PAM

context

dit document beschrijft de werking van **P**luggable **A**uthentication **M**odules

werking

PAM is een set van modules waarmee je instelt hoe gebruikers zich op een programma authenticeren. Je kan dus **zelf** de module kiezen (zeg maar: de authenticatie methode) dat best past bij een bepaalde programma:

- Wil je dat op je jumphost alleen kan aangemeld worden met one-time password? Gebruike de Google Authenticator PAM module en het kan.
- mogen alleen gebruikers uit een bepaalde groep op je systeem aanmelden. PAM heeft daar een eigen module voor, dus het kan.
- volstaat een simpele trust en hoeft er niet geauthenticeerd te worden. PAM kan het ook!

PAM is dus je eerste halte als je authenticatie op Linux wilt instellen, gaande van trust tot high-tech retina scan, stemherkenning en OTP.

OPGELET! Zoals met elke configuratie van een authenticatie systeem moet je SUPER-voorzichtig zijn. Maak een fout en je kan mogelijks niet meer aanmelden. Zorg dus steeds voor EEN actieve sessie op je systeem waarop je de laatste (fatale) wijziging kunt terugdraaien.

De PAM modules die op je systeem beschikbaar zijn, vind je onder **/lib/x86_64-linux-gnu/security**
Een complete beschrijving van elke module vind je hier.

PAM kent 4 types (management) taken:

1. authentication: bepaalt welke authenticatie methode wordt gebruikt: wachtwoord, vingerafdruk, iris scan, …
2. account: bepaalt of de gebruiker mag aanmelden, het wachtwoord niet vervallen is, …
3. session: wat er moet gebeuren voor en na de authenticatie (home directory monteren, logon/logout loggen, …)
4. password: geeft aan hoe gebruikers hun wachtwoord kunnen wijzigen

In het configuratiebestand wordt aan deze taak een PAM module (en parameters) gekoppeld die

samen bepalen hoe wordt aangemeld.

Aan elke van deze taken wordt een zgn CONTROL toegekend. Deze geeft aan wat er moet gebeuren als de taak faalt:

1. requisite: breek de authenticatie af.
2. required: ga verder met de volgende modules, maar breek nadien authenticatie af.
3. sufficient: als authenticatie slaagt, wordt gebruiker aangemeld __zelfs als de overige (required) modules mislukten.
4. optional: slagen/mislukken van deze module is enkel belangrijk als het de enige service is.

configuratie

Alle bestanden bevinden zich in /etc/pam.d. Elk programma dat gebruikers authenticeert via een PAM-module heeft daar een eigen configuratiebestand met onderstaande syntax:

```
auth       required   pam_unix.so nulok
```

Deze verwijzen dus naar:

```
type  control  module-path  module-arguments
```

meer info

- Linux Documentation Project
- The Linux-PAM System Administrators' Guide

Linux