pam_tally2

Module compteur de login

Ce module maintient un compteur de tentative d'accès, peut ré-initialiser ce compteur en cas de succès et peut refuser l'accès si trop de tentatives échouent.

pam_tally2 est composé de 2 parties : **pam_tally2.so** et **pam_tally2**. Ce dernier est une application optionnelle qui peut être utilisé pour interroger et manipuler le fichier compteur. Il peut afficher le compteur de l'utilisateur, définir les compteurs individuels ou reset tous les compteurs Définir des compteurs élevés peut être utile pour bloquer les utilisateurs sans changer leur mot de passe. Par exemple, il peut être utile effacer tous les compteurs à minuit depuis un cron.

Normalement, les tentatives échouées au compte root ne bloque pas ce compte, pour prévenir les DOS. Fournit les types de module auth et account.

Options globales

Peuvent être utilisées par les types de module auth et account.

onerr=fail Si quelque-chose se produit (comme l'impossibilité d'ouvrir le fichier), retourne PAM_SUCCESS si onerr=succeed.

file=/path/to/counter Fichier où sont conservés les compteurs

audit log les noms d'utilisateurs qui ne sont pas trouvés

silent mode silencieux

no_log_info ne syslog rien

Options Auth

La phase d'authentification incrémente d'abord le compteur de tentative de login et vérifie si l'utilisateur devrait avoir l'accès refusé. Si l'utilisateur est authentifié et le processus de login continus à l'appel pam_setcred, le compteur est ré-initialisé.

deny=n Refuse l'accès si le compteur excède N tentatives.

lock_time=n Refuse toujours après n secondes après qu'une tentative échoue

unlock_time=n Autorise l'accès après n secondes après une tentative échouée. Si cette option est utilisée l'utilisateur sera bloqué pendant la durée de temps spécifiée après avoir dépassé le nombre de tentative maximum. Sinon le compte est bloqué jusqu'à ce qu'il soit débloqué manuellement

magic_root Si le module est invoqué par une utilisateur d'uid=0 le compteur n'est pas incrémenté.

no_lock_time N'utilise pas le champs **.fail_locktime** dans **/var/log/faillog** pour cet utilisateur

even_deny_root Le compte root peut devenir indisponible

root_unlock_time=n Cette option implique **even_root**. Autorise l'accès après n secondes au compte root après une tentative échouée.

serialize Sérialise l'accès au fichier compteur utilisant les locks. Cette options peut être utilisée seulement pour les services non-multi-threads parce qu'il dépend du fcntl locking dans le fichier compteur. C'est également une bonne idée d'utiliser cette option seulement dans des configuration où le temps entre la phase auth et la phase account ou setcred n'est pas dépendant du client. Sinon le client sera capable de prévenir les authentification simultanées par le même utilisateur en prolongeant artificiellement le temps que le fichier lock.

Options Account

La phase account ré-initialise le compteur de tentatives si l'utilisateur n'est pas root. Cette phase peut être utilisée optionnellement pour les services qui n'appellent pas pam_setcred correctement ou si le reset devrait être fait sans regarder les échecs de la phase account des autres modules.

magic_root Si le module est invoqué par un utilisateur avec uid=0 le compteur n'est pas changé. Le sysadmin devrait l'utiliser pour les services utilisateurs, comme su, sinon cet argument devrait être omis.

Valeurs retournées

PAM_AUTH_ERR option invalide, le module ne peut pas retrouver le nom d'utilisateur, compteur invalide, fichier non trouvé ou trop de logins échoués

PAM_SUCCESS Tous est ok

PAM_USER_UNKNOWN Utilisateur inconnus

Exemples

Exemple de /etc/pam.d/login pour bloquer le compte au bout de 4 tentatives. Le root ne sera pas bloqué. Le compte sera débloqué après 20 minutes. Le module n'a pas à être appelé dans la phase account parce que login appelle pam_setcred correctement

```
auth required pam_securetty.so
auth required pam_tally2.so deny=4 even_deny_root unlock_time=1200
auth required pam_env.so
auth required pam_unix.so
auth required pam_nologin.so
account required pam_unix.so
password required pam_unix.so
session required pam_limits.so
session required pam_unix.so
session required pam_lastlog.so nowtmp
session optional pam_mail.so standard
```