilisateurs associés
- Chaque ligne contient :
  - le nom du groupe (unique)
  - le mot de passe chiffré (utilisé par **newgrp** sur certains systèmes)
  - le numéro du groupe (GID) entre 0 et 32767
  - la liste des utilisateurs du groupe qui n'ont pas ce groupe par défaut.

Ces champs (dans cet ordre) sont séparés par des " :"
Pas de commentaires possibles

Format du fichier /etc/group

```
groupe :mot-de-passe :gid :liste
```

Exemple

```
wheel:*:0:root,card,dntt
staff:*:10:root,card
users:*:1000:
```

Sur certains systèmes (BSD), seul les utilisateurs déclarés dans le groupe 0 (wheel) ont le droit d'utiliser la commande **su**.

Fichier /etc/shells

Sur les systèmes Berkeley, /etc/shells liste les shells valide sur le système.
Utilisé par certains programmes comme par **chsh** et **ftpd**.

```
/bin/sh
/bin/csh
/usr/bin/ksh
/usr/local/bin/bash
```

Le fichier /etc/shadow

- Le fichier /etc/passwd est en lecture pour tous
- Le mot de passe chiffré n'est pas déchiffrable ...
- ... mais une attaque brutale à base de dictionnaires peut aboutir (exemple : Crack)
- Sous certains systèmes, la liste des utilisateurs est décomposée en deux fichiers :
  - /etc/passwd (sans mots de passe) lisible par tous
  - /etc/shadow ou /etc/master.passwd (avec mots de passe) lisible par 'root' uniquement

```
root:x:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:x:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:x:1002:1000:Remy CARD:/users/card:/bin/csh
```

Le fichier /etc/shadow (System V)

Chaque ligne contient :

- le nom de l'utilisateur
- le mot de passe chiffré
- la date du dernier changement de mot de passe
- le nombre minimum de jours entre deux changements du mot de passe
- le nombre maximum de jours de validité du mot de passe
- le nombre de jours avant l'expiration du mot de passe à partir duquel l'utilisateur est averti
- le nombre de jours pendant lesquel le compte peut être inutilisé
- la date d'expiration du compte
- un champ 'réservé'

(masque appliqué à /etc/passwd pour les informations complémentaires confidentielles)

Le fichier /etc/shadow (System V)

Fichier /etc/shadow (non lisible par les utilisateurs)

```
root:$1$8ofzSt0:12982:0:99999:7:::
daemon:*:12957:0:99999:7:::
webmaster:*:13080:0:99999:7:::
dntt:$1$4w/jIYh/aXv:12977:0:99999:7:::
card:$4HUcta/uYY:13140:28:30:7:14::
```

Fichier /etc/passwd (lisible par tous les utilisateurs)

```
root:x:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:x:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:x:1002:1000:Remy CARD:/users/card:/bin/csh
```

Rq : les dates se font nombre de jours écoulés depuis le 1er janvier 1970

Fichier /etc/master.passwd sous FreeBSD

- Chaque ligne contient :
  - le nom de l'utilisateur
  - le mot de passe chiffré
  - le numéro d'utilisateur (uid)
  - le numéro de groupe d'utilisateurs (gid)
  - la classe d'utilisateur (défini dans /etc/login.conf pour le paramétrage de son environnement.
  - la date du dernier changement de mot de passe : si vide, pas de gestion de durée de validité des mots de passe
  - la date d'expiration du compte : si vide, pas de gestion de durée de validité des mots de passe
  - le nom complet de l'utilisateur
  - le répertoire d'accueil
  - le shell

(informations complètes d'où est extrait le fichier /etc/passwd)

Fichier /etc/master.passwd sous FreeBSD

Fichier /etc/master.passwd (non lisible par les utilisateurs)

```
root:$1$8ofzSt0:0:0::0:0:Le chef:/root:/bin/sh
daemon:*:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster*:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:$1$4w/IYh/aXv:1001:1000::0:0:Tuyet Tram DANG NGOC:/users/dntt:/usr
card:$4HUcta/uYY:1002:1000:xuser:13140:13168:Remy CARD:/users/card:/bin
```

Fichier /etc/passwd (lisible par tous les utilisateurs)

```
root:x:0::Le chef:/root:/bin/sh
daemon:x:1:1:Le demon:/usr/sbin:/usr/sbin/nologin
webmaster:x:80:500:Maitre de la toile:/local/web/www:/usr/sbin/nologin
dntt:x:1001:1000:Tuyet Tram DANG NGOC:/users/dntt:/usr/bin/ksh
card:x:1002:1000:Remy CARD:/users/card:/bin/csh
```

Rq : les dates se font nombre de jours écoulés depuis le 1er janvier 1970

Modification des informations sur un utilisateur

- Changement de mot de passe : **passwd**
- Changement de GECOS : **chfn**
- Changement du shell : **chsh**
- Changement des informations : **chpass**
- Modification de `/etc/passwd` et `/etc/shadow` : **passmgmt** ou **pw**

Modification de la liste d'utilisateurs (ajout, suppression, modification)

Édition du fichier `/etc/passwd` : **vipw**

- Vérification de `/etc/passwd` : `pwck` (linux)
- Vérification de `/etc/group` : `grpck` (linux) ou `chkgrp` (FreeBSD)
- Conversion du fichier `/etc/shadow` :
  - **pwconv**
  - **pwunconv**
- **mkpasswd** (linux) : chiffrement du mot de passe
- Création des fichiers hachés : **pwd_mkdb** (FreeBSD) : Génération de `/etc/pwd.db`

Création d'un utilisateur en 10 points

1. Choisir le groupe (GID) auquel appartiendra l'utilisateur
2. Choisir le répertoire par défaut (maison)
3. Choisir un login unique
4. Demander à l'utilisateur son shell par défaut pris dans `/etc/shells`
5. Ajouter la ligne regroupant ces informations dans `/etc/passwd` en mettant '*' comme mot de passe chiffré
6. Créer le répertoire maison de l'utilisateur : **mkdir repertoire**
7. Rendez l'utilisateur propriétaire de son répertoire maison : **chown utilisateur repertoire**
8. Rendez le groupe propriétaire du répertoire maison : **chgrp groupe repertoire**
9. Utiliser **passwd** pour initialiser son mot de passe.
10. Créer éventuellement quelques fichiers d'initialisation (`.profile`, `.bashrc`, ...

Suppression d'un utilisateur

- Invalidation du compte :
  - remplacement du mot de passe chiffré par '*' ou '**No Login**'
  - remplacement du shell par `/bin/false`
- Suppression effective :
  - (archivage +) suppression du répertoire d'accueil
  - (archivage +) suppression de tous les fichiers de l'utilisateur :
    - mailbox
    - crontab
    - etc ...
  - suppression dans `/etc/passwd` (et dans `/etc/group` éventuellement)

Droits des utilisateurs

Le système interdit un certain nombre d'opérations, par exemple :

- l'accès à un fichier pour lequel les droits sont insuffisants
- l'envoi d'un signal à un processus appartenant à un autre utilisateur
- le changement de valeur « système » : priorité d'un processus, ou nouvelle identité pour un processus
- actions affectant l'ensemble des utilisateurs :
  - ajout ou suppression de disques
  - changement de l'heure
  - changement du nom de la machine, de ses paramètres réseaux

En cloisonnant ainsi les droits sur les fichiers et les processus (chaque utilisateur ne peut modifier que ce qui lui appartient), on a une bonne sécurité et on évite les conflits.

Pour gérer la machine (ajouter un disque, sauvegarder tous les répertoire, terminer un processus indésirable, supprimer un utilisateur), il faut des droits qui permettent de s'affranchir de toutes les restrictions.

root : le super-utilisateur

- Une erreur en tant qu'utilisateur normal est limitée (au pire, on ne détruit que ses propres informations).
- Une erreur en tant que root peut être fatale pour tout le système et l'ensemble des utilisateurs..

> « Un grand pouvoir implique de grandes responsabilités »
>
> *Peter Parker (alias Spiderman)*

Règles de base sur le compte root.

1. Il faut utiliser le moins possible le compte root
2. Il faut minimiser l'ensemble des personnes qui peuvent utiliser le compte root
3. Le choix du mot de passe du compte root est crucial

Le compte 'root'

- Unix surveille le comportement de tous les utilisateurs ...
- ... sauf 'root' qui a tous les droits

Connexion sous 'root' :

- pour acquérir les droits de root : se déconnecter en tant qu'utilisateur normal puis se connecter sur le compte root (fastidieux)
- connexion normale (login) : déconseillée (double sécurité).
- D'abord se connecter en tant qu'utilisateur normal, puis utiliser :
  - **su** permet de prendre l'identité d'un autre utilisateur, par génération d'un shell lancé sous l'identité de l'autre utilisateur. Utilisé sans argument on prend l'identité de root (après mot de passe). Il est recommandé d'utiliser **su** - pour provoquer l'exécution du vrai shell de root.
  - **sudo**, **calife**, ... permet de donner les droits sur certaines commandes d'administration à certains utilisateurs (avec traçage, limitation, restrictions plus ou moins paramétrables)

Quelques règles sur le compte root

- le compte root ne doit pas avoir . dans son PATH
- le compte root doit avoir une valeur de umask de 022
- avoir un répertoire maison sur la partition contenant la racine
- aucun des fichiers de configuration de root ne doit être modifiable par un autre utilisateur

Bit set-user-id

Motivation : pour changer son mot de passe, on utilise la commande passwd qui permet de modifier le fichier /etc/passwd.
Or /etc/passwd appartient à root et l'utilisateur normal n'a pas le droit (heureusement) de le modifier.
bit set-user-id sur les fichiers indique que la commande prend les droits du propriétaire du fichier (ici root) et non les droits de celui qui lance le programme.
$

Plusieurs commandes utilisent le bit set-user-id : **chfn**, **chpass**, **chsh**, **su**, **lpr**, **login**, **ping**, etc.
Mais, il faut utiliser le bit set-user-id avec parcimonie et dicernement (faille de sécurité possible) et surtout pas dans des scripts shells.

Bit set-user-id

Motivation : pour changer son mot de passe, on utilise la commande passwd qui permet de modifier le fichier /etc/passwd.
Or /etc/passwd appartient à root et l'utilisateur normal n'a pas le droit (heureusement) de le modifier.
bit set-user-id sur les fichiers indique que la commande prend les droits du propriétaire du fichier (ici root) et non les droits de celui qui lance le programme.

```
$ ls -als /usr/bin/passwd
```

Plusieurs commandes utilisent le bit set-user-id : **chfn**, **chpass**, **chsh**, **su**, **lpr**, **login**, **ping**, etc.
Mais, il faut utiliser le bit set-user-id avec parcimonie et dicernement (faille de sécurité possible) et surtout pas dans des scripts shells.

Bit set-user-id

Motivation : pour changer son mot de passe, on utilise la commande passwd qui permet de modifier le fichier /etc/passwd.
Or /etc/passwd appartient à root et l'utilisateur normal n'a pas le droit (heureusement) de le modifier.
bit set-user-id sur les fichiers indique que la commande prend les droits du propriétaire du fichier (ici root) et non les droits de celui qui lance le programme.

```
$ ls -als /usr/bin/passwd
-r-sr-xr-x 2 root wheel 6052 8 mai 2005
/usr/bin/passwd
$
```

Plusieurs commandes utilisent le bit set-user-id : **chfn**, **chpass**, **chsh**, **su**, **lpr**, **login**, **ping**, etc.
Mais, il faut utiliser le bit set-user-id avec parcimonie et dicernement (faille de sécurité possible) et surtout pas dans des scripts shells.

Utilisateurs spéciaux

Un certain nombre de comptes sur le système sont des comptes spéciaux.

- root : le super-utilisateur (uid = 0) : tout utilisateur d'UID nul est administrateur. L'usage veut qu'il s'appelle root

Les utilisateurs fictifs (souvent des comptes créé par défaut sans possibilité de login).

- Servent de propriétaire de fichiers (pour impliquer root au minimum)
- Il est déconseillé de les modifier
- Ils prennent souvent des GID en dessous de 1000, il est déconseillé de faire les comptes utilisateurs en dessous de 1000.

Exemple d'utilisateurs fictifs fréquents

- daemon : utilisateur fictif des démons
- bin : propriétaire de `/bin` et de `/usr/bin`
- sys : utilisateur système (System V)

Commandes d'administration

- Les commandes pour les utilisateurs sont contenues dans les répertoires `/bin` et `/usr/bin`
- Il existe des répertoires spécifiques pour les commandes d'administration :
  - `/sbin`
  - `/usr/sbin`
  - `/etc`
  - `/usr/etc`
- Les fichiers de configuration du système sont généralement placés dans le répertoire `/etc`