

Administration systèmes

Chapitre 4 - Utilisateurs et mécanismes de droits

Gorgoumack SAMBE

Université Assane Seck de Ziguinchor

Version 1.0 ¹

1. Novembre 2022



Objectifs

être capable de :

- 1 distinguer les types de comptes d'utilisateurs sur un système UNIX ;
- 2 gérer les comptes et personnaliser un profil d'utilisateur ;
- 3 gérer les groupes d'utilisateurs ;
- 4 distinguer et gérer les droits liés à un fichier ;
- 5 configurer les droits par défaut des fichiers.



1 Utilisateurs et groupes

2 Mécanismes de droits

1 Utilisateurs et groupes

2 Mécanismes de droits

Comptes d'utilisateurs

- Permet à un **utilisateur** d'exploiter le système avec un **login**(nom) éventuellement couplé à un **mot de passe**.
- Identifié par un **User Identifier (UID)**.
- Assurer la sécurité et la confidentialité (système et données).



Comptes d'utilisateurs

- Permet à un **utilisateur** d'exploiter le système avec un **login(nom)** éventuellement couplé à un **mot de passe**.
- Identifié par un **User Identifier (UID)**.
- Assurer la sécurité et la confidentialité (système et données).
- Trois types de comptes
 - ① **Utilisateur racine** : création à l'installation, tous les droits d'usage et d'administration du système ;
 - **Login** : root
 - **Répertoire personnel** : /root
 - ② **Utilisateur régulier** : usage du système, connexion normale, suppression et désactivation possible, possibilité d'accord de privilèges d'administration ;
 - **Répertoire personnel** : sous répertoire de /home
 - ③ **Compte de service** : sans connexion, liés à des services ;
 - **Exemples** : mysql, vboxuser, ...



Groupe d'utilisateurs

- Permet de définir une **politique d'accès** pour un **groupe d'utilisateurs** sur des fichiers et répertoires.
- Identifié par un **Group Identifier (GID)** et possède un **nom**.
 - un **groupe** est défini à partir d'une **liste d'utilisateurs éventuellement vide**.
 - un **utilisateur** doit faire partie **au moins d'un groupe** : groupe primaire.
 - un **utilisateur** peut appartenir à d' **autres groupes** : groupes secondaires.
- **Session** : connexion avec login de connexion et groupe actif.
 - fichiers et répertoires créés \in **login :groupe** ;
- **groupe sudo** : groupe possédant plus ou moins des droit d'administration à travers la commande sudo.



Les commandes

- **useradd** (adduser) : créer un nouvel utilisateur.
- **userdel** : supprimer un compte et les fichiers associés.
- **usermod** : modifier un compte utilisateur.
- **lslogins** : affichage des informations sur les comptes
- **passwd** : modifier le mot de passe d'un utilisateur



Les commandes

- **useradd** (adduser) : créer un nouvel utilisateur.
- **userdel** : supprimer un compte et les fichiers associés.
- **usermod** : modifier un compte utilisateur.
- **lslogins** : affichage des informations sur les comptes
- **passwd** : modifier le mot de passe d'un utilisateur
- **groupadd** (addgroup), **groupdel**, **groupmod**, **groups/id** ;



Les commandes

- **useradd** (adduser) : créer un nouvel utilisateur.
- **userdel** : supprimer un compte et les fichiers associés.
- **usermod** : modifier un compte utilisateur.
- **lslogins** : affichage des informations sur les comptes
- **passwd** : modifier le mot de passe d'un utilisateur

- **groupadd** (addgroup), **groupdel**, **groupmod**, **groups/id** ;

- **newgrp** : changement de groupe actif ;
- **su/sg** : exécuter une commande avec un UID /GID de substitution ;
- **sudo** : exécuter une commande avec des privilèges d'administrateur.



Les fichiers

- **Gestion des comptes et groupes**

- **/etc/passwd** : informations sur les comptes
sept champs séparés par " : "
login :passwd :UID :GID :infos :HOME :SHELL
- **/etc/shadow** : informations cryptés de mot de passe
neuf champs séparés par " : "
mots de passe chiffré et dates de validités ;
- **/etc/group** : informations sur les groupes
quatre champs séparés par " : "
nom_groupe :passwd :GID :membres du groupe

- **Fichiers de profil**

- Fichiers lu à la connexion pour définir l'environnement de travail (shell, prompts, couleur terminal, ...)
 - **/etc/profile** (modifiable par root)
 - shell de connexion : `~/.bash_profile`, `~/.profile` ;
 - non-login shell : `~/.bashrc`.



1 Utilisateurs et groupes

2 Mécanismes de droits

Propriétaires d'un fichier

- Trois identités par fichier et répertoire

- ① utilisateur propriétaire (u)
- ② groupe propriétaire (g)
- ③ autres utilisateurs (o)
- ④ ...et tous les utilisateurs (a=ugo)

- Visualisation : ls -l



- Propriétaire d'un fichier ou répertoire

- à la création : login connecté et groupe actif.
- possibilité de modification
 - ① **chown** : modification du propriétaire et du groupe.
 - ② **chgrp** : modification du groupe



Droits sur un fichier

❶ Droits standards

- ❶ **r (Read)** : droit de lecture [4=100]
- ❷ **w (Write)** : droit d'écriture [2=010]
- ❸ **x (eXecute)** : droit d'exécution ² [1=001]

❷ Droits spéciaux

- ❶ **sticky bit**(1000) : modification de fichiers dans un répertoire(/tmp)
- ❷ **setUID**(4000), **setGID**(2000) : endossement de l'identité du propriétaire (passwd, crontab)

	Droits standards								
	user			group			other		
Mode symbolique	r	w	x	r	w	x	r	w	x
Mode numérique	400	200	100	40	20	10	4	2	1

	Droits spéciaux								
	user			group			other		
Mode symbolique			s/S			s/S			t/T
Mode numérique	4000			2000			1000		

2. traversée pour un répertoire

Les commandes

① Gestion des droits *aposteriri* : `chmod`

- **Syntaxe**

`chmod [OPTION] [u g o a] [+ - =] [r w x X s t] FICHER ...`
`chmod [OPTION] mode-octal FICHER ...`

- **Exemples :**

\$ `chmod 644 tic tac`
\$ `chmod u+x,go-w,o-r test oups`

② Gestion des droits *apriori* : `umask`

- **Syntaxe** : `umask masque`

"masque" : valeur numérique comprise entre 000 et 777

Exemple : \$ `umask 022`

- **Principe de fonctionnement**

Droits = Droit_maxima - umask

Droit_maxima=666 pour les fichiers, 777 pour les répertoires

