Chapitre 7
Droits d'accès aux fichiers

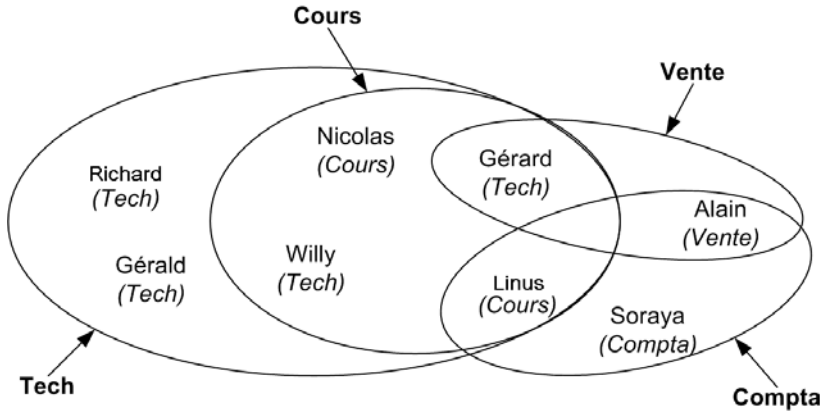
1. Concepts de comptes utilisateur et de groupes

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 consulter les fichiers personnels de "Richard" sans l'accord de ce dernier.

Ces personnes possèdent donc chacune un "compte utilisateur" sur le système ; elles peuvent utiliser ce dernier tout en étant clairement identifiées. Cependant, il est permis de partager des fichiers entre collaborateurs et une notion de "groupe d'utilisateurs" existe sous GNU/Linux.

Un utilisateur doit obligatoirement être membre d'un groupe d'utilisateurs sur un système Unix comme GNU/Linux : c'est son groupe principal qui est utilisé lors de la création des fichiers. Par contre, il peut éventuellement appartenir à plusieurs autres groupes : ses groupes secondaires déterminent ses droits d'accès aux fichiers créés par d'autres membres des 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 assumer plusieurs missions :



On voit ici que :

– Richard et Gérald appartiennent tous les deux au service technique (Tech).
– Nicolas, qui est avant tout formateur (Cours), fait aussi partie du service technique (Tech).
– Willy, appartenant au service technique (Tech) principalement, travaille aussi dans le service formation (Cours).
– Linus est un formateur (Cours) qui collabore avec les services technique (Tech) et comptabilité (Compta).
– Gérard, du service technique (Tech), offre ses compétences au service commercial (Vente).
– Alain est un commercial (Vente) qui s'acquitte aussi de tâches administratives (Compta).
– Soraya fait uniquement partie du service comptabilité (Compta).

Pour identifier tous ces utilisateurs au niveau du système d'exploitation, un numéro unique leur est attribué : l'UID (*User ID*) ; le propriétaire d'un fichier est déterminé par ce numéro sous Unix. Ces utilisateurs sont 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 sont représentés par un nom unique auquel est associé un identifiant numérique : le GID (*Group ID*). Ce dernier est également utilisé pour déterminer le groupe propriétaire d'un fichier.

1.1 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 pas les droits d'accès aux fichiers et peut faire à peu près tout sur le système, excepté écrire sur un système de fichiers monté en lecture seule (CD-ROM). Son UID égal à 0 lui confère sa spécificité. Ce "super-utilisateur" a donc à sa charge les tâches d'administration du système. Pour éviter toute erreur de manipulation, il est fortement conseillé d'utiliser le compte d'administration uniquement pour les tâches nécessitant les droits du super-utilisateur.

`bin`, **`daemon`**, **`sync`**, **`apache`**...

Il existe sur le système 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. Les UID compris entre 1 et 999 sont généralement utilisés pour ces comptes.

`linus`, **`nicolas`**...

Tous les autres comptes utilisateur sont associés à des personnes réelles ; leur vocation est de permettre à des utilisateurs standards de se connecter et d'utiliser les ressources de la machine. L'UID d'un utilisateur est normalement un nombre supérieur ou égal à 1 000.

Remarque

On appelle "démons" les programmes s'exécutant en tâche de fond, comme un serveur web ou un serveur d'impression.

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**, **sync**, **apache**...

Ces groupes ont 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 ont un GID compris entre 1 et 999.

cours, **tech**...

Ces groupes représentent un ensemble de personnes réelles devant accéder aux mêmes fichiers. Typiquement, ils ont un GID supérieur ou égal à 1000.

1.2 Commandes utiles

Les commandes **id** et **groups** permettent d'afficher les informations en rapport avec les groupes. La première donne l'UID de l'utilisateur, le GID de son groupe principal et les GID de tous les groupes auxquels il appartient. La seconde ne fournit que la liste complète des groupes mais accepte plusieurs noms d'utilisateurs en argument :

```
[nicolas]$ whoami
nicolas
[nicolas]$ id
uid=1000(nicolas) gid=1000(cours) groupes=1000(cours),1001(tech)
[nicolas]$ id dennis
uid=1002(dennis) gid=1001(tech) groupes=1001(tech)
[nicolas]$ groups
cours tech
[nicolas]$ groups gerard alain willy root
gerard : tech cours vente
alain : vente compta
willy : tech cours
root : root
```

2. Droits Unix

Les permissions d'accès aux fichiers déterminent les actions que peuvent entreprendre les utilisateurs.

Remarque

La majorité des problèmes d'installation, de configuration et de fonctionnement des applications sous GNU/Linux est due à des droits d'accès mal positionnés.

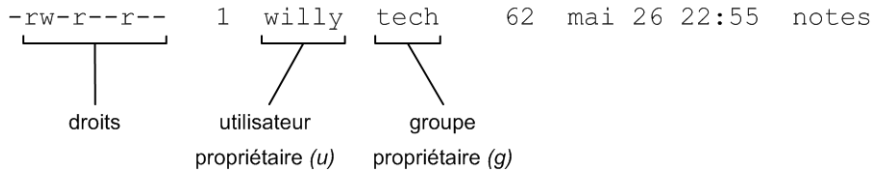
En premier lieu, il est nécessaire de savoir que les droits d'accès sous Linux sont définis pour :

– Un compte utilisateur : propriétaire du fichier, c'est en principe l'utilisateur qui a créé celui-ci.
– Un groupe : ce groupe est généralement le groupe principal du propriétaire du fichier mais peut être modifié par ce dernier et prendre la valeur d'un de ses groupes secondaires.
– Les autres : cette entité représente toute personne autre que le propriétaire et qui n'est pas membre du groupe cité précédemment.

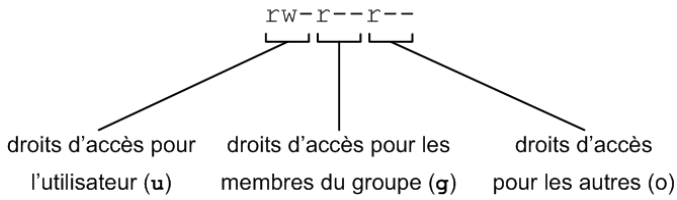
Remarque

Les droits d'accès à un fichier sont aussi appelés "modes" sous Unix.

Les droits, l'utilisateur et le groupe propriétaires d'un fichier sont affichés avec la commande **`ls -l`** :



Dans ce dernier exemple, le fichier appartient à l'utilisateur **willy** et au groupe **tech** ; les neuf caractères **rw-r--r--** définissent les droits d'accès à ce fichier pour l'utilisateur **willy** (user ou **u**), les membres du groupe **tech** (group ou **g**) et les autres (other ou **o**). Plus précisément, ces caractères sont répartis comme suit :



Tout utilisateur est donc associé à l'une de ces entités pour déterminer les permissions en vigueur.

Remarque

Attention, si l'utilisateur est propriétaire du fichier, ce sont les droits du propriétaire qui s'appliquent et non ceux du groupe, même si cet utilisateur est aussi membre de ce groupe.

La commande GNU **ls** peut ajouter un caractère supplémentaire à la suite des neuf droits Unix standards lorsque des autorisations particulières sont positionnées. Un point **.** indique alors un contexte sécurité SELinux spécifique et un **+** indique qu'une autre méthode d'autorisation telle que des ACL (*Access Control Lists*) est utilisée.

2.1 Droits standards

Les droits d'accès fondamentaux sur les fichiers et les répertoires sous Unix/Linux sont les droits de lecture **r** (*Read*), d'écriture **w** (*Write*) et d'exécution **x** (*eXecute*).

Ces droits – définis pour les entités **u**, **g** et **o** – apparaissent dans l'ordre **r**, suivi de **w**, lui-même suivi de **x** avec la commande **ls -l**. Lorsque l'un de ces caractères est remplacé par un tiret, cela signifie que le droit associé n'est pas autorisé.

Dans l'exemple du paragraphe précédent, l'utilisateur **willy** qui a les droits **rw-** :

– a le droit de lire le fichier *notes*.

– a le droit de modifier le fichier *notes*.

– n'a pas le droit d'exécuter le fichier *notes*.

De façon plus précise, on distingue les droits Unix standards selon le type de fichier : fichier ordinaire ou répertoire.

Droit	Fichier	Répertoire
r	Autorisation de lire le contenu du fichier.	Autorisation de lister les entrées du répertoire.
w	Autorisation de modifier le contenu du fichier.	Autorisation de modifier les entrées du répertoire.
x	Autorisation d'exécuter le fichier.	Autorisation d'accéder aux entrées du répertoire.

S'il est relativement simple de retenir les autorisations correspondantes lorsque ces droits sont positionnés pour un fichier ordinaire, cela devient moins évident pour un répertoire.

En considérant les répertoires comme des tableaux contenant, dans une colonne les inodes et dans une autre les noms des fichiers présents dans le répertoire, il est plus facile d'appréhender les droits standards :