pam_access

Module de contrôle d'accès

Ce module est principalement utilisé pour la gestion d'accès. Il fournit contrôle d'accès de login style logdaemon sur les noms de logins, hôtes ou noms de domaines, les adresses internet ou réseaux ou nom de lignes terminal. Les règles d'accès par défaut sont pris dans **/etc/security/access.conf**. Si PAM est compilé avec le support d'audit, le module reporte quand il refuse l'accès basé sur l'origine (hôte ou tty).

Le fichier de règles par défaut spécifie des combinaisons (**user/group, host**) (**user/group, network/mask**) (**user/group, tty**) pour qu'un login soit accèpté ou refusé. L'ordre est important, le module s'arrête à la première correspondance trouvée. Chaque ligne possède la syntaxe suivante :

permission :users/groups :origins

- Le premier champs est soit '+' pour authoriser l'accès soit '-' pour l'interdire.
- Le second champ est une liste d'un ou plusieurs noms de login, groups, ou ALL. Pour différencier les noms des groupes, les groupes sont écris entre parenthèses.
- Le troisième champ est une liste de noms tty, noms d'hôtes, noms de domaines (commençant par '.'), numéros de réseau (se termine par '.'), addresse réseaux avec le masque, ALL ou LOCAL qui correspond uniquement si PAM_RHOST n'est pas définis et le champs origin est définis depuis PAM_TTY ou PAM_SERVICE. Il est possible d'utiliser @netgroupname dans l'hôte ou les pattern utilisateur.
- L'opérateur EXCEPT permet d'écrire des règles compacte.
- Si **nodefgroup** n'est pas définis, le fichier group est recherché quand un nom ne correspond pas à l'utilisateur. Seul les groupes qui correspondant à de tels utilisateurs sont explicitement listés.

OPTIONS

accessfile=/path/to/access.conf Spécifie le fichier de règles à utiliser

debug syslog de nombreuses informations

noaudit Ne report pas les logins des hôtes et tty non autorisés dans le sous-système d'audit.

fieldsep=separators Modifie le séparateur par défaut

listsep=separators Modifie le séparateur de listes

nodefgroup Les tokens utilisateurs qui ne sont pas entre parenthèse ne correspondent jamais aux groupes

Codes de retour

PAM_SUCCESS accès autorisé

PAM_PERM_DENIED Accès non autorisé

PAM_IGNORE pam_setcred a été appelé et ne fait rien

PAM_ABORT Aucune donnée ou option ne peut être donné.

PAM_USER_UNKNOWN utilisateur inconnus du système

Exemples

l'utilisateur root devrait toujours être autorisé à accéder à cron, X11, et les tty
+ :root :crond :0 tty1 tty2 tty3 tty4 tty5 tty6
root devrait avoir accès depuis les hôtes qui ont une IPv4
+ :root :192.168.200.1 192.168.200.4 192.168.200.9
+ :root :127.0.0.1
root devrait avoir accès depuis les réseau 192.168.201.0
+ :root :192.168.201.
ou
+ :root :192.168.201.0/24
ou
+ :root :192.168.201.0/255.255.255.0.
root devrait avoir accès depuis les hôtes foo1.bar.org et foo2.bar.org
+ :root :foo1.bar.org foo2.bar.org
root devrait avoir accès depuis le domaine foo.bar.org
+ :root :.foo.bar.org
root ne devrait pas avoir accès à toutes les ressources
- :root :ALL
l'utilisateur foo et le groups admins devraitent avoir accès à toutes les sources
+ :@admins foo :ALL
Les utilisateurs john et foo devraient avoir accès depuis une adresse IPv6
+ :john foo :2001 :db8 :0 :101 : :1
john devrait avoir accès depuis le réseau IPv6
+ :john :2001 :db8 :0 :101 : :/64
interdire les logins console à tout le monde sauf shutdown, sync et tous les autres comptes, qui sont membre du groupe wheel
- :ALL EXCEPT (wheel) shutdown sync :LOCAL
Tous les autres utilisateurs devraient être refusés depuis toutes les autres sources
- :ALL :ALL