Comment définir la politique de mot de passe sur Linux


La gestion des logins est l'un des emplois les plus critiques des administrateurs système.
En particulier, la sécurité des mots de passe doit être considérée comme la principale préoccupation pour tout système Linux sécurisé.
Je vais décrire comment configurer la politique de mot de passe sur Linux.


Je suppose que vous utilisez PAM (Pluggable Authentication Modules) sur votre système Linux, ce qui est le cas sur toutes les distributions récentes de Linux.

Preparation

Installer le module PAM `cracklib` pour activer le support, il peut fournir des capacités de contrôle de mot de passe supplémentaires.
Sur Debian ou équivalent :

```
aptitude install  libpam-cracklib
```


Le module PAM `cracklib` est installé par défault sur CentOS ou équivalent, donc l'installation de cette module n'est pas nécessaire sur ces distribution.

Empêcher la réutilisation d'anciens mots de passe

Pour appliquer une politique de mot de passe, nous avons besoin de modifier un fichier de configuration PAM liées à l'authentification situé à `/etc/pam.d`.
Le changement de politique prendra effet immédiatement après le changement.


Notez que les règles de mot de passe présentés dans cette article seront appliquées uniquement lorsque les logins non-root modifies leurs mots de passe, mais pas avec le privilège root.

Recherchez une ligne qui contient à la fois `password` et `pam_unix.so` et ajouter `remember=3` à cette ligne.
Elle permettra d'éviter que l'utilisateur reprenne les trois mots de passe les plus récemment utilisés (en les stockant dans `/etc/security/opasswd`).

Sur Debian ou équivalent :

```
 vim /etc/pam.d/common-password
```

```
 password     [success=1 default=ignore]    pam_unix.so obscure sha512
remember=3
```

Sur CentOs ou équivalent :

```
 vim /etc/pam.d/system-auth
```

```
 password   sufficient   pam_unix.so sha512 shadow nullok try_first_pass
use_authtok remember=3
```

Définir la taille minimum du mot de passe

Recherchez une ligne qui contient à la fois `password` et `pam_cracklib.so` et ajouter `minlen=10` à cette ligne.
Cela va appliquer un mot de passe d'une longueur (10 - <# de types>), où <# de types> indique combien de types de caractères différents sont utilisés dans le mot de passe.
Il existe quatre types (majuscules, minuscules, numériques et symboles) de caractères.
Donc, si vous utilisez une combinaison de tous les types et que `minlen` est fixée à 10, le mot de passe le plus court autorisé serait 6 caractères.

Sur Debian ou équivalent :

```
vim /etc/pam.d/common-password
```

```
password   requisite    pam_cracklib.so retry=3 minlen=10 difok=3
```

Sur CentOS ou équivalent :

```
vim /etc/pam.d/system-auth
```

```
password   requisite   pam_cracklib.so retry=3 difok=3 minlen=10
```

Définir la complexité du mot de passe

Recherchez une ligne qui contient `password` et `pam_cracklib.so` et ajouter `ucredit = -1 lcredit = -2 dcredit = -1 ocredit = -1` à cette ligne.
Cela va forcer qu'il y est au moins une lettre majuscule (ucredit), deux lettres minuscules (lcredit), un chiffre (dcredit) et un symbole (ocredit) dans le mot de passe.

Sur Debian ou équivalent :

```
vim /etc/pam.d/common-password
```

```
password   requisite    pam_cracklib.so retry=3 minlen=10 difok=3 ucredit=-1
lcredit=-2 dcredit=-1 ocredit=-1
```

Sur Centos ou équivalent :

```
vim /etc/pam.d/system-auth
```

```
password   requisite   pam_cracklib.so retry=3 difok=3 minlen=10 ucredit=-1
lcredit=-2 dcredit=-1 ocredit=-1
```

Définir la période d’expiration du mot de passe

Pour définir la période de validité du mot de passe actuel, modifier les variables suivantes de `/etc/login.defs`.

```
vim /etc/login.defs
```

```
PASS_MAX_DAYS   150
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

Cela va forcer tous les utilisateurs à changer leur mot de passe une fois tous les six mois et envoyer un message d'avertissement sept jours avant l'expiration du mot de passe.

Si vous souhaitez définir une période de péremption sur chaque utilisateur, utilisez la commande chage au lieu de cela.
Pour voir la politique d'expiration de mot de passe pour un utilisateur spécifique :

```
chage -l toto
```

```
Dernier changement de mot de passe                                        :
oct. 21, 2015
Fin de validité du mot de passe                                    : jamais
Mot de passe désactivé                                       : jamais
Fin de validité du compte                                                 :
jamais
Nombre minimum de jours entre les changements de mot de passe           : 0
Nombre maximum de jours entre les changements de mot de passe           :
99999
Nombre de jours d'avertissement avant la fin de validité du mot de passe
: 7
```

Par défaut les mots de passe n’expire jamais

Pour changer la période de péremption du mot de passe de toto :

```
 chage -E 8/25/2015 -m 5 -M 90 -I 30 -W 14 toto
```

La commande ci-dessus fais expiré le mot de passe le 25/08/2015.
Le nombre maximum/minimum de jours entre les changements de mot de passe est réglé sur 5 et 90.
Le compte sera bloqué 30 jours après l'expiration d'un mot de passe et un message d'avertissement sera envoyé 14 jours avant l'expiration du mot de passe.

Pour désactivé le changement de mot de passe pour un login utilisez ça:

```
chage -I -1 -m 0 -M 99999 -E -1 toto
```

avec la commande chage vous pouvez vérifier

```
# chage -l toto
Last password change                    : oct. 21, 2015
Password expires                        : jamais
Password inactive                       : jamais
Account expires                         : jamais
Minimum number of days between password change      : 0
Maximum number of days between password change      : 99999
Number of days of warning before password expires   : 28
```

Source :xmodulo.com