pam_limits

Limiter les ressources

pam_limits définit les limites des ressources système qui peuvent être obtenues dans une session utilisateur. Les utilisateurs uid=0 sont affectés par cette limite également. Par défaut, les limites sont définies dans **/etc/security/limits.conf**, puis les fichiers *.conf dans **/etc/security/limits.d/**. Ce module ne doit pas être appelé avec une application multi-thread.

Si Linux-PAM est compilé avec le support audit, le module report quand il refuse l'accès basé sur une limite du nombre maximum d'utilisateurs de sessions login courante. Ne fournit que le type de module session.

Description de la configuration

<domain> <type> <item> <value>

domain un utilisateur, un @groupe, '*' pour l'entrée par défaut et '%' pour la limite maxlogins uniquement, peut aussi être utilisée avec la syntaxe %groupe

type hard, soft et '-' le dernier force les 2 limites ensemble

item Peut avoir les éléments suivant :

- **core** limite la taille du fichier core (Ko)
- **data** taille de donnée maximum (Ko)
- **fsize** taille de fichier max (Ko)
- **memlock** allocation mémoire max (Ko)
- **nofile** nombre max de fichiers ouverts
- **stack** taille de pile max (Ko)
- **cpu** nombre de CPU
- **nproc** nombre max de processus
- **as** limite d'espace d'adresse (Ko)
- **maxlogins** nombre max de logins pour cet utilisateur (sauf pour uid=0)
- **maxsyslogins** Nombre max de logins sur le système
- **priority** (priorité du processus utilitateur)
- **locks** nombre max de fichiers lockés
- **sigpending** nombre max de signaux en suspend
- **msqueue** mémoire max utilisée par la queue de message POSIX
- **nice** priorité nice max autorisé
- **rtprio** priorité realtime max pour les processus non-privilégiés

toutes les valeurs peuvent être **-1**, **unlimited** ou **infinity** sauf pour priority et nice

OPTIONS

change_uid change le real uid de l'utilisateur pour qui les limites sont définies.

conf=/path/to/limits.conf Spécifie l'emplacement du fichier de limites

debug Affiche des informations de debugage

utmp_early certains applications cassés allouent une entrée utmp pour l'utilisateur avant que l'utilisateur soit admis sur le système. si certains services configurés pour faire çà, vous pouvez sélectivement utiliser cet argument pour compenser ce fonctionnement.

noaudit Ne rapporte pas les excès de logins au système d'audit

Valeurs retournées

PAM_ABORT Ne peut pas avoir les limites

PAM_IGNORE Aucune limite trouvée pour l'utilisateur

PAM_PERM_DENIED les nouvelles limites ne peuvent pas être définies

PAM_SERVICE_ERR Ne peut pas lire le fichier de config

PAM_SUCCESS Les limites ont été changés

Exemples

*** soft core 0**
*** hard rss 10000**
@student hard nproc 20
@faculty soft nproc 20
@faculty hard nproc 50
ftphard nproc 0
@student - maxlogins 4