passwd

La commande `passwd` est une commande utilisée dans les systèmes d'exploitation de type Unix, tel que Linux, pour changer le mot de passe d'un utilisateur.

Lorsqu'un utilisateur exécute la commande `passwd` dans un terminal, le système lui demande d'abord de saisir son ancien mot de passe pour vérifier son identité. Ensuite, il lui est demandé de saisir le nouveau mot de passe deux fois pour s'assurer qu'il a été correctement saisi. Si les deux saisies sont identiques, le système enregistre le nouveau mot de passe.

Seuls les utilisateurs ayant les droits d'administration (tels que l'utilisateur `root` dans Linux) peuvent utiliser la commande `passwd` pour changer les mots de passe des autres utilisateurs.

Il est généralement déconseillé d'utiliser la commande `passwd` dans un script, car cela nécessiterait de saisir le mot de passe manuellement à chaque fois que le script est exécuté, ce qui peut ne pas être pratique ou sûr.

Au lieu de cela, pour changer le mot de passe d'un utilisateur dans un script, il est recommandé d'utiliser la commande chpasswd. Cette commande permet de changer le mot de passe d'un utilisateur en fournissant le nom d'utilisateur et le nouveau mot de passe directement en ligne de commande ou en utilisant des fichiers de texte.

Changer son mot de passe

Pour changer votre mot de passe sous Linux en utilisant Bash, vous pouvez utiliser la commande `passwd`. Voici les étapes à suivre :

- Ouvrez un terminal Bash.
- Entrez la commande `passwd` suivie de votre nom d'utilisateur Linux. Si vous êtes déjà connecté sous votre propre compte, vous pouvez omettre le nom d'utilisateur et simplement taper `passwd` pour changer votre propre mot de passe.

```
passwd nom_utilisateur
```

- Vous serez alors invité à entrer votre mot de passe actuel pour vous authentifier.
- Ensuite, vous serez invité à saisir votre nouveau mot de passe deux fois, pour confirmer qu'il est correct.
- Une fois que vous avez entré votre nouveau mot de passe, celui-ci sera mis à jour.

Si tout s'est bien passé, vous devriez voir un message indiquant que votre mot de passe a été mis à jour avec succès. Vous pouvez maintenant utiliser votre nouveau mot de passe pour vous connecter à votre compte Linux.

Lorsque vous changez votre mot de passe sur un système Linux, il est important de mettre à jour tous les autres secrets qui l'utilisent. Voici une liste de certains des secrets qui peuvent nécessiter une mise à jour :

- Clés SSH : si vous utilisez des clés SSH pour vous connecter à des serveurs ou pour effectuer des opérations automatisées, vous devez mettre à jour les clés pour refléter votre nouveau mot de passe.
- Certificats SSL/TLS : si vous utilisez des certificats SSL/TLS pour sécuriser des connexions sur des sites web ou des applications, vous devez mettre à jour les certificats pour refléter votre nouveau mot de passe.
- Configuration de l'application : si vous utilisez une application qui stocke votre mot de passe, vous devez mettre à jour la configuration de l'application pour refléter votre nouveau mot de passe.
- Services tiers : si vous utilisez des services tiers tels que des services de stockage de fichiers en ligne, des services de messagerie, etc., vous devez mettre à jour les informations d'identification de votre compte pour refléter votre nouveau mot de passe.

Voici un exemple de script Bash qui vous permettra de mettre à jour plusieurs secrets après avoir changé votre mot de passe :

```
#!/bin/bash

# Mettre à jour les clés SSH
for keyfile in ~/.ssh/*
do
    if ssh-keygen -y -f "$keyfile" >/dev/null 2>&1 ; then
        echo "Mise à jour du mot de passe pour la clé : $keyfile"
        pwfile="${keyfile}.password"
        if [ -f "$pwfile" ]; then
            password=$(cat "$pwfile")
        else
            password=$(openssl rand -base64 32 | tr -d '=')
        fi
        echo "$password" > "$pwfile"
        chmod 600 "$pwfile"
        ssh-keygen -p -P "$password" -f "$keyfile"
    fi
done

# Mettre à jour les certificats SSL/TLS
# (vous devez remplacer les noms de fichiers et de dossiers par les vôtres)
sudo openssl rsa -in /etc/ssl/private/server.key -out
/etc/ssl/private/server.key
sudo openssl req -key /etc/ssl/private/server.key -new -out
/etc/ssl/certs/server.csr
sudo openssl x509 -req -days 365 -in /etc/ssl/certs/server.csr -signkey
/etc/ssl/private/server.key -out /etc/ssl/certs/server.crt

# Mettre à jour la configuration de l'application
```

```
# (vous devez remplacer les noms de fichiers et de dossiers par les vôtres)
sudo sed -i 's/ancien_mot_de_passe/nouveau_mot_de_passe/g'
/etc/application/config.ini

# Mettre à jour les informations d'identification pour les services tiers
# (vous devez remplacer les noms d'utilisateur et les mots de passe par les
vôtres)
echo 'ancien_nom_utilisateur:ancien_mot_de_passe' | sudo chpasswd
echo 'nouveau_nom_utilisateur:nouveau_mot_de_passe' | sudo chpasswd
```

Ce script utilise les commandes standard Linux pour mettre à jour les secrets courants qui peuvent nécessiter une mise à jour. Vous devez remplacer les noms de fichiers, de dossiers, d'utilisateurs, de mots de passe et autres informations par les vôtres. Vous pouvez également ajouter ou supprimer des commandes en fonction de vos besoins spécifiques.

Notez que certaines commandes dans ce script nécessitent des privilèges d'administration, vous devrez donc peut-être exécuter le script avec le compte d'utilisateur ayant ces privilèges ou utiliser la commande `sudo`.

Créer un compte utilisateur

Pour créer un compte utilisateur, il est nécessaire d'utiliser le commande `passwd`. Consultez la page concernant la commande useradd.

Forcer un utilisateur à changer son mot de passe au prochain démarrage

Sous Linux, vous pouvez utiliser la commande “**passwd**” avec l'option “-e” pour forcer un utilisateur à changer son mot de passe au prochain démarrage. La commande est généralement utilisée par un administrateur pour changer le mot de passe d'un utilisateur. Voici un exemple :

```
sudo passwd -e <username>
```

Cela forcera l'utilisateur <username> à changer son mot de passe lors de sa prochaine connexion. À noter que cette commande n'affectera pas les utilisateurs connectés en ce moment.

Vous pouvez vérifier le fichier de `/etc/shadow` contenant les informations cryptées des utilisateurs, que la date (en jours depuis le 1er janvier 1970) à laquelle le mot de passe a été modifié pour la dernière fois soit à la valeur 0.

```
sudo cat /etc/shadow | grep <username>
```

Vous pouvez utiliser la commande `chage` avec l'option `-l` pour afficher les informations de l'utilisateur, et vérifier que la date d'expiration du mot de passe est définie sur la mention `password must be changed` / `le mot de passe doit être changé` apparaisse.

```
sudo chage -l <username>
```

Vous pouvez utiliser la commande `passwd` avec l'option `-S` pour vérifier les informations de l'utilisateur, et vérifier que la date d'expiration du mot de passe est définie sur un jour antérieur à aujourd'hui (par exemple le `1970-01-01`) .

```
sudo passwd -S <username>
```

Changer de mot de passe dans un script

Voir la commande chpasswd