Sommaire

Gestion des utilisateurs et des groupes

Introduction

Pour utiliser une système GNU/Linux, il faut se connecter, pour cela l'utilisateur s'authentifie en fournissant un nom de connexion (*login name*) et un mot de passe (*password*). Si la connexion réussie, l'utilisateur a normalement un *shell* et se trouve positionné dans l'arborescence dans son répertoire de connexion (*working directory*).

Les informations relatives à l'authentification sont stockées dans des fichiers ASCII du répertoire **`/etc`** :

- L'ensemble des informations caractérisant un utilisateur sont définis dans le fichier `/etc/passwd`
- Des groupes d'utilisateurs sont définis dans le fichier `/etc/group`
- Les mots de passe cryptés sont stockés dans un fichier séparé `/etc/shadow`
- des fichiers complémentaires sont situés dans `/etc/security/`

Les fichiers de base

Le fichier /etc/passwd est un fichier ASCII dont chaque ligne définit un compte utilisateur. Une ligne est composé de champs délimités par le symbole ':' :

```
nom de connexion:mot de passe:UID:GID:commentaire:répertoire de
connexion:commande de connexion
```

Remarque : le champ 'commande de connexion' précise le chemin absolu de la commande à exécuter lors de la connexion. C'est généralement un shell (/bin/bash).

Le fichier /etc/group est un fichier ASCII dont chaque ligne définit un groupe d'utilisateurs. Une ligne est composé de champs délimités par le symbole ':' :

```
nom du groupe:mot de passe:GID:liste des utilisateurs autorisés
à se connecter au groupe
```

Remarque : le champ 'mot de passe' permet de demander à un utilisateur qui veut se connecter au groupe et qui ne figure pas dans la liste des utilisateurs du groupe (rarement utilisé dans la pratique)

La commande newgrp permet de changer le groupe de référence utilisé lors de la création de nouveaux fichiers.

Quelques commandes d'administration

```
useradd, usermod, userdel : gestion des comptes utilisateurs
groupadd, groupmod, groupdel : gestion des groupes
pwck, grpck : vérification des fichiers /etc/passwd et
/etc/group
finger : informations sur un utilisateur
chfn, chsh : changement de shell ou de commentaire d'un
utilisateur
passwd : modification du mot de passe d'un utilisateur
su, sudo : exécution d'un shell de connexion sous un autre
compte
id : informations sur l'identité d'un compte
groups : liste des groupes d'un utilisateur
vipw, vigr : édition des fichiers /etc/passwd et /etc/group en
les verrouillant
getent : affiche des données (passwd, group, ...)
d'administration
chage : permet de modifier les attributs sur la pérennité du mot
de passe
```

Mécanisme d'authentification

Tout d'abord, il faut distinguer les deux situations suivantes :

- la 'base de données' des comptes est locale à la machine : fichiers locaux (/etc/passwd, ...)
- la 'base de données' des comptes est distante, on utilise habituellement : NIS (les yellow pages) ou LDAP (système d'annuaire) pour exporter les comptes de la machine distante

Le système permet de configurer cette situation (où chercher la 'base de données' des comptes ?) par l'intermédiaire de NSS (*Name Service Switch*, commutateur de services de nommages) dans un fichier /etc/nsswitch.conf :

```
passwd:     files ldap nisplus nis
shadow:     files ldap nisplus nis
group:      files ldap nisplus nis
hosts:      files nis dns
```

Si on regarde le fonctionnement d'une machine, on s'aperçoit qu'il y a de nombreux programmes qui nécessitent un service d'authentification (login, rlogin, su, xdm, ...). Pour éviter que chaque programme n'est à écrire sa propre authentification, il est possible d'utiliser une bibliothèque adaptée. On parle alors de SSO (*Single Sign-On*, authentification unique).

C'est ce que propose PAM (*Pluggable Authentication Modules*, modules d'authentification enfichables) qui permettent de paramétrer à l'envie les procédures et sources d'authentification, mais aussi d'offrir des services supplémentaires aux programmes qui savent les utiliser. Chaque programme peut alors décrire son utilisation de PAM en paramétrant un fichier portant son nom dans /etc/pam.d/.

En résumé : Le service PAM est donc une API (disponible sous formes de bibliothèques dynamiques) utilisée par des programmes pour construire leur service d'authentification. L'administrateur pourra adapter et modifier les règles et les méthodes d'authentification (sans toucher aux programmes).

Remarque : il existe aussi des serveurs d'authentification externes sécurisés : Kerberos, SASL (Simple Authentication and Security Layer).

Automatisation

L'administrateur automatisera la création d'utilisateurs et de groupes :

- en écrivant un script qui saura utiliser des données externes en provenance d'une base de données, d'un tableur, ...)
- en paramétrant le répertoire /etc/skel qui contient les fichiers qui sont automatiquement ajoutés dans le répertoire de connexion d'un nouvel utilisateur