

Memo PAM = Pluggable Authentication

PAM INFO PAM: Pluggable Authentication Modules c'est un système unifié de délégation de l'authentification. But: Les applications qui le souhaitent peuvent déléguer au système la gestion de l'authentification. PAM fournit une API en langage C aux applications. Tous les services utilisent PAM. Conséquence et Intérêts: - c'est donc l'administrateur système qui a le contrôle sur le mode d'authentification des applications - finesse de configuration au niveau de chaque application - Cela permet d'étendre sans difficultés les modes d'authentification de chaque application

schéma global: +-----+ | application: X | +-----+ / +-----+ +-----+
|authentification-[--->--\--] Linux |--<--|fichier config PAM| | + [---<--\--] PAM | |danss /etc/pam.d/X| | [conversa
| | |=====| +-----+ | / +-n--n-----+ | auth .. pam_a.so | | service user | | |
+-----+ A | | | ... / | V A | | |-----+ +-----+
-[b]--[c] +-----+ | acct.... |--[b]--[d] +-----+
c] +-----+ \...../ sous /lib/security sous le répertoire /etc/pam.d/ il exi
su,xdm,ssh,ftp,samba,passwd Attention il existe aussi /etc/pam.conf --> obsolete! **FORMAT FICHIER PAM**

SYNTAXE ===== format des
fichiers PAM: [phase] [mot de controle] [module] [args] | | | | | -auth | -required |
requisite | | -en commun: debug | -session | -suffisant | +-en commun: use_first_pass +-password +-
pam_xxx.so Exemple: auth required pam_unix.so shadow nullok use_first_pass password required pam_u
nullok obscure min=4 max=8 md5 Arguments optionnels génériques (commun a tous les modules) -----
----- - Debug

utilise syslog pour logger des information de debugage
sous debian/ubuntu, c'est sous /var/log/auth.log - use_first_pass
réutilise le token d'authentification (le mot de passe) du module precedent
en cas d'empilement de modules. **DEFINITION DES PHASES**

===== auth mode
d'authentification de l'utilisateur (par mdp ou autre méthode). (correspond à pam_authenticate()) account Utilisé
pour s'assurer que l'accès est autorisé. Restriction du compte : expiration, en fonction de l'heure, de la machine
source, des ressources disponibles (pam_acct_mgmt()) password Gestion du mots de passe.
(pam_chauthtok()).mode de verification, peut etre utilisé pour changer les mots de passe à traver les applications
session Evenements juste avant l'utilisation du service (par ex ouverture d'une session), et juste après. par ex monter
le repertoire home, afficher un message. **EMPILEMENT DE MODULES (MOTS DE CONTROLE)**
===== * suffisant: est suffisant
pour valider l'authentification. Si le module répond OK, on a immédiatement une acceptation quelquesoit la ré
des autres modules de la phase * required: Doit réussir pour valider l'authentification, mais les autres modules
testés malgré tout. * requisite: Doit réussir pour valider l'authentification, différence par rapport à
d'echec, on ne continue pas à tester les autres modules * optional: l'execution du module n'affecte pas
l'authentification. **PARTIES COMMUNES (inclusion de fichier)**

===== PAM permet d'inclure
des fichiers dans les fichiers de config. directive: @include fichier c'est utilisé pour gérer des parties commune dans
l'authentification des services, c'est à dire l'execution de modules pour tous les services. Quand on modifie un fichier
PAM, il faut donc se poser la question: - spécifique à la commande que j'edite ou commun? **MODULES PAM**
STANDARDS SECTION AUTH

===== pam_securetty.so assure
que root ne peut se connecter que sur les consoles tty definis dans /etc/securetty pam_unix.so utiliser
unix : /etc/passwd et /etc/shadow. option nullok : indiquer qu'on accepte les passwd vide pam_p
pam_nologin.so si /etc/nologin existe, seul root peut se logger le contenu de /etc/nologin est affiché si essai
pam_env.so charge les des variables d'environnements présentes dans /etc/security/pam_env.conf

ACCOUNT =====
pam_unix.so fait les verifs standards/établi la validité utilisateur ou mot de passe (account expiré,change pa
forcé) **SECTION PASSWORD**

===== pam_cracklib.so quand
on change un password, vérifie que le mot de passe n'est pas dans un dictionnaire option retry=
tentatives) minlen=n (la longueur imposée-ne peut être inférieur à 4) difok=n (nombre de
l'ancien et le nouveau) va aussi gérer la durée de validité du mdp. Plus de détails: voir la rubrique
fin du support pam_unix.so politique d'authentification au standard unix options: -shad
shadow) -nullok (passwd vide ok) -use_authtok (utilise le passwd accepte par le
md5 pour le type de cryptage -remember=n pour se souvenir des n derniers mdp utilisés

===== pam_unix.so
envoie un log dans /var/log/messages) pam_limits.so Permet de limiter les ressources mis à la disposition
utilisateur (process,memoire..) quotas defini dans /etc/security/limits.conf pam_lastlog.so affiche la date de
login, ou d'echec pam_motd.so affiche le "message of the day", en general ce sont des infos sur le syste
AUTRES MODULES PAM CLASSIQUES pam_time (account): autorise un accès par heure. La configuration se
faisant dans le fichier /etc/security/time.conf. pam_wheel : permet de limiter l'accès à root via la commande su qu'aux
seuls membres du groupe wheel. On peut changer le nom du groupe par défaut avec l'option group=mon_group.

pam_warm : log les informations à syslog pam_console : permet de spécifier les autorisations d'accès à la console. Il faut alors configurer /etc/security/console.perms. EXEMPLES DE FICHIER PAM PAM POUR SU

```
=====
sufficient pam_ldap.so          # This allows root to su without passwords (normal operation)
auth    required pam_unix.so shadow nullok use_first_pass
pam_unix.so          password sufficient pam_ldap.so nullok md5
max=8 md5            session required pam_unix.so          PAM POUR LOGIN
=====
sufficient pam_ldap.so          auth    required pam_nologin.so          auth    required pam_unix.so shadow nullok use_
required pam_env.so            account sufficient pam_ldap.so          account required pam_unix.so
pam_ldap.so nullok md5          password required pam_unix.so nullok obscure min=4 max=8 md5
pam_unix.so          session optional pam_lastlog.so          session optional pam_motd.so          session optional
noenv    SELECTION DE MODULES PAM ADDITIONNELS    Radius : module PAM associé à FreeRADIUS Server
http://www.freeradius.org/pam_radius_auth    OTP: (One-time password) authentication    * pam_sotp:
http://www.cavecanen.org/cs/projects/pam_sotp/    * module PAM-OPIE : http://www.tho.org/~andy/pam-opie.html    voir
aussi http://www.inner.net/pub/opie    * OTPW (http://www.cl.cam.ac.uk/~mgk25/otpw.html)    USB dongle:
http://usbauth.delta-xi.net/doku.php    placer une clé USB pour éviter de taper les mdp    PAM BlueTooth: idem avec un
peripherique BlueTooth    http://pam.0xdef.net/    authentification base de données SQL:    * Postgres SQL
http://www.kernel.org/pub/linux/libs/pam/pre/modules    http://freshmeat.net/projects/pam_pgsql/download    * MySQL
http://sourceforge.net/projects/pam-mysql/    pam_require: module de type "account" qui permet de limiter à un utilis
ou un groupe l'accès à un service (par exemple sur pam pour SSH limité à un groupe admin et à root)    pam_user_auth:
permet different type d'authentification selon l'utilisateur    http://www-dev.cites.uiuc.edu/pam/    pam_ldap : permet
d'effectuer l'authentification sur une base ldap.    REFERENCES    page Linux-PAM
http://www.kernel.org/pub/linux/libs/pam/    PAM CRACKLIB    http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-
html/sag-pam_cracklib.html    Le guide Administrateur Systeme de Linux PAM
http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html    La liste des modules Linux-PAM
http://www.kernel.org/pub/linux/libs/pam/modules.html
```