Pour mettre en œuvre une politique de mot de passe forte sur un système Linux, nous allons configurer des règles de complexité pour les mots de passe et utiliser les commandes `passwd` pour changer les mots de passe et `chage` pour gérer les expirations.

Configuration des règles de complexité des mots de passe

Les règles de complexité des mots de passe sont généralement configurées dans le fichier `/etc/security/pwquality.conf` sur les distributions Linux utilisant PAM (Pluggable Authentication Modules).

Étape 1 : Installation des outils nécessaires

Assurez-vous que les outils `libpwquality` sont installés sur votre système. Si ce n'est pas le cas, installez-les à l'aide de votre gestionnaire de paquets. Par exemple, sur Ubuntu ou Debian, vous pouvez installer `libpam-pwquality` :

```
sudo apt-get update
sudo apt-get install libpam-pwquality
```

Étape 2 : Configuration des règles de complexité des mots de passe

1. Ouvrez le fichier de configuration `/etc/security/pwquality.conf` en tant qu'administrateur dans un éditeur de texte. Par exemple :

   ```
   sudo nano /etc/security/pwquality.conf
   ```

2. Vous pouvez configurer divers paramètres de complexité des mots de passe dans ce fichier. Par exemple, définir les règles suivantes :

   ```
   # Minimiser la longueur du mot de passe
   minlen = 8

   # Exiger au moins une majuscule
   ucredit = -1

   # Exiger au moins une minuscule
   lcredit = -1

   # Exiger au moins un chiffre
   dcredit = -1

   # Exiger au moins un caractère spécial
   ocredit = -1
   ```

- `minlen`: Définit la longueur minimale du mot de passe.
- `ucredit`, `lcredit`, `dcredit`, `ocredit`: Spécifiez les exigences pour les majuscules, minuscules, chiffres et caractères spéciaux respectivement. La valeur `-1` signifie que l'élément est requis mais pas pénalisé s'il est absent.

3. Enregistrez et fermez le fichier après avoir effectué les modifications.

Étape 3 : Appliquer la politique de mot de passe

Après avoir configuré `pwquality.conf`, vous devez également vérifier que PAM est configuré pour utiliser ces règles. Cela se fait généralement via le fichier de configuration PAM approprié, comme `/etc/pam.d/common-password` sur de nombreuses distributions.

1. Ouvrez le fichier `/etc/pam.d/common-password` :

```
sudo nano /etc/pam.d/common-password
```

2. Assurez-vous que la ligne qui inclut `pam_pwquality.so` est présente et décommentée (sans le symbole `#` au début) :

```
password   requisite   pam_pwquality.so retry=3
```

   Cette ligne indique à PAM d'utiliser `libpwquality` pour vérifier la qualité des mots de passe en fonction des règles que vous avez configurées dans `pwquality.conf`.

3. Enregistrez et fermez le fichier après avoir effectué les modifications.

Gestion des mots de passe et expirations

Maintenant que vous avez configuré les règles de complexité des mots de passe, vous pouvez utiliser les commandes suivantes pour changer les mots de passe et gérer leurs expirations :

Changer un mot de passe utilisateur avec `passwd`

Pour changer le mot de passe d'un utilisateur (par exemple, `user1`), utilisez la commande `passwd` :

```
sudo passwd user1
```

Vous serez invité à saisir le nouveau mot de passe selon les règles de complexité que vous avez définies.

Gérer l'expiration des mots de passe avec `chage`

La commande `chage` est utilisée pour modifier les paramètres d'expiration du mot de passe d'un utilisateur. Par exemple, pour définir une expiration de mot de passe pour l'utilisateur `user1`, utilisez :

```
sudo chage -d 0 user1
```

Cela configure l'expiration du mot de passe de `user1` pour le prochain login, ce qui signifie que l'utilisateur devra changer son mot de passe lors de la prochaine connexion.

Conclusion

En suivant ces étapes, vous pouvez mettre en œuvre une politique de mot de passe robuste sur votre système Linux, en configurant des règles de complexité avec `pwquality.conf`, en utilisant `passwd` pour changer les mots de passe et `chage` pour gérer les expirations. Cela contribue à renforcer la sécurité de votre système en protégeant les comptes utilisateurs avec des mots de passe forts et régulièrement mis à jour.