MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD

FSSM
كلية العلوم السملالية

Chapitre 6 Unix/Linux : Utilisateurs, Groupes et Droits Avancés

Groupes

- Quand un fichier est crée, il est automatiquement la propriété d'un utilisateur et un groupe.

  Exemple : rw-rw-r-- airaj staff /home/airaj/test

- /etc/group est le fichier qui définit les groupes.
  - airaj:x:500:800:Mohammed AIRAJ:/home/airaj:/bin/bash
  - staff:x:800
  - Le groupe principal de l'utilisateur airaj est staff
- Le groupe propriétaire d'un fichier est le groupe principal de l'utilisateur qui l'a crée.
- Pourquoi les groupes?
  - Permettent une organisation flexible des fichiers.
  - Permettent à un nombre arbitraire d'utilisateurs de partager des fichiers de façon transparente.

Création d'un utilisateur : commande useradd et passwd

useradd airaj –g staff

Création du compte utilisateur **airaj** membre du groupe principal **staff**

en utilisant les valeurs définies dans le système de fichiers.

(définies dans /etc/default/useradd, /etc/login.defs)

useradd -D : affiche les valeurs par défaut.

passwd airaj

Permet d'entrer le mot de pass pour l'utilisateur airaj

userdel

userdel airaj

Supprime le compte utilsateur **airaj** du système.

userdel –r airaj

L'option –r supprime aussi le répertoire home de l'utilisateur.

! Peut pas supprimer un compte si son utilisateur est connecté ou si l'utilisateur a un processus démarré.

Utilisateurs : Caractéristiques

- Chaque utilisateur d'un système Linux est inscrit dans une base de données locale ou dans un annuaire réseau. Un compte utilisateur représente bien une personne qu'une application (Apache, lp,…)

- Les caractéristiques d'un compte utilisateur :

Login	Nom de l'utilisateur (ou de l'application)
Mot de passe	Utilisé lors de la connexion pour authentifier l'utilisateur
UID	Un numéro qui identifie l'utilisateur
GID	Un numéro spécifiant le groupe principale de l'utilisateur
Commentaire	
Répertoire de connexion	
Shell	Le plus souvent un véritable shell, activé en début de session en mode texte

- **L'UID 0** est réservé à l'administrateur **root.** L'utilisateur **root** a tous les droits sur le système.

Les commandes

useradd, userdel	Ajout, destruction d'un compte utilisateur
groupadd, groupdel	Ajout, destruction d'un compte groupe
passwd	Modifie le mot de passe d'un compte
id	Affiche les identités d'un compte
su	Réalise une connexion secondaire, on doit déjà être connecté. Exemple (user connecté airaj) : $ **su – root** Je suis connecté en tant que airaj et je voudrais réaliser une connexion en tant que root
chgrp	Change le groupe propriétaire d'un fichier ou d'un répertoire(***chrgp group*** fichier ou répertoire)
chown	Change le propriétaire d'un fichier ou répertoire(***chown user.group*** fichier ou répertoire)

Les utilisateurs et les droits : avancé

- Le sticky bit : Par défaut un répertoire accessible en écriture à un ensemble d'utilisateurs permet à l'un d'entre eux de détruire les fichiers d'un autre utilisateurs!. Avec le sticky bit il faut être propriétaire d'un fichier pour avoir le droit de le détruire.

- Les droits d'endossement (SUID, SGID) pour un exécutable : Ils servent à augmenter les privilèges des utilisateurs. Par exemple, le droit Set-UID (SUID pour **S**et owner **U**ser **ID** up on execution) sur un binaire exécutable permet à l'utilisateur de l'application correspondante d'avoir les mêmes droits d'accès que le propriétaire du binaire. Le droit Set-GID (SGID) permet d'endosser les droits du groupe auquel est affilié le binaire.

- Exemple : le fichier /etc/shadow n'est en théorie accessible qu'à root. Or, tout utilisateur à accès en écriture à ce fichier lorsqu'il change son passwd grâce à la commande /usr/bin/passwd. Cela est dû au fait que cette commande, détenue par root possède le droit SUID et donne de fait à tous les utilisateurs les mêmes droits que root.

Les utilisateurs et les droits : avancé

- Le droit SGID pour un répertoire : Lorsque l'on crée un fichier il est automatiquement affilié à son groupe principal. Si l'on crée un fichier dans un répertoire qui possède le droit SGID, son groupe sera identique à celui du répertoire.

- Le droit de modifier les droits : Un administrateur peut modifier le propriétaire d'un fichier.

- Les droits en octal : 4000 pour SUID, 2000 pour SGID et 1000 Sticky bit

- Equivalent en symbolique : s

- Exemple : supposons que vous souhaitiez appliquer les droits de SUID et SGID à un fichier nommé testme qui devrait être lisible et exécutable par le propriétaire et le groupe, et lisible par les autres. Vous entrez chmod 6554 testme à l'invite de commandes ou chmod ug+srx,o+r testme

- Si vous affichez les droits avec ls -l : le sticky bit est représenté par t si il cache les droits d'exécution pour others (ex : rwxrws--t), T sinon. De même pour les SUID et SGID, s si cache les droits d'exécution, S sinon.

Exemple (suite)

- Par exemple, supposons que vous souhaitiez appliquer les droits de SUID et SGID à un fichier nommé *testme* qui devrait être lisible et exécutable par le propriétaire et le groupe, et lisible par les autres. Vous entrez *chmod 6554 testme* à l'invite de commandes (ou *chmod ug+srx,o+r testme*).

- Ceci indique que le fichier a les droits SUID (4) et SGID (2) attribuées (pour un total de 6 dans le premier nombre).

- Il précise également que le propriétaire et le groupe ont les droits de lecture (4) et d'exécution (1) attribuées (pour un total de 5 dans les deuxième et troisième nombres).

- Il précise également que les autres sont autorisés à lire (4) le fichier, mais ne sont pas en mesure de le modifier ou de l'exécuter (pour un total de 4 dans le dernier nombre).

Exemple

- Permettre à un programme de s'exécuter en utilisant les droits du propriétaire du programme

```
mbp-stratuslab:dir2 airaj$ ls -l monfichier.txt
-rwxrwxrwx  2 airaj  staff  0 Oct  3 19:26 monfichier.txt
mbp-stratuslab:dir2 airaj$ chmod u+s monfichier.txt
mbp-stratuslab:dir2 airaj$ ls -l monfichier.txt
-rwsrwxrwx  2 airaj  staff  0 Oct  3 19:26 monfichier.txt
mbp-stratuslab:dir2 airaj$ chmod u-x monfichier.txt
mbp-stratuslab:dir2 airaj$ ls -l monfichier.txt
-rwSrwxrwx  2 airaj  staff  0 Oct  3 19:26 monfichier.txt
```

Droits	Description	Effet sur les fichiers	Effet sur les répertoires
SUID	Set User ID, s'applique aux fichiers binaires	Quand un fichier exécutable avec un SUID défini, l'utilisateur qui a démarré le fichier devient temporairement son propriétaire	Rien
SGID	Set Group ID, peut s'appliquer aux fichiers binaires	Quand un utilisateur démarre un fichier exécutable avec un SGID défini, l'utilisateur devient temporairement membre du groupe propriétaire du fichier	Quand un utilisateur crée un fichier dans un répertoire qui a un SGID défini, le propriétaire du fichier est le propriétaire du compte (c'est normal). Néanmoins le groupe propriétaire du répertoire parent est assigné comme groupe propriétaire au nouveau fichier
Sticky Bit		Rien	Quand un Sticky Bit est assigné à un répertoire, les utilisateurs peuvent supprimer uniquement les fichiers dont ils sont propriétaires dans ce répertoire ou le répertoire lui même. C'est la négation de l'effet d'avoir des droits write sur un répertoire, qui permettent à un utilisateur de supprimer des fichiers dans un répertoire dont il est pas le propriétaire.