

TP2 : Gestion des utilisateurs

Objectif : Découvrir le système GNU/ Linux et exécuter les commandes de base.

1. La gestion des comptes utilisateurs

a. Le compte root

Sous Unix et Linux, le compte root est le compte du super administrateur du système.

L'invite de commande root utilise le caractère **#**.

Les bonnes pratiques stipulent qu'un administrateur utilisera un **compte standard** pour les opérations courantes puis effectuera ponctuellement **une élévation de privilèges** selon les besoins. Cette bonne pratique est surtout valable pour les connexions à distance (en **ssh**).

- Quel est le dossier personnel de l'utilisateur root ?

b. La commande **passwd**

- Afficher la page du manuel de la commande **passwd** et expliquer à quoi sert-elle ?
- Taper la commande **passwd**. Que remarquez-vous ?
Remarque : pour annuler la commande, appuyer sur **CTRL+d**.
- Taper la commande **passwd -S** et noter le résultat :

c. La commande **adduser**

- Afficher la page du manuel de la commande **adduser** et expliquer à quoi sert-elle ?
- Taper **adduser votre-nom** et saisir les informations demandées.
- Vérifier la présence de votre compte dans le fichier **/etc/passwd**. Que contient ce fichier ?
- Vérifier à l'aide de la commande : **passwd -S nom-utilisateur**
- Ouvrir le fichier **/etc/group**. Vérifier l'existence de votre compte. Que contient ce fichier ?
- Ouvrir le fichier **/etc/shadow**. Vérifier l'existence de votre compte. Que contient ce fichier ?
- Taper **passwd -e nom-utilisateur**. Connectez-vous avec ce compte utilisateur. Que fait la commande **passwd -e** ?

d. La commande **userdel**

- Afficher la page du manuel de la commande **userdel** et expliquer à quoi sert-elle ?

- Créer un utilisateur **util3** à l'aide de la commande **adduser**.
- Supprimer l'utilisateur **util3** en utilisation l'option **-r** pour supprimer son répertoire personnel.

e. La commande **groupadd**

- Afficher la page du manuel de la commande **groupadd** et expliquer à quoi sert-elle ?
- Créer un groupe **groupe1** à l'aide de la commande **groupadd**.
- Créer un utilisateur **util3** à l'aide de la commande **useradd**.
- Ajouter l'utilisateur **util3** au **groupe1** à l'aide de la commande **gpasswd -a util3 groupe1**.

f. La commande **id**

- Taper la commande **id util3**. Quel est son résultat ?
- Taper la commande **groups util3**. Quel est son résultat ?

2. Le groupe **sudo** :

Les utilisateurs du groupe **sudo** possèdent plus de privilèges (droits) que les utilisateurs standards.

Exemple de privilèges :

- o Modification des fichiers de configuration,
- o Démarrage, arrêt, redémarrage des services,
- o Création d'utilisateurs, ...
- Taper la commande **su util3**.
- Editer le fichier **hosts** à l'aide de la commande : **nano /etc/hosts**. Que remarquez-vous ?
- Retaper la commande **groups util3**. Constater que l'utilisateur n'appartient pas au groupe **Sudo**.
- Taper la commande **adduser util1 sudo**. Vérifier cet ajout à l'aide de la commande **groups**.
- Editer à nouveau le fichier **hosts** à l'aide de la commande : **sudo nano /etc/hosts**. Que remarquez-vous ?

Pourquoi les membres du groupe "sudo" ont le droit d'effectuer des actions d'administration sur la machine ?

La réponse se trouve dans le fichier ***/etc/sudoers***.

- En tant que root, éditer le fichier */etc/sudoers*. Que constatez-vous ?

Modification du fichier */etc/sudoers*.

Il est possible de modifier ce fichier avec la commande : ***visudo /etc/sudoers***.

En savoir plus :

Le fichier `/etc/passwd`

Le fichier `/etc/passwd` contient la liste des utilisateurs du système local. Il est lisible par tout le monde. Chaque ligne représente un utilisateur et est composée de sept champs :

```
Login:password:UID:GID:comment:homedir:shell
```

- Champ 1 : le login ou nom d'utilisateur.
- Champ 2 : s'il contient x comme valeur. le mot de passe est placé dans `/etc/shadow`. Si c'est un point d'exclamation le compte est verrouillé.
- Champ 3 : le User ID.
- Champ 4 : le GID, c'est-à-dire le groupe principal.
- Champ 5 : un commentaire ou descriptif. C'est un champ d'information.
- Champ 6 : le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte.
- Champ 7 : le shell par défaut de l'utilisateur.

Le fichier `/etc/group`

Le fichier `/etc/group` contient la définition des groupes d'utilisateurs et pour chacun la liste des utilisateurs dont il est le groupe secondaire. Chaque ligne est composée de quatre champs :

```
Group:password:GID:user1,user2,...
```

- Champ 1 : le nom du groupe.
- Champ 2 : le mot de passe associé. Voyez l'explication juste en dessous.
- Champ 3 : le Group Id.
- Champ 4 : la liste des utilisateurs appartenant à ce groupe.

Il est inutile de replacer dans le quatrième champ les utilisateurs ayant ce groupe pour groupe principal, c'est induit.

Le fichier `/etc/shadow`

Le fichier `/etc/shadow` accompagne le fichier `/etc/passwd`. C'est là que sont stockés, entre autres, les mots de passe chiffrés des utilisateurs. Il contient toutes les informations sur les mots de passe et leur validité dans le temps. Chaque ligne est composée de 9 champs séparés par des « : » :

```
bean:$2a$10$AjADxPEfE5iUJcltzYA4wOZO.f2UZ0qP/8EnOFY.P.m:15141
:0:99999:7:::
```

- Champ 1 : le login.
- Champ 2 : le mot de passé haché. Le \$xx\$ initial indique le type de hachage.
- Champ 3 : nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
- Champ 4 : nombre de jours avant lesquels le mot de passe ne peut pas être changé (0 : il peut être changé n'importe quand).
- Champ 5 : nombre de jours après lesquels le mot de passe doit être changé.
- Champ 6 : nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
- Champ 7 : nombre de jours après l'expiration du mot de passe après lesquels le compte est désactivé.
- Champ 8 : nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
- Champ 9 : réservé.
- Les valeurs courantes pour le chiffrement des mots de passe sont les suivantes :
 - o \$1\$: MD5
 - o \$5 : SHA-256
 - o \$6 : SHA-512
 - o Autre : DES