Admin Linux Fiche 5 :

Gestion des utilisateurs

1 Gestion des utilisateurs

1.1 adduser-deluser-addgroup-delgroup

Ces commandes sont suffisamment explicites.Consulter la documentation à ce sujet pour connaître les options intéressantes. Il est à noter que Adduser crée un profil pour l'utilisateur basé sur un squelette situé dans /etc/skel. Par défaut, la home directory créée par adduser est accessible en lecture à tout le monde (voir /etc/adduser.conf). Attention, ceci peut ne pas correspondre à votre politique de confidentialité.

1.2 SU

Cette commande permet de changer d'utilisateur. Sans argument, cela permet de devenir root.

```
su admin
```

1.3 SUDO

La commande sudo a pour objectif de permettre à des utilisateurs d'exécuter des commandes en tant que superutilisateur.

1.3.1 Fonctionnement

Pour qu'un utilisateur puisse exécuter une commande avec « sudo », il doit faire partie du groupe sudo.

1.3.2 Installation

```
apt-get install sudo
```

1.3.3 Configuration

Par défaut, un utilisateur ajouté au groupe sudo possède les mêmes privilèges que root. On peut cependant changer ce comportement dans le fichier de configuration /etc/sudoers. On peut par exemple faire en sorte qu'un utilisateur sudo ne puisse exécuter que certaines commandes.

Le fichier /etc/sudoers s'édite via la commande particulière visudo.

```
sudo visudo
```

1.3.4 Utilisation

Pour ajouter un utilisateur au groupe sudo :

```
adduser toto sudo
```

Pour vérifier l'appartenance d'un utilisateur au groupe sudo :

```
groups
```

Pour permettre à un utilisateur d'exécuter une commande privilégiée (« root »). Ajouter une ligne dans le fichier /etc/sudoers.

```
user_name ALL=NOPASSWD: /usr/bin/apt-get install
```

1.4 Passwd

Il est possible de verrouiller ou de désactiver le compte root. Verrouiller le compte root empêche simplement de pouvoir se connecter directement avec le compte root tandis que la désactivation le rend totalement inutilisable.

Pour verrouiller le compte root :

```
sudo passwd -l root
```

Pour désactiver le compte root :

```
sudo usermod --expiredate 1 root
```

On peut cependant encore utiliser le compte root via :

```
sudo -s
```

1.5 Sécurité

1.5.1 SUDO

Les avantages du SUDO sont les suivants :

1. Permettre à des utilisateurs d'exécuter une commande en tant que superutilisateur sans devoir le mot de passe de root.
2. Travailler en mode non privilégié et n'utiliser le mode privilégié que quand cela est nécessaire. Ceci réduit le risque de commettre des dommages pour le systèmes.
3. Contrôler et enregistrer qui fait quoi (SUDO enregistre toutes le commandes sudo effectuées dans /var/log/auth.log).
4. Renforcer la sécurité. En désactivant le compte root et en le remplaçant par un compte « sudo », un attaquant ne connaîtra pas le mot de passe mais également le nom du compte !

1.5.2 Politique de sécurité des mots de passe

Il est important d'avoir des mots de passe assez solides et de s'assurer qu'ils ne pourront pas être facilement «crackés ». Les systèmes Linux ont une sécurité de mot de passe par défaut pour les utilisateurs normaux. Les mot de passes doivent avoir une longueur de 6 caractères minimum. Ceci peut s'avérer assez faible comme sécurité.

Cette politique de sécurité peut être améliorée notamment ceci :

1. Imposer un minimum de 8 caractères pour les mot de passes
2. N'autoriser que x essais pour le mot de passe
3. Imposer un nombre minimum de caractères différents lors du changement de mot de passe.
4. Fixer une durée de vie minimale et maximale du mot de passe (adduser)

La politique de sécurité se gère au moyen du module PAM(Pluggable Authentication Module) sous Linux. Pour améliorer la politique de sécurité, on peut installer le paquet suivant :

```
apt-get install libpam-cracklib
```

Ensuite dans le fichier de configuration de pam → /etc/pam.d/common-password.

```
password  requisite  pam_cracklib.so retry=3         minlen=8   difok=3
```

1. retry →nombre de tentatives autorisées
2. minlen → nombre minimum de caractères pour le mot de passe
3. difok →nombre de caractères différents entre ancien et nouveau mot de passe