Le système GNU/Linux étant multiutilisateur, les personnes employant celui-ci doivent être identifiées afin d'assurer la confidentialité des informations contenues dans les fichiers. En effet, il ne serait pas acceptable que l'utilisateur "Nicolas" puisse en toute impunité consulter les fichiers personnels de "Stéphane" sans l'accord de ce dernier.

Ces personnes posséderont donc chacune un "compte utilisateur" sur le système pour l'employer en étant clairement identifiées.

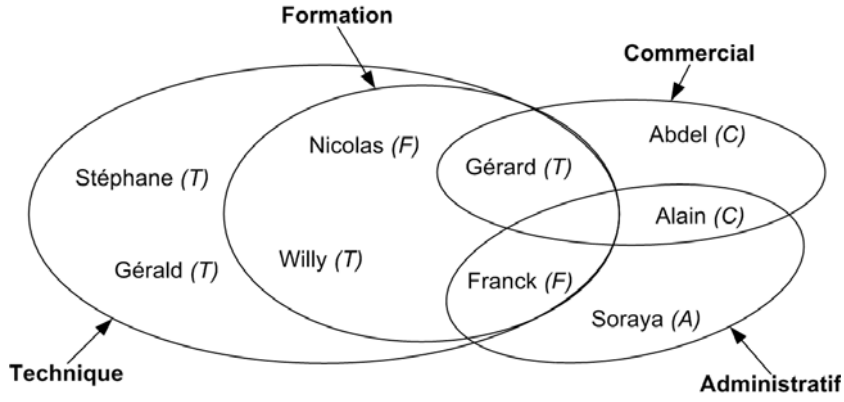
Cependant, il est heureusement permis de partager des fichiers entre collaborateurs et une notion de "groupe d'utilisateurs" existe sous GNU/Linux.

A. Concepts de comptes utilisateur et de groupes

Un utilisateur devra obligatoirement être membre d'un groupe d'utilisateurs sur un système Unix comme GNU/Linux : son groupe principal sera utilisé lors de la création des fichiers.

Par contre, il pourra éventuellement appartenir à plusieurs autres groupes : ses groupes secondaires détermineront ses droits d'accès aux fichiers créés par d'autres membres de ces groupes.

Par exemple, si l'on représente les différents services d'une société avec leurs personnels, bien que chaque individu ait une fonction première (indiquée entre parenthèses), certains peuvent avoir plusieurs missions.



On voit ici que :

- Stéphane et Gérald appartiennent tous les deux au service technique.
- Nicolas, qui est avant tout formateur, fait aussi partie du service technique.
- Willy, appartenant au service technique principalement, travaille aussi dans le service formation.
- Franck est un formateur qui collabore avec les services technique et administratif.
- Gérard, du service technique, offre ses compétences aux services commercial et formation.

- Alain est un commercial qui s'acquitte aussi de tâches administratives.
- Soraya fait uniquement partie du service administratif.
- Abdel n'appartient qu'au service commercial.

Pour les exemples suivants, nous considérons que les comptes **franck** et **nicolas** correspondant respectivement aux utilisateurs Franck et Nicolas ainsi que le groupe **formation** correspondant au service Formation existent déjà.

Pour identifier tous ces utilisateurs au niveau du système d'exploitation, un numéro unique leur sera attribué : l'UID (*User's ID*) ; le propriétaire d'un fichier est déterminé par ce numéro sous Unix. Ces utilisateurs seront aussi dotés d'un nom d'utilisateur unique (*login*) et d'un mot de passe (*password*) pour qu'ils puissent s'authentifier lors de leur connexion au système.

De la même manière, les groupes d'utilisateurs seront représentés par un nom unique auquel sera associé un identifiant numérique : le GID (*Group's ID*). Ce dernier sera aussi utilisé pour déterminer le groupe propriétaire d'un fichier.

B. Hiérarchie des utilisateurs

Les utilisateurs, et par conséquent les comptes utilisateur, ne sont pas tous égaux sous Unix. On peut distinguer trois types de comptes :

- **root** : c'est l'utilisateur le plus important du système du point de vue de l'administration. Il n'est pas concerné par les droits d'accès aux fichiers et peut faire à peu près tout sur le système, sauf écrire sur un système de fichiers monté en lecture seule (CD-Rom). Son UID égal à 0 lui confère sa spécificité. Ce "superutilisateur" aura donc à sa charge les tâches d'administration du système. Pour éviter toute erreur de manipulation, il est fortement conseillé de réserver le compte d'administration aux tâches nécessitant les droits du superutilisateur.
- **bin, daemon, sync, www-data...** : on trouvera sur le système toute une série de comptes qui ne sont pas affectés à des personnes physiques. Ceux-ci servent à faciliter la gestion des droits d'accès de certaines applications et démons. Ainsi, en lançant le serveur Web sous l'identité du compte **www-data**, on pourra aisément limiter ses droits d'accès à certains fichiers. D'une manière générale, on ne lance jamais un service exposé aux attaques réseau comme un serveur Web sous l'identité de **root**. Sinon, quelqu'un de mal intentionné qui réussirait à exploiter une faille de sécurité du logiciel obtiendrait automatiquement les droits d'administration. Toujours pour des raisons de sécurité, on fera en sorte que personne ne puisse se connecter à la machine à partir de l'un de ces comptes. Les UID compris entre 1 et 999 sont généralement utilisés pour ces comptes.
- **franck, nicolas...** : tous les autres comptes utilisateur sont associés à des personnes réelles ; leur vocation est de permettre à des utilisateurs standard de se connecter et d'utiliser les ressources de la machine. L'UID d'un utilisateur sera normalement un nombre supérieur ou égal à 1000.

À l'instar des comptes utilisateur, il existe différents types de groupes sur un système GNU/Linux permettant de donner des droits communs à un ensemble d'utilisateurs :

- **root** : son GID est 0 et c'est le groupe principal de l'administrateur.
- **bin**, **daemon**, **www-data...** : ces groupes jouent le même rôle que les comptes du même nom et permettent de donner les mêmes droits d'accès à un ensemble d'applications. Par convention, les groupes système auront un GID compris entre 1 et 1000.
- **formation...** : ces groupes représentent un ensemble de personnes réelles devant accéder aux mêmes fichiers. Typiquement, ils auront un GID supérieur ou égal à 1000.

1. Connexion

a. Console graphique

Lorsque le système est installé en poste de bureau, le dernier programme exécuté par le processus Init est le gestionnaire de connexion graphique. Son rôle est de lancer le système X Window sur la console graphique et d'authentifier l'utilisateur qui veut s'y connecter.

Plusieurs gestionnaires de connexion graphique sont disponibles sous Debian Sarge :

X Display Manager

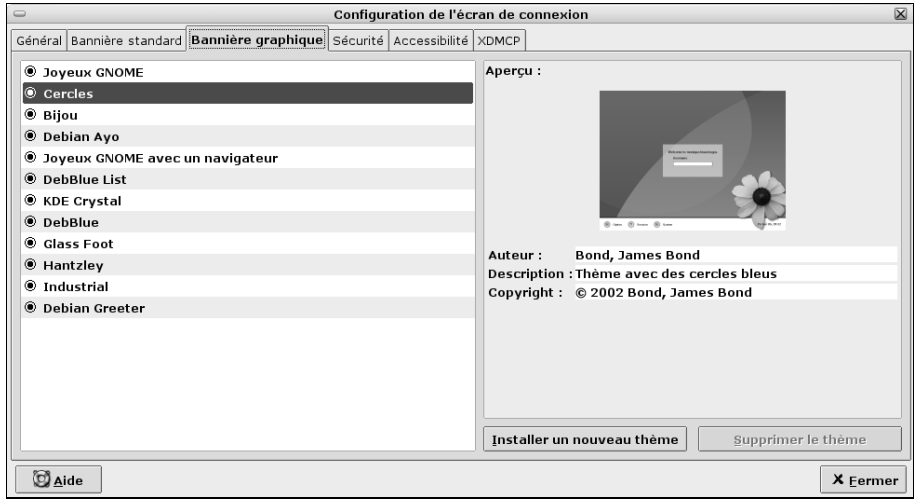
La commande **xdm** qui est fournie avec le système X Window propose l'écran de connexion suivant :

Son fichier de configuration est */etc/X11/xdm/xdm-config* (ou */usr/X11R6/lib/X11/xdm/xdm-config* si celui-ci n'existe pas).

GNOME Display Manager

Sous Debian Sarge, le gestionnaire de connexion graphique par défaut est GDM (*GNOME Display Manager*) dont le fichier binaire est **gdm** :

L'interface de ce programme est paramétrable en modifiant directement son fichier de configuration */etc/X11/gdm/gdm.conf* ou en utilisant la commande **gdmsetup** :



KDE Display Manager

C'est le pendant de XDM pour l'environnement de bureau KDE :

Son fichier de configuration est */etc/kde3/kdm/kdmrc*. Il est possible de modifier la configuration de **kdm** via le centre de contrôle KDE disponible dans cet environnement graphique.

Si plusieurs gestionnaires de connexion sont installés, il est possible de définir celui qui est utilisé par défaut en reprenant la configuration de n'importe quel paquet Debian qui contient un de ces gestionnaires de connexion graphique. Par exemple, en reprenant la configuration de **xdm** via la commande "**dpkg-reconfigure xdm**" nous arrivons à l'écran de configuration suivant :

b. Terminaux texte

Sur un terminal texte, le programme permettant de se connecter à un système GNU/Linux s'appelle **login**. Il est facilement configurable en modifiant certaines directives du fichier */etc/login.defs*.

Les seuls terminaux auxquels pourra se connecter l'administrateur seront indiqués dans le fichier */etc/securetty*. Debian Sarge utilisant PAM (*Pluggable Authentication Modules*), il est aussi possible de modifier le comportement de la commande **login** avec le fichier */etc/pam.d/login*.

Changement d'identité

Une fois connecté, il est possible de changer d'identité ou plus exactement de lancer un nouveau shell avec un autre UID. La commande utilisée pour cela est **su** (*Substitute User identity*) suivie du nom d'utilisateur sous lequel doit être lancé le nouveau shell ; si aucun nom n'est mentionné, le nom **root** sera utilisé par défaut.

Invoquée sans option, la commande **su** lancera le shell indiqué dans la variable **SHELL** et certaines variables d'environnement comme **PATH** et **MAIL** resteront inchangées. Pour remédier à cela et charger l'environnement de l'utilisateur "cible", l'option **-** (ou **-l**, ou **--login**) est utilisée :

```
Login: nicolas
Password: <le mot de passe n'est pas affiché>

[nicolas]$ echo $MAIL
/var/mail/nicolas
[nicolas]$ su franck
Password: <le mot de passe n'est pas affiché>
[franck]$ echo $MAIL
/var/mail/nicolas
[franck]$ exit
exit
[nicolas]$ su - franck
Password: <le mot de passe n'est pas affiché>
[franck]$ echo $MAIL
/var/mail/franck
[franck]$ su -
Password: <le mot de passe n'est pas affiché>
[root]#
```