**PAM**

|  |  |  |  |
| --- | --- | --- | --- |
| **DESC** | | | |
| Pluggable Authentication Modules  Système d’authentification centralisé des services | | | |
| **FILES** | | | |
| /lib64/security/ | | Bibliothèques PAM modules | |
| /etc/ | pam.d/ | Fichiers de configuration :  Chaque service nécessitant une authentification a son propre fichier | |
|  | nsswitch.conf | Configuration de NSS avec une entrée pour chaque service | |
|  | securetty | Limitation de l’accès à root pour certains tty via module pam\_securetty | |
|  | Security/ | Access.conf | Limitation des accès via module pam\_access |
|  |  | Group.conf | Limitation des groupes via pam\_group |
|  |  | Pam.env.conf | Définition variables d’env via pam\_env |
|  |  | Limits.conf | Limitation de ressource via pam\_linits |
|  |  | Time.conf | Limitation de temps via pam\_time |
|  | environment | Définition var d’env supplémentaires via pam\_env et le paramètre readenv=1 | |
|  | Systemd/logind.conf |  | |
| **QUICK START** | | | |
|  | | | |

**Généralités :**

* Permet de combiner des mécanismes d’authentification comme :
  + Fichiers locaux
  + LDAP
  + Active directory
  + Kerberos
  + Clef USB
  + Lecteur d’empreinte
* Chaque module est essayé une fois et on configure quoi faire si un des modules a échoué ou non.
* Scripts lors de la connexion/déconnexion
* Librairie utilisable par n’importe quelle application (librairies PAM pour tous les langages)
* Chaque application possède son service PAM dans /etc/pam.d/ qui lui dicte tous les modules à implémenter pour l’authentification : dès que le programme a besoin d’une authentification, chaque module PAM est invoqué.
* Evolution :
  + A l’origine, authentification sur la machine locale via les bibliothèques du système (/etc/passwd et /etc/shadow)
  + Puis NSS : On élargit les mécanismes d’authentification (LDAP, SQL, active directory…) mais ça reste les bibliothèques du système local qui authentifie.
  + Puis PAM : authentification plus forcément faite sur les bibliothèques du système, mais peut être faite à l’extérieur.
* Fonctionne avec NSS en sous-couche
* Lorsqu’une application ne possède pas son fichier PAM, elle va par défaut utiliser le fichier de configuration PAM "other" : on doit absolument refuser toute authentification dessus et le créer s’il n’existe pas.
* Logs de PAM sont confiés à Syslog

**Syntaxe d’un fichier de configuration PAM :**

#Commentaire

<Type\_module> <drapeau\_de\_controle> <path\_vers\_bibliothèque> [Options]

-<Type\_module> … #Pas logs si le module ne peut pas être chargé pour une raison X ou Y

|  |  |
| --- | --- |
| **Type de module** | **Comments** |
| auth | Authentification |
| account | Restriction du compte :   * expiration en fonction de l’heure, de la machine source, des ressources… * Validité du login/mdp pour ce type de service |
| password | Gestion mdp (expiration…) |
| session | Ouverture d’une session, avant et après |

|  |  |
| --- | --- |
| **Drapeau de contrôle** | **Comments** |
| required | Doit réussir mais on test les autres modules aussi. |
| requisite | Doit réussir. On ne lit pas les autres modules, échec est renvoyé immédiatement.. |
| optional | Est ignoré |
| sufficient | Test correct = acceptation immédiate  Echec = on continue la liste des modules |
| Include <Type> | Inclure toutes les lignes de la configuration PAM de type |
| substack | Idem include mais le fichier type à inclure est considéré comme un module complet |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bibliothèque** | **[Opts]** | **Comments** | |
| **AUTH** | | | |
| Pam\_sepermit.so | Login autorisé uniquement quand SE Linux est en mode enforcing | | |
| Pam\_env.so | Définit les variables d’environnements dans /etc/security/pam.env.conf à tout user qui se connecte | | |
| Pam\_faildelay.so | Timeout avant échec | | |
| Pam\_unix.so | Authentification standard unix (/etc/password et shadow) | | |
|  | nullok | | Par défaut accès refusé si le user qui se connecte ne possède pas de mpd.  Nullok permet d’outrepasser cette règle |
|  | Try\_first\_pass | | Essaye les mdp déjà utilisés par les modules d’avant |
| Pam\_suceed\_if.so | Module de test de conditions | | |
|  | Field>X | | Field = user|uid|gid|home|ruser|tty|service |
|  | Quiet\_sucess | | Pas de logs en cas de réussite du test |
| Pam\_ldap.so | LDAP | | |
| Pam\_krb5.so | Kerberos | | |
| Pam\_deny.so | Utiliser /etc/security/other pour définir politique si fichier de configuration PAM absent | | |
| **ACCOUNT** | | | |
| Pam\_nologin.so | Empêche un user de se connecté si le fichier /etc/nologin est présent  Uniquement root peut | | |
| **SESSION** | | | |
| Pam\_selinux.so | Définit le contexte de sécurité SE Linux pour le prochain Shell exécuté | | |
| Pam\_loginuid.so | Pour les logs d’audit | | |
| Pam\_namespace.so | Définit un espace de nom | | |
| **OTHER** | | | |
|  |  | | |
| Pam\_cracklib.so | Permet :   * De vérifier que le mdp ne se trouve pas dans un dictionnaire * Qu’il n’est pas réutilisé * Nombres de tentatives * Longueur imposée * #caractères de l’ancien mdp que l’on ne veut pas dans le nouveau | | |
|  |  | | |
| Pam\_time.so | Autorise un accès par heure via /etc/security/time.conf | | |
| Pam\_wheel.so | Autorise les accès à root que par les seuls membres du groupe wheel | | |
| Pam\_limits.so | Limite les ressources accordées à un user via /etc/security/limits.conf | | |
|  |  | | |
| Pam\_access.so | Contrôle des users par nom, machine, domaine, IP, tty via /etc/security/access.conf | | |
|  |  | | |
| Pam\_securetty.so | Vérifie que le compte root peut se connecter dans cette console via /etc/securetty | | |
| Pam\_warn.so | Log les informations à syslog | | |
| Pam\_console.So | Autorisation d’accès à la console via /etc/security/console.perms | | |
|  |  | | |
|  |  | | |
| Pam\_timestamp.so | Validité d’une session : une fois connecté, plus besoin de s’authentifier pendant X minutes. | | |
|  |  | | |