

Chapitre 04 : Utilisateurs et Droits

Dr Mandicou BA

mandicou.ba@esp.sn

<http://www.mandicouba.net>

Diplôme Universitaire de Technique (DUT, 1^{er} année)

Diplôme Supérieure de Technologie (DST, 1^{er} année)

Informatique



ÉCOLE SUPÉRIEURE POLYTECHNIQUE

www.esp.sn



Plan du Chapitre

- 1 Objectifs et Contenu
- 2 Gestion des utilisateurs
- 3 Gestion des Droits

Sommaire

- 1 Objectifs et Contenu
- 2 Gestion des utilisateurs
- 3 Gestion des Droits

Objectifs

- ☛ Connaître les utilisateurs et les droits :
- ☛ Gérer les comptes des utilisateurs et leurs groupes
- ☛ Utiliser et positionner les droits sur les fichiers

Contenu

- ☛ Gestion des utilisateurs
- ☛ Gestion des Droits

Sommaire

- 1 Objectifs et Contenu
- 2 Gestion des utilisateurs
- 3 Gestion des Droits

La théorie

Concept de compte

- ☛ Chaque utilisateur d'un système Linux est inscrit
 - ① dans une base de données locale
 - ② ou dans un annuaire réseau
 - NIS, LDAP comme l'AD (Active Directory)
- ☛ Un compte utilisateur représente aussi bien :
 - une personne (Pierre, Paul...)
 - qu'une application (Apache, Postfix...)

Caractéristiques d'un compte utilisateur

- ☞ **Login** : c'est le nom de l'utilisateur (ou de l'application)
- ☞ **Mot de passe** : il est utilisé lors de la connexion pour authentifier l'utilisateur
- ☞ **UID** : ce numéro identifie l'utilisateur (« User IDentification »)
- ☞ **GID** : ce numéro spécifie le groupe principal de l'utilisateur (« Group IDentification »)
- ☞ **Commentaire**
- ☞ **Répertoire de connexion**
- ☞ **Shell** : ce logiciel, le plus souvent un véritable shell, est activé en début de session en mode texte.

Caractéristiques d'un groupe

Caractéristiques d'un groupe

- ☛ **Le nom du groupe**
- ☛ **GID** : ce numéro identifie le groupe
- ☛ **Un mot de passe** : cette valeur n'est jamais renseignée
- ☛ *La liste des membres en tant que membres secondaires, ce qui exclut les comptes dont c'est le groupe principal*

Gestion des comptes

- ☛ La gestion des comptes (création...) est une prérogative de l'administrateur (root)

Les fichiers de gestion des utilisateurs

- ☞ **/etc/passwd** : contient la base locale des comptes utilisateur.
- ☞ **/etc/group** : contient la base locale des comptes groupe
- ☞ **/etc/shadow** : contient les mots de passe locaux et leur durée de vie

Les commandes de gestion des utilisateurs

Manipulation des utilisateurs

- ☛ **useradd** : ajout d'un compte utilisateur local
- ☛ **usermod** : modification d'un compte utilisateur local
- ☛ **userdel** : supprime un utilisateur
- ☛ **groupadd** : ajoute un groupe
- ☛ **groupmod** : modification d'un groupe
- ☛ **groupdel** : destruction d'un compte groupe local
- ☛ **passwd** : Modifie le mot de passe d'un compte
- ☛ **chpasswd** : Change un mot de passe de manière scriptable
- ☛ **id** : Affiche les identités d'un compte (local ou non)

Focus : la structure des fichiers passwd et group

```
root@linux1 ~]# head -5 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

- ☛ Chaque ligne du fichier passwd décrit un utilisateur. Les champs sont séparés par deux points (« : »)
- ☛ La dernière ligne décrit l'utilisateur lp :
 - son uid est 4, son gid est 7
 - le commentaire contient la chaîne lp
 - son répertoire de connexion est /var/spool/lpd
 - son shell est /sbin/nologin (ce qui signifie que l'on ne peut se connecter à ce compte).

Focus : la structure des fichiers passwd et group

```
[root@linux1 ~]# head -3 /etc/group  
root:x:0:root  
bin:x:1:root,bin,daemon  
daemon:x:2:root,bin,daemon
```

- ☛ Chaque ligne du fichier group décrit un groupe.
- ☛ La dernière ligne décrit le groupe de nom « daemon » :
 - son GID est 2
 - et ses membres sont les comptes root, bin et daemon.

Focus : la commande useradd

- ☛ La commande useradd permet de créer un compte utilisateur.
- ☛ Ses principales caractéristiques peuvent être précisées

```
[root@linux1 ~]# useradd -u 1001 -g lp -G news,mail -c vampire -d /usr/dracula -m -s /bin/bash dracula
```

- ☛ La commande précédente crée le compte utilisateur **dracula**.
 - son uid est 1001,
 - son groupe principal (son gid) est lp
 - il fait partie également des groupes news et mail (en tant que groupes secondaires)
 - le champ commentaire contient la chaine vampire
 - son répertoire de connexion est /usr/dracula :
 - ce répertoire sera créé (option -m).
 - son shell est le shell **bash**

Sommaire

- 1 Objectifs et Contenu
- 2 Gestion des utilisateurs
- 3 Gestion des Droits**

La théorie

Catégories d'utilisateurs

- ☛ Lors de l'accès à un fichier, le noyau Linux considère trois catégories d'utilisateurs :
 - 1 Le propriétaire du fichier (user ou u)
 - 2 Les membres du groupe (group ou g) auquel est affilié le fichier
 - 3 Les autres utilisateurs (other ou o)
- ☛ Pour chaque catégorie, il existe trois droits d'accès, dont la signification dépend de la nature du fichier : ordinaire ou répertoire.

La théorie

Droits pour un fichier ordinaire

- ☛ Le droit de lecture (read ou r) permet de lire les octets du fichier
- ☛ Le droit d'écriture (write ou w) permet d'ajouter, supprimer ou modifier des octets
- ☛ Le droit d'exécution (execute ou x) permet de considérer le fichier comme une commande

Remarque : le droit exécution ne doit être utilisé que pour des binaires résultants d'une compilation ou pour des scripts

La théorie

Droits pour un répertoire

- ☛ Le droit de lecture (r) permet de connaître la liste des fichiers du répertoire
- ☛ Le droit d'écriture (w) permet de modifier le répertoire : créer ou supprimer des entrées dans le répertoire
- ☛ Le droit d'accès (x) permet d'accéder aux fichiers du répertoire

IMPORTANT ! Le dernier, le droit d'accès est le plus important. Sans lui une personne n'a aucun accès aux fichiers présents dans le répertoire, quels que soient leurs droits.

Manipulation des droits

Les commandes

- 👁 **ls -l** : Liste les caractéristiques d'un fichier, dont les droits
- 👁 **chmod** : Modifie les droits d'un fichier
- 👁 **chgrp** : Change le groupe d'un fichier
- 👁 **chown** : Change le propriétaire d'un fichier
- 👁 **umask** : Fixe les droits retirés automatiquement lors de la création d'un fichier
- 👁 **cp -p** : Copie de fichiers avec conservation des attributs

Le savoir concret : droits en octal

400	read	user
200	write	
100	execute	
40	read	group
20	write	
10	execute	
4	read	other
2	write	
1	execute	

Le savoir concret : droits en octal

- ☛ Les droits sont marmorisés sur disque sous forme de bits
- ☛ C'est la raison pour laquelle beaucoup de commandes utilisent la vision octale des droits
- ☛ La valeur 751, par exemple, est égale à $400+200+100+40+10+1$
 - Elle signifie donc tous les droits pour le propriétaire (user), les droits de lecture et d'exécution pour le groupe, et d'exécution pour les autres

Le savoir concret : Focus sur la commande ls -l

```
$ ls -l le_fichier
```

```
-rwxr-x-- 1 root bin 153 Jul 23 20:21 le_fichier
```

Propriétaire (u)

Groupe (g)

r = lecture
w = écriture
x = exécution

u g o = other

Figure: Voir les droits avec la commande ls -l

- ☛ La commande ls -l liste les caractéristiques d'un fichier
- ☛ Derrière le type du fichier, neuf caractères indiquent les droits
- ☛ Ils sont repartis en trois groupes de trois caractères
 - le premier spécifie les droits du propriétaire,
 - le deuxième ceux des membres du groupe auquel est affilié le fichier,
 - le dernier indique les droits des autres utilisateurs.
 - l'absence d'un droit est indiqué par un « - ».

Le savoir concret : Focus sur la commande ls -l

<code>rwXrwxrwx</code>	Toutes les catégories (u, g, o) ont tous les droits (r,w,x).
<code>rwXrwx---</code>	Les autres n'ont aucun droit.
<code>rwX-----</code>	Seul le propriétaire a tous les droits (r,w,x).
<code>rwXr-x--x</code>	Le propriétaire a tous les droits, le groupe a les droits de lecture et d'exécution, les autres n'ont que le droit d'exécution.
<code>r--r--r--</code>	Tout le monde a le droit de lecture.

Le savoir concret : Focus sur la commande chmod

- ☛ La commande **chmod** a pour premier argument la modification des droits. Elle peut s'exprimer en octal ou de manière symbolique.

```
[root@linux1 tmp]# chmod 444 toto  
[root@linux1 tmp]# chmod ug+w toto  
[root@linux1 tmp]# chmod u+w,g+w toto
```

- ☛ Dans l'approche symbolique, la modification se divise en trois groupes :
 - Les catégories : **u**, **g**, **o**. L'absence de catégorie ou la lettre « **a** » indique tout le monde
 - Un l'opérateur : **+**, **-**, **=**. Plus et moins indiquent l'ajout ou le retrait de droits.
 - Le signe égal indique que l'on fixe les droits sans référence aux droits antérieurs (comme en octal)
 - Les droits: **r**, **w**, **x**, **s**, **t** (et « **-** » dans le cas de l'utilisation du signe égal)
 - On peut mettre plusieurs modifications symboliques séparées par des virgules

Chapitre 04 : Utilisateurs et Droits

Dr Mandicou BA

mandicou.ba@esp.sn

<http://www.mandicouba.net>

Diplôme Universitaire de Technique (DUT, 1^{er} année)

Diplôme Supérieure de Technologie (DST, 1^{er} année)

Informatique



ÉCOLE SUPÉRIEURE POLYTECHNIQUE

www.esp.sn

