Chapitre 9
Les droits des utilisateurs

1. Gérer les utilisateurs

La gestion des droits est un point crucial de l'administration de votre système d'exploitation Ubuntu. Elle est fortement liée au système de fichiers (car rappelez-vous qu'Unix est construit autour des systèmes de fichiers) et c'est pourquoi vous trouvez ici beaucoup de manipulations en mode console.

Une erreur dans les droits et c'est toute la sécurité de votre installation qui est en jeu.

1.1 Principe

1.1.1 Linux en général

Les utilisateurs sont référencés par :

- Un **login**, ou nom de connexion.
- Un **UID** (*User ID*), identifiant numérique unique de l'utilisateur, codé sur 32 bits.
- Un **GID** (*Group ID*), identifiant du groupe principal auquel appartient l'utilisateur.
- Divers autres groupes secondaires.

Ces informations sur votre compte utilisateur sont obtenues avec la commande ID. Dans l'exemple ci-dessous, l'utilisateur eni a comme uid 1000 et comme gid 1000. Il fait partie d'un grand nombre de groupes.

```
$ id
uid=1000(eni) gid=1000(eni)
groupes=1000(eni),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),10
9(lpadmin),124(sambashare)
```

Les utilisateurs ont des droits sur tout ce qui leur appartient et sur ce qui appartient à leurs groupes.

Une commande est exécutée avec les droits de l'utilisateur.

Les informations sur les comptes locaux sont stockées dans **/etc/passwd** et **/etc/shadow**. Les groupes sont dans **/etc/group** et **/etc/gshadow**.

Le mot de passe, crypté, est le deuxième champ de chaque ligne du fichier **/etc/shadow**. Seul l'administrateur peut lire le contenu de ce fichier.

L'administrateur du système est appelé **root** et porte toujours l'uid 0. Il est le seul, sauf mécanismes spécifiques, à pouvoir exécuter les tâches administratives les plus importantes.

Pour passer root, un utilisateur peut utiliser la commande su. Il saisit le mot de passe root et devient celui-ci. En fermant le shell root il reprend ses droits par défaut.

```
$ su
Mot de passe : xxxxxxxx
#
```

1.1.2 Ubuntu en particulier

À moins d'avoir installé Ubuntu en mode expert, vous avez remarqué que :

– à aucun moment vous n'avez saisi le mot de passe du compte root.

– un seul compte, le vôtre, a été créé, et qu'il dispose de droits particuliers.

Ce mécanisme utilise les droits sudo. C'est une fonctionnalité d'Unix qui permet de donner des droits supplémentaires à des utilisateurs, sur tout le système ou des commandes en particulier.

Le compte que vous avez créé lors de l'installation dispose de ces droits : ils lui permettent d'utiliser toutes les commandes en tant qu'administrateur, à condition de les faire précéder de la commande `sudo` et de saisir son mot de passe :

```
$ sudo apt update
[sudo] password for eni:
```

Pour rester root, ce qui est plus pratique si vous avez beaucoup de commandes à taper, tapez :

```
$ sudo -i
#
```

Ubuntu a donc une politique des droits plus restrictive que les autres distributions Linux :

– L'utilisateur courant ne doit pas avoir accès aux fichiers et processus du système et ne peut pas les modifier.
– Le compte root est désactivé car il est trop dangereux pour une utilisation courante du système.

Personne n'est à l'abri d'une mauvaise manipulation aux conséquences très graves. Pour utiliser LibreOffice, écouter de la musique, surfer sur le Web et envoyer des mails, nul besoin d'être root.

Si vos actions nécessitent une action de l'administrateur, Ubuntu demandera votre mot de passe et les commandes associées seront jouées par sudo.

1.1.3 Rétablir le compte root

Il ne faut pas élever la règle de l'utilisation de `sudo` à un rang de dogme. Si elle est plus sécurisante, elle devient vite ennuyeuse, notamment si vous devez configurer un serveur ou utiliser temporairement un grand nombre de commandes. Dans ce cas, deux solutions :

– Faites un `sudo -i`.
– Rétablissez le compte root.

Pour rétablir le compte root, il suffit de lui donner un mot de passe.

```
$ sudo passwd root
[sudo] password for eni:
```

```
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
```

Vous pouvez alors vous connecter en tant que root ou taper la commande `su` (sans passer par sudo) : saisissez le mot de passe que vous lui avez donné.

Pour annuler cette action, vous devez verrouiller le compte. Cette commande ajoute un point d'exclamation devant le mot de passe crypté de root dans **/etc/shadow**.

```
$ sudo passwd -l root
```

Même root rétabli, toutes les actions effectuées par sudo via la console ou l'interface continuent de demander votre mot de passe et pas celui de root. Pour demander le mot de passe de root, faites ceci :

Éditez **/etc/sudoers** avec `visudo`.

```
$ sudo visudo
```

- Modifiez la ligne suivante comme ceci :

```
Defaults        env_reset,rootpw
```

- Sauvegardez le fichier.

1.2 Les fichiers

1.2.1 /etc/passwd

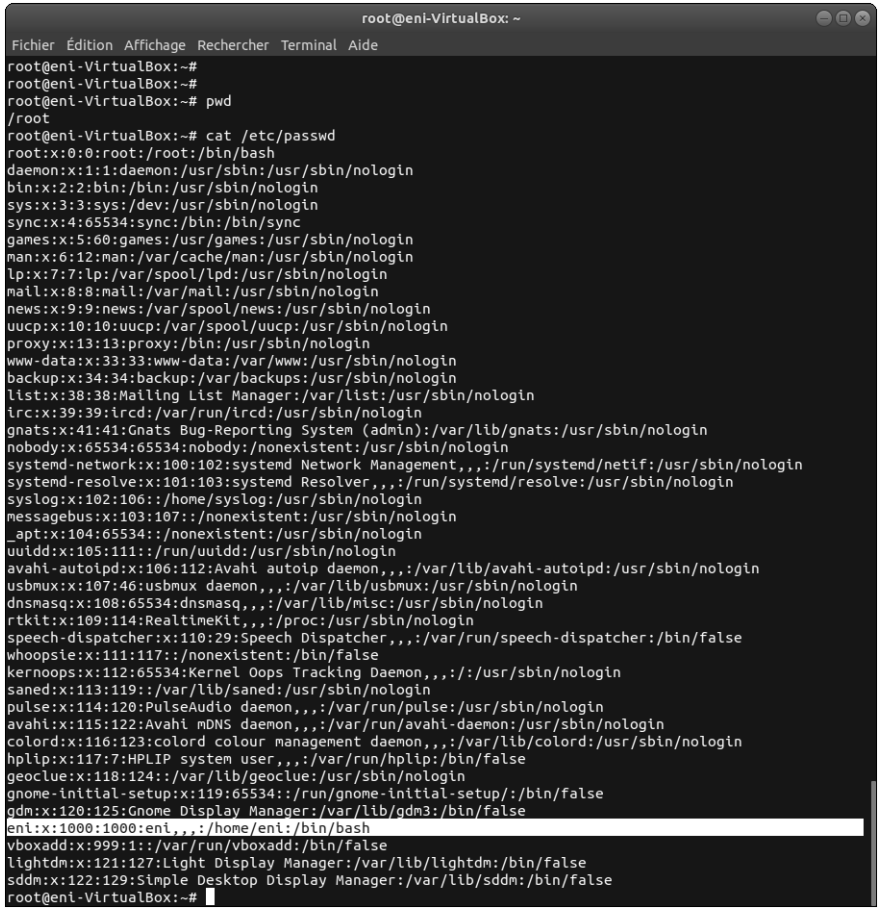
Le fichier **/etc/passwd** contient la liste des utilisateurs du système local. Il est lisible par tout le monde. Les informations qu'il contient sont publiques et utiles tant pour le système que pour les utilisateurs. Chaque ligne représente un utilisateur et est composée de sept champs.

```
login:password:UID:GID:comment:homedir:shell
```

– Champ 1 : le login ou nom d'utilisateur.

– Champ 2 : sur les vieilles versions, le mot de passe crypté. Actuellement, 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.

– Champ 3 : le User ID.
– Champ 4 : le GID, c'est-à-dire le groupe principal.
– Champ 5 : un commentaire ou descriptif. C'est un champ d'information qui contient souvent le prénom et le nom de l'utilisateur, mais qui peut contenir autre chose.
– Champ 6 : le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte.
– Champ 7 : le shell par défaut de l'utilisateur. Mais ce peut être toute autre commande, y compris une commande interdisant la connexion.



1.2.2 /etc/group

Le fichier **/etc/group** contient la définition des groupes d'utilisateurs et pour chacun, la liste des utilisateurs dont il est le groupe secondaire. Chaque ligne est composée de quatre champs :

```
group:password:GID:user1,user2,...
```

– Champ 1 : le nom du groupe.
– Champ 2 : le mot de passe associé. Voyez l'explication ci-après.
– Champ 3 : le Group ID.
– Champ 4 : la liste des utilisateurs appartenant à ce groupe.

Il est inutile de replacer dans le quatrième champ les utilisateurs ayant ce groupe pour groupe principal, c'est induit.

Vous pouvez être surpris de voir la présence d'un champ de mot de passe pour les groupes. Il est peu utilisé. Un utilisateur a le droit de changer de groupe afin de prendre, temporairement tout du moins, un groupe secondaire comme groupe principal avec la commande `newgrp`.

L'administrateur peut mettre en place un mot de passe sur le groupe pour protéger l'accès à ce groupe en tant que groupe principal.

1.2.3 /etc/shadow

C'est là que sont stockés, entre autres, les mots de passe cryptés des utilisateurs. Il contient toutes les informations sur les mots de passe et leur validité dans le temps. Chaque ligne est composée de 9 champs séparés par des « : » :

```
bean:$2a$10$AjADxPEfE5iUJcltzYA4wOZO.f2UZ0qP/8EnOFY.P.m10HifS7J8i:
15141:0:99999:7:::
```

– Champ 1 : le login.
– Champ 2 : le mot de passé crypté. Le xx initial indique le type de cryptage.
– Champ 3 : nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
– Champ 4 : nombre de jours avant lesquels le mot de passe ne peut pas être changé (0 : il peut être changé n'importe quand).

– Champ 5 : nombre de jours après lesquels le mot de passe doit être changé.
– Champ 6 : nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
– Champ 7 : nombre de jours, après l'expiration du mot de passe, après lesquels le compte est désactivé.
– Champ 8 : nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
– Champ 9 : réservé.

Dans l'exemple de la ligne bean, le mot de passe a été changé 15141 jours après le 01/01/1970. Le mot de passe doit être changé avant 0 jour mais il est toujours valide car le champ suivant indique qu'il faut le changer au bout de 99999 jours (273 ans) et le champ 5 est vide (pas d'obligation de changement de mot de passe). Le compte est désactivé après 7 jours, ce qui évidemment ne risque pas d'arriver…

Les valeurs courantes pour le cryptage des mots de passe sont les suivantes :

– 1 : MD5
– $2a$: Blowfish
– $5 : SHA-256
– $6 : SHA-512
– Autre : DES

Pour connaître la date en fonction du 01/01/1970, utilisez la commande `date` comme ceci, en ajoutant le nombre de jours désiré :

```
$ date --date "1 jan 1970 +15141days"
jeu. juin 16 00:00:00 CEST 2011
```

1.2.4 /etc/gshadow

Le fichier **/etc/gshadow** est le pendant du fichier précédent mais pour les groupes. Sa syntaxe est la suivante :

```
groupe:password:admins:members
```