

Introduction

❖ Un des rôles du système d'exploitation est d'assurer la sécurité et l'accès aux données, ce qui se fait grâce au mécanisme des **droits**.

❖ Chaque fichier se voit attribué des droits qui lui sont propres, des autorisations d'accès individuelles. Lors d'un accès le système vérifie si celui-ci est permis.

UID: User Identifier

- A sa création par l'administrateur, un utilisateur se voit affecté un **UID** (« User Identifier») unique.
- Les utilisateurs sont définis dans le fichier **/etc/passwd**.

GID: Group Identifier

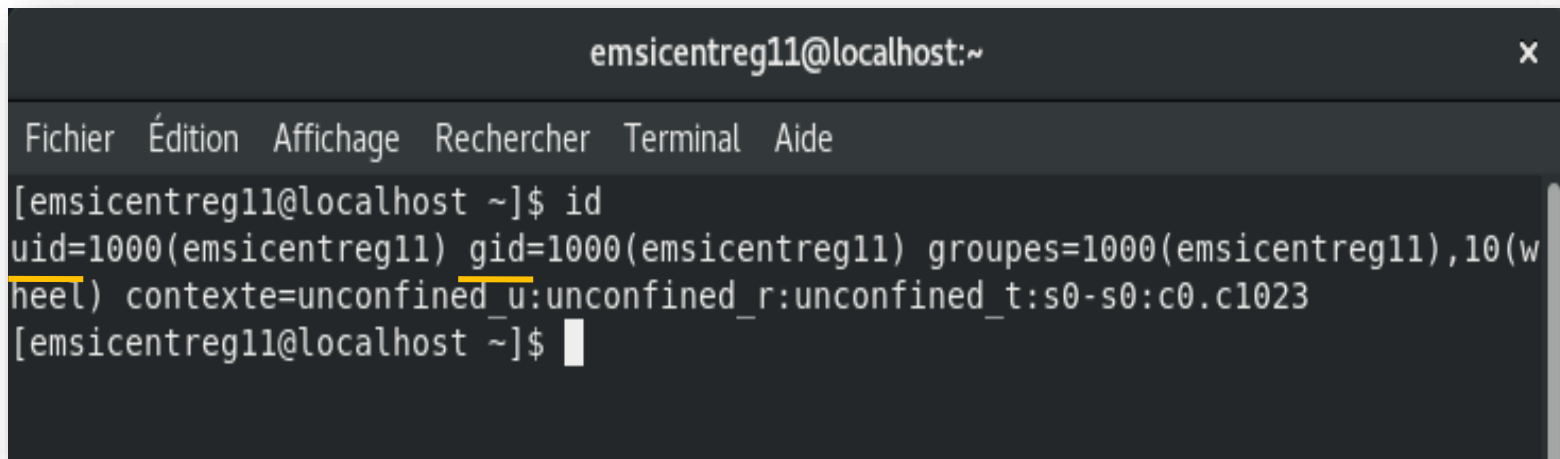
- De même chaque utilisateur est rattaché à au moins un groupe (groupe principal), chaque groupe possédant un identifiant unique, le **GID** (« Group Identifier»).
- Les groupes sont définis dans **/etc/group**.

Introduction

La commande: id

La commande **id** permet d'obtenir ces informations.

En interne, le système travaille uniquement avec les UID et GID, et pas avec les noms par eux-mêmes.

A terminal window titled 'emsicentreg11@localhost:~' with a close button 'x' in the top right corner. The window has a menu bar with 'Fichier', 'Édition', 'Affichage', 'Rechercher', 'Terminal', and 'Aide'. The terminal shows the command 'id' being executed, resulting in the output: 'uid=1000(emsicentreg11) gid=1000(emsicentreg11) groupes=1000(emsicentreg11),10(wheel) contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023'. The prompt '[emsicentreg11@localhost ~]\$' is shown at the end of the line.

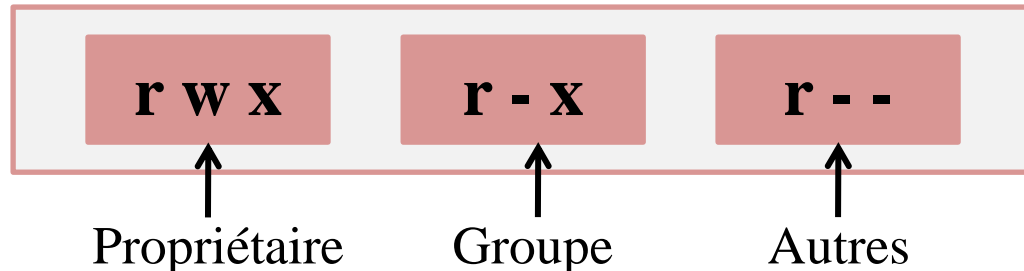
```
emsicentreg11@localhost:~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
[emsicentreg11@localhost ~]$ id  
uid=1000(emsicentreg11) gid=1000(emsicentreg11) groupes=1000(emsicentreg11),10(wheel) contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[emsicentreg11@localhost ~]$
```

Introduction

A chaque fichier (numéro d'inode) sont associés un UID et un GID définissant son propriétaire et son groupe d'appartenance.

On peut affecter des droits pour le propriétaire, pour le groupe d'appartenance et pour le reste du monde. On distingue de ce fait trois cas de figure

1. UID de l'utilisateur identique à l'UID défini pour le fichier : cet utilisateur est propriétaire du fichier.
2. Les UID sont différents : le système vérifie si le GID de l'utilisateur est identique au GID du fichier : si oui l'utilisateur appartient au groupe associé au fichier.
3. Dans les autres cas (aucune correspondance) : il s'agit du reste du monde (others), ni les propriétaires, ni appartenant au groupe.



Signification des droits

Droit	Signification Général
r	Readable (lecture)
w	Writable (écriture)
x	Executable (exécutable comme programme)
Droit	Signification pour un fichier normal
r	Le contenu du fichier peut être lu, chargé en mémoire, visualisé, recopié.
w	Le contenu du fichier peut être modifié, on peut écrire dedans. La suppression n'est pas forcément liée à ce droit (voir droits sur répertoire).
x	Le fichier peut être exécuté depuis la ligne de commande, s'il s'agit soit d'un programme binaire (compilé), soit d'un script (shell, ...)

Signification des droits

Droit	Signification pour un répertoire
r	<p>Les éléments du répertoire (catalogue) sont accessibles en lecture. Sans cette autorisation, le ls et les critères de filtres sur le répertoire et son contenu ne sont pas possibles.</p> <p>Ce droit ne suffit pas pour entrer dans le catalogue.</p>
w	<p>Les éléments du répertoire (catalogue) sont modifiables et il est possible de créer, renommer et supprimer des fichiers dans ce répertoire.</p> <p>On voit donc que c'est ce droit qui contrôle l'autorisation de suppression d'un fichier même si on est pas propriétaire des fichiers du répertoire.</p>
x	<p>Le catalogue peut être accédé par cd et listé.</p> <p>Sans cette autorisation il est impossible d'accéder et d'agir sur son contenu qui devient verrouillé.</p> <p>Avec uniquement ce droit les fichiers et répertoires inclus dans celui-ci peuvent être accédés mais il faut alors obligatoirement connaître leur nom.</p>

Modification des droits

- Lors de sa création, un fichier ou un répertoire dispose de droits par défaut.
- On utilise la commande **chmod** (*change mode*) pour modifier les droits sur un fichier ou un répertoire.
- Il existe deux méthodes pour modifier ces droits : par **la forme symbolique** et par **la base 8**.
- Seul le propriétaire d'un fichier peut en modifier les droits (sauf l'administrateur système).
- Le chmod sur un lien symbolique est possible comme sur tout autre fichier, mais cela ne modifie pas les droits du lien par lui-même mais les droits du fichier pointé.

Modification des droits

Modification par symboles:

La syntaxe est la suivante :

***chmod** modifications Fich1 [Fich2...]*

S'il faut modifier les droits de **l'utilisateur**, on utilisera le caractère « **u** ».

Pour les droits du **groupe**, le caractère « **g** », pour le reste du monde le caractère « **o** », pour tous le caractère « **a** ».

Pour ajouter des droits, on utilise le caractère « **+** », pour en retirer le caractère « **-** », et pour ne pas tenir compte des paramètres précédents le caractère « **=** ».

Enfin, le droit d'accès par lui-même : « **r** », « **w** » ou « **x** ».

Modification des droits

Modification par symboles:

Exemple 1:

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[emsicentreg11@localhost Droits]$ touch file1
[emsicentreg11@localhost Droits]$ ls -l
total 0
-rw-rw-r--. 1 emsicentreg11 emsicentreg11 0  1 nov.  14:37 file1
[emsicentreg11@localhost Droits]$
[emsicentreg11@localhost Droits]$ chmod u+x,g-w,o+x file1
[emsicentreg11@localhost Droits]$
[emsicentreg11@localhost Droits]$ ls -l
total 0
-rwxr--r-x. 1 emsicentreg11 emsicentreg11 0  1 nov.  14:37 file1
[emsicentreg11@localhost Droits]$
```

Modification des droits

Modification par symboles:

Exemple 2:

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[emsicentreg11@localhost Droits]$ mkdir repl
[emsicentreg11@localhost Droits]$ ls -l
total 4
-rwxr--r-x. 1 emsicentreg11 emsicentreg11    0  1 nov.  14:37 file1
drwxrwxr-x. 2 emsicentreg11 emsicentreg11 4096  1 nov.  14:38 repl
[emsicentreg11@localhost Droits]$
[emsicentreg11@localhost Droits]$ chmod a-x,g-w repl
[emsicentreg11@localhost Droits]$
[emsicentreg11@localhost Droits]$ ls -l
total 4
-rwxr--r-x. 1 emsicentreg11 emsicentreg11    0  1 nov.  14:37 file1
drw-r--r--. 2 emsicentreg11 emsicentreg11 4096  1 nov.  14:38 repl
[emsicentreg11@localhost Droits]$
[emsicentreg11@localhost Droits]$ cd repl
bash: cd: repl: Permission denied
[emsicentreg11@localhost Droits]$
```

Modification des droits

Modification par base 8:

La syntaxe est identique à celle des symboles.

A chaque droit correspond une valeur octale c'est à dire de zéro (0) à sept (7), positionnelle et cumulable.

Propriétaire			Groupe			Autres		
r	w	x	r	w	x	r	w	x
400	200	100	40	20	10	4	2	1

Pour obtenir le droit final il suffit d'additionner les valeurs. Par exemple si on veut **rwxrw-rw-** alors on fera : $400+200+100+40+20+0+4+2+0 = \mathbf{766}$

et pour **rw-r--r--**: $400+200+0+40+0+0+4+0+0 = \mathbf{644}$

Modification des droits

Modification par base 8:

Exemple:

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[emsicentreg11@localhost Droits]$ touch file2
[emsicentreg11@localhost Droits]$ ls -l
total 0
-rw-rw-r--. 1 emsicentreg11 emsicentreg11 0  1 nov.  14:45 file2
[emsicentreg11@localhost Droits]$ 
[emsicentreg11@localhost Droits]$ chmod 740 file2
[emsicentreg11@localhost Droits]$ 
[emsicentreg11@localhost Droits]$ ls -l
total 0
-rwxr-----. 1 emsicentreg11 emsicentreg11 0  1 nov.  14:45 file2
[emsicentreg11@localhost Droits]$
```

Masque des droits

Les droits d'un fichier ou d'un répertoire après leur création sont:

- `rw-r--r--` (644) pour un fichier
- `rw-r--r--` (755) pour un répertoire

Ces valeurs sont contrôlées par un masque, lui-même modifiable par la commande **umask**.

La commande prend comme paramètre une valeur octale qui sera soustraite aux droits d'accès maximum.

Par défaut, tous les fichiers sont créés avec les droits 666 (`rw-rw-rw-`) et les répertoires avec les droits 777 (`rw-rw-rw-`), puis le masque est appliqué.

Sur la plupart des Unix, le masque par défaut est 022, soit `---w--w-`. Pour obtenir cette valeur, on tape **umask** sans paramètre.

```
[root@localhost emsicentreg11]# umask
0022
[root@localhost emsicentreg11]#
```

Masque des droits

Pour un fichier :

Maximum	rw-rw-rw-	(666)
Retirer	----w--w-	(022)
Reste	rw-r--r--	(644)

Pour un répertoire :

Maximum	rwxrwxrwx	(777)
Retirer	----w--w-	(022)
Reste	rwxr-xr-x	(755)

ATTENTION : le calcul des droits définitifs (effectifs) n'est pas une simple soustraction de valeurs octales ! Le masque retire des droits mais n'en ajoute pas.

Pour un fichier :

Maximum	rw-rw-rw-	(666)
Retirer	---r-xrw-	(056)
Reste	rw--w----	(620) et PAS 610 !

Changement de propriétaire et de groupe

Il est possible de changer le propriétaire et le groupe d'un fichier à l'aide des commandes **chown** (change owner) et **chgrp** (change group).

chown utilisateur fich1 [Fich2...]

chgrp groupe fich1 [Fich2...]

Sur les UNIX récents seul root peut utiliser chown.

La commande chgrp peut être utilisée par n'importe qui à condition que cet utilisateur fasse aussi partie du nouveau groupe.

En précisant le nom d'utilisateur (ou de groupe), le système vérifie d'abord leur existence.

On peut préciser un UID ou un GID, dans ce cas le système n'effectuera pas de vérification.

Pour les deux commandes on peut préciser l'option **-R**, **dans ce cas les droits seront changés de** manière récursive. Les droits précédents et l'emplacement du fichier ne sont pas modifiés.

Changement de propriétaire et de groupe

Exemples:

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[emsicentreg11@localhost Droits]$ ls
file2
[emsicentreg11@localhost Droits]$ chown user1 file2
chown: modification du propriétaire de 'file2': operation not permitted
[emsicentreg11@localhost Droits]$ su root
Mot de passe :
[root@localhost Droits]# ls -l
total 0
-rwxr-----. 1 emsicentreg11 emsicentreg11 0  1 nov.  14:45 file2
[root@localhost Droits]# chown user1 file2
[root@localhost Droits]#
[root@localhost Droits]# ls -l
total 0
-rwxr-----. 1 user1 emsicentreg11 0  1 nov.  14:45 file2
[root@localhost Droits]#
```


Changement de propriétaire et de groupe

Exemples:

```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
[emsicentreg11@localhost Droits]$ ls -l
total 0
-rwxr-----. 1 user1 emsicentreg11 0 1 nov. 14:45 file2
[emsicentreg11@localhost Droits]$ chgrp users file2
chgrp: modification du groupe de 'file2': Operation not permitted
[emsicentreg11@localhost Droits]$ su root
Mot de passe :
[root@localhost Droits]# chgrp users file2
[root@localhost Droits]#
[root@localhost Droits]# ls -l
total 0
-rwxr-----. 1 user1 users 0 1 nov. 14:45 file2
[root@localhost Droits]#
```