Comment générer le mot de passe par commande

Table of Contents

Domaines du fichier /etc/shadow

Le fichier `/etc/shadow` stocke les mots de passe utilisateur sous forme de hachages dans un format particulier.

Chaque ligne dans `/etc/shadow` est une chaîne avec 9 champs séparés par '**:**'. Une ligne typique ressemble à ceci:

```
aychedee:$6$vb1tLY1qiY$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQ
Vk4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7:::
```

Les neuf domaines différents sont:

- Le nom d'utilisateur local
- Le hachage du mot de passe
- Nombre de jours depuis le début de l'heure unix (01/01/1970) pendant lesquels le mot de passe a été modifié pour la dernière fois
- Nombre minimum de jours avant que le mot de passe puisse être modifié
- Nombre maximum de jours avant que le mot de passe ne soit modifié. 99999 signifie que l'utilisateur ne sera pas obligé de changer son mot de passe
- Nombre de jours avant de forcer le changement de mot de passe que l'utilisateur sera averti.
- Le nombre de jours après l'expiration que le compte sera désactivé
- Jours depuis le début de l'heure Unix où le compte a été désactivé
- Actuellement inutilisé mais réservé pour une utilisation future

La plupart de ces champs ne sont généralement pas utilisés par les distributions Linux. Les plus importants sont le nom d'utilisateur et le hachage. Le champ de hachage lui-même est composé de trois champs différents. Ils sont séparés par '**$**' et représentent:

- le mécanisme de hachage cryptographique utilisé pour générer le hachage réel, les méthodes standard prises en charge par GNU/Linux sont:
    - **1**: md5
    - **$2a$**: Blowfish
    - **$2y$**: Blowfish, avec une gestion correcte des caractères 8 bits
    - **5**: sha256
    - **6**: sha512
    - par défaut l'algorithme est DES

- Un sel généré aléatoirement pour se protéger contre les attaques de la table rainbow
- Le hachage qui résulte de la jonction du mot de passe des utilisateurs avec le sel stocké et de son exécution via le mécanisme de hachage spécifié dans le premier champ.

Génération du mot de passe

Générer une chaîne aléatoire

/dev/urandom permet de générer des mots de passe à la volée sous Linux.

Voici un exemple d'utilisation :

```
< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c8
```

Quelques explications sur le fonctionnement de cette commande :

- **/dev/urandom**: c'est l'interface avec le générateur de nombres aléatoires du noyau Linux
- **tr -dc _A-Z-a-z-0-9**: indique les caractères à utiliser pour créer le mot de passe. Ici on utilise tous les caractères de l'alphabet (minuscule et majuscule) plus les chiffres.
- **head -c8**: permet d'ajuster la longueur du mot de passe. Ici il fera 8 caractères.

Si l'on souhaite avoir un retour chariot en fin de ligne, on pourra simplement utiliser echo :

```
echo `< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c8`
```

Créer le hash du mot de passe

openssl permet de créer la chaîne de hachage.

```
echo 'password' |openssl passwd -1 -salt QidasQKZ -stdin | cut -d" " -f1
```

Substitution du mot de passe

Pour substituer le mot de passe dans un fichier de type shadow:

```
user1:motdepassecrypté1:655196:0:99999:7::
user2:motdepassecrypté2:655656:0:99999:7:::
user3:motdepassecrypté3:655765:0:99999:7:::
user4:motdepassecrypté4:655999:0:99999:7::::
```

utiliser le script suivant:

```

```

```
sed '/^'"$user"'/s/\([^:]*\):[^:]*:\(.*\)/\1:'"$newPwd"':\2/' 1erFichier
```

Pour substituer le mot de passe dans un fichier de type XML:

```
user1:
password = motdepassecrypter1
lastupdate = 1234133
flags =

user2:
password = motdepassecrypter2
lastupdate = 1234333
flags =

user3:
password = motdepassecrypter3
lastupdate = 1234633
flags =

user4:
password = motdepassecrypter4
lastupdate = 1234933
flags =
```

Utiliser le scripte suivant

```
sed '/^'"$user"'/{N; s/\(.* = \).*/\1'"$newPwd"'/}' 2emeFichier
```

Pour changer un mot de passe en une ligne de commande, exécuter simplement:

```
echo "linuxpassword" | passwd --stdin linuxuser
```

ou

```
echo -e "linuxpassword\nlinuxpassword" | passwd linuxuser
```

Pour mettre à jour son propre mot de passe en tant qu'utilisateur normal, utiliser:

```
echo -e "your_current_pass\nlinuxpassword\nlinuxpassword" | passwd
```