pam_pwhistory

Autoriser l'accès en utilisant le fichier .pwhistory

Ce module sauve les derniers mots de passe pour chaque utilisateur dans le but de forcer l'historique de changement de mot de passe et empêcher l'utilisateur d'alterner entre les même mots de passe trop fréquemment. Ce module ne fonctionne pas avec kerberos. En général, il n'a aucun sens en conjonction avec NIS ou LDAP, vu que les anciens mot de passe sont stockés sur la machine local et ne sont pas disponible sur une autre machine. Ne fournis que le type de module password.

OPTIONS

debug syslog les informations de debuggage

use_authtok En changeant de mot de passe, force à utiliser le nouveau mot de passe fournis par un module précédent (par exemple pam_cracklib)

enforce_for_root La vérification est forcée également pour root

remember=N Sauve les derniers N mots de passe dans **/etc/security/opasswd**. Défaut 10.

retry=N Demande à l'utilisateur N fois avant de retourner une erreur. Défaut 1.

authtok_type=STRING voir pam_get_authtok pour plus de détails

Valeurs retournées

PAM_AUTHTOK_ERR Aucun nouveau motde passe n'a été rentré, l'utilisateur a annulé le changement demot de passe ou le nouveau mot de passe ne peut pas être changé

PAM_IGNORE l'historique des mots de passe est désactivé

PAM_MAXTRIES Le mot de passe a été rejeté trop de fois

PAM_USER_UNKNOWN Utilisateur inconnus

Exemples

exemple de section password
password required pam_pwhistory.so
password required pam_unix.so use_authtok
En combinaison avec pam_cracklib
password required pam_cracklib.so retry=3
password required pam_pwhistory.so use_auththok
password required pam_unix.so use_authtok