

Huiswerk Linux: installatie mod_auth_pam

We hebben in de vorige opdracht de *winbind* daemon geïnstalleerd om te kunnen communiceren met een Windows *Domain Controller*. Winbind geeft ons de mogelijkheid om Windows *Active Directory* functionaliteit in te zetten op een Linux machine (PAM). Apache is modulair opgebouwd. Omdat we Apache de logins van een Domain Controller willen gebruiken, moeten we de *mod_auth_pam* module installeren.

Over PAM

PAM (Pluggable Authentication Modules) is vergelijkbaar met de Windows *Active Directory* functionaliteit. PAM regelt niet alleen de login, maar ook wat er daarna moet gebeuren, zoals het starten van scripts of het instellen van de home directory in een Windows domein. PAM kent vier soorten functies:

Naam	omschrijving
auth	authenticatie: voert wachtwoordverificatie uit
account	account-management: regelt policies, zoals vervaldatum wachtwoord en/of <i>user profile</i>
session	sessie-management: logging, instellen home directory, starten scripts
password	wachtwoord-management: wijzigen wachtwoord

Installatie PAM modules

Het configureren van Linux doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator.

Cygwin gebruikers	Andere Linux gebruikers
<p>Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor Als administrator uitvoeren. Als Apache nog niet op je systeem staat, installeer dan eerst het <i>apache</i> pakket:</p> <pre>apt-get install apache</pre> <p>Installeer de Apache <i>mod_auth_pam</i> module:</p> <pre>apt-get install apache-mod_auth_pam</pre> <p>Zorg er ook voor dat de <i>winbind</i>-daemon draait. Dit doe je met het <i>service</i> programma:</p> <pre>service winbind start</pre>	<p>Sudo voor de overige Linux-smaken (<i>Ubuntu, Debian, Mint, etc.</i>): start een terminal met de toetsencombinatie: <Ctrl><Alt>-T. We gebruiken het commando <i>sudo</i> alleen om in te loggen met het <i>su</i> (super user) commando. Daardoor blijven we ingelogd:</p> <pre>sudo su</pre> <p>Als Apache nog niet op je systeem staat, installeer dan eerst het <i>apache2</i> pakket:</p> <pre>apt install apache2</pre> <p>Installeer de Apache module voor PAM (<i>mod_authnz_pam</i>):</p> <pre>apt install libapache2-mod-authnz-pam</pre> <p>Installeer de Winbind module voor PAM (<i>libpam-winbind</i>):</p> <pre>apt install libpam-winbind</pre>

PAM configureren

De PAM module voor Apache is geïnstalleerd. We moeten nu aangeven dat we de Domain Controller willen raadplegen voor de gebruiker-logins. Open het configuratiebestand met de *vi* editor:

```
vi /etc/pam.d/httpd
```

Het kan zijn dat je een leeg scherm ziet. We hebben in ieder geval de volgende regels nodig. Toets **i** (insert) om naar de *INSERT* modus te gaan. Zorg dat de instellingen er als volgt uitzien:

```
##PAM-1.0
auth      required  pam_winbind.so
account   required  pam_permit.so
```

Door deze wijziging geven we aan dat de authenticatie via de *winbind* daemon (dus via onze Domain Controller) moet worden uitgevoerd.

Toets **<Esc>** om uit de *INSERT* modus te komen en geef de commando's *w* (write) en *q* (quit):

```
:wq
```

Het bestand wordt nu opgeslagen en we zijn terug op de commando prompt.

Apache configureren

We hebben vorige keer alleen de localhost als VirtualHost ingesteld. Daar deze van buiten niet bereikbaar is, gaan we nu ook onze laptop als VirtualHost instellen.

<h3>Cygwin gebruikers</h3> <p>In een Cygwin distributie staan de Apache configuratiebestanden in de <i>/etc/httpd</i> map. Zorg ervoor dat je in die directory staat:</p> <pre>cd /etc/httpd</pre>	<h3>Andere Linux gebruikers</h3> <p>De Apache configuratiebestanden van Debian distributies (<i>Ubuntu, Knoppix, Kali, etc.</i>) staan in <i>/etc/apache2</i>. Ga in de map <i>sites-enabled</i> staan:</p> <pre>cd /etc/apache2/sites-enabled</pre> <p>Op Slackware distributies, zoals <i>Suse Linux</i> worden de configuratiebestanden bijgehouden in de <i>vhosts.d</i> (virtual hosts) directory:</p> <pre>cd /etc/apache2/vhosts.d</pre>
--	---

Open het Apache configuratiebestand in de *vi* editor:

```
vi downloads.probook.conf
```

Let op: gebruik in plaats van *probook* de host-naam van je eigen machine.

Toets **i** (insert) om naar de *INSERT* modus te gaan. Het kan zijn dat je dit bestand nog van vorige opdrachten hebt staan. Voeg dan alleen de vetgedrukte regels toe:

```
<VirtualHost probook>
  DocumentRoot "/home/daniel/Downloads"
</VirtualHost>
<Directory "/home/daniel/Downloads">
  Options Indexes
  AuthName "Mijn Downloads"
  AuthType basic
  Require valid-user
  AuthBasicProvider PAM
  AuthPAMService httpd
</Directory>
```

Let op: Vul, in plaats van *daniel*, je eigen gebruikersnaam in. Gebruik ook je eigen hostname in plaats van *probook*.

Toets **<Esc>** om uit de *INSERT* modus te komen en geef de commando's *w* (write) en *q* (quit):

```
:wq
```

Het bestand wordt nu opgeslagen en we zijn terug op de commando prompt.

Controleren configuratie

Om te kijken of Apache goed is geconfigureerd, kunnen we de configuratie testen. Dit doen we met het *apachectl* (Apache Control) programma:

```
apachectl -S
```

Met de optie *S* (server) kunnen we een lijst met alle geconfigureerde websites tonen. De output moet er ongeveer als volgt uitzien:

```
Processing config directory: /etc/httpd/*.conf
Processing config file: /etc/httpd/downloads.probook.conf
[Sun Apr 24 11:59:12 2016] [alert] httpd: Could not determine the server's fully qualified
domain name, using 10.0.20.22 for ServerName
VirtualHost configuration:
10.0.20.22:80      is a NameVirtualHost
    default server probook.sassenheim.dmz (/etc/httpd/downloads.probook.conf:1)
    port 80 namevhost probook.sassenheim.dmz (/etc/httpd/downloads.probook.conf:1)
127.0.0.1:80      is a NameVirtualHost
    default server localhost.localdomain (/etc/httpd/conf/access.conf:16)
    port 80 namevhost localhost.localdomain (/etc/httpd/conf/access.conf:16)
```

Let op: *probook* is de host-naam van mijn Linux machine. Je zou hier jouw eigen host- (en domein-) naam moeten zien.

Het hoera-moment

Allereerst moeten we ervoor zorgen dat Apache de gewijzigde instellingen inleest. Dit doen we door Apache te herstarten met het *service* commando:

```
service apache restart
```

Open een web-browser, zoals *Firefox* of *Chrome* en geef de URL van onze nieuwe website in:

```
http://probook
```

Let op: vul in plaats van *probook* (mijn eigen hostname) de via *hostname* gevonden naam van je laptop. Je zou nu het volgende scherm moeten kunnen zien.

Geef de login-gegevens in. We gebruiken een *back-slash* om de Windows werkgroep van de gebruikersnaam te scheiden:

```
linux\testuser
```

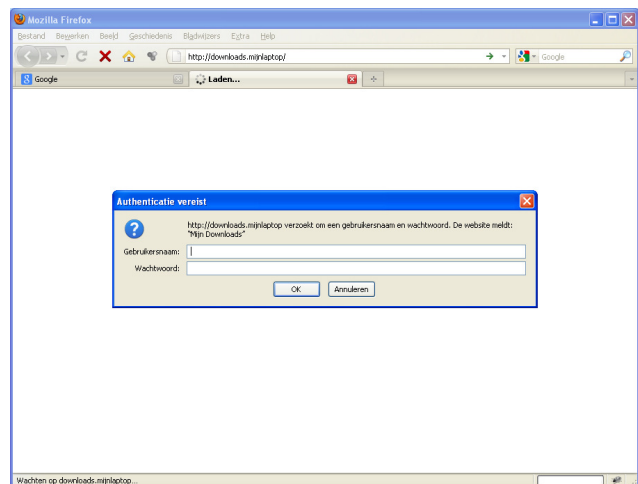
Let op: *LINUX* is de Windows werkgroep van mijn Domain Controller. Gebruik hier de werkgroep van jouw eigen DC. Hetzelfde geldt voor de *testuser*.

Huiswerk opsturen

Zoals je weet, kun je de opdracht aftekenen door een e-mail met daarin de output van het *cat* commando te versturen. Dit doen we met een pijpleiding tussen de commando's *cat* en *email*. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
cat *.conf | email -s "Apache mod_auth_pam" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.



Administrator uitloggen

We hebben de Apache *PAM* module geïnstalleerd zodat de wachtwoorden van een *Domain Controller* kunnen worden gebruikt, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.

Problemen oplossen

Bij problemen, kijk dan altijd eerst in het Apache fout-log.

Cygwin gebruikers De logbestanden op een Cygwin systeem staan in de <i>/var/log/httpd</i> directory. tail /var/log/httpd/error_log	Andere Linux gebruikers De logbestanden op andere Linux systemen staan in de <i>/var/log/apache2</i> directory. tail /var/log/apache2/error.log
--	---

AuthUserFile not specified

Het kan zijn dat je in het log deze foutmelding ziet:

```
[Tue May 24 23:08:15 2016] [error] [client 127.0.0.1] AuthUserFile not specified in the configuration
```

Dit is een *bug* in sommige Linux distributies. Je kunt hem oplossen door de vetgedrukte regel aan het configuratiebestand toe te voegen:

```
<VirtualHost probook>
    DocumentRoot "/home/daniel/Downloads"
</VirtualHost>
<Directory "/home/daniel/Downloads">
    Options Indexes
    AuthName "Mijn Downloads"
    AuthType basic
    AuthBasicProvider PAM
    AuthPAMService httpd
    AuthBasicAuthoritative off
</Directory>
```

De PAM module voor Apache is onhandig geschreven. Apache probeert de login zelf uit te voeren (via de *mod_auth* module) en heeft niet door dat dit al gedaan wordt door een andere module (*mod_authnz_pam*). Je zou dus de hele *mod_auth* module moeten de-activeren, maar dan werken andere web-sites niet meer. Deze oplossing is daarom eleganter.

Module is unknown

Het kan zijn dat je deze foutmelding in het Apache log-bestand ziet:

```
[Sun Feb 17 17:22:02.945049 2019] [authnz_pam:warn] [pid 4102] [client 10.0.20.22:2394] PAM authentication failed for user linux\\testuser: Module is unknown
```

Je bent vergeten de Winbind module voor PAM te installeren. Kijk onder het kopje “Installatie PAM modules”.

Password Mismatch

Het kan zijn dat je deze foutmelding in het Apache log-bestand ziet:

```
[Sun Feb 17 17:22:02.945276 2019] [auth_basic:error] [pid 4102] [client 10.0.20.22:2394] AH01617: user linux\\testuser: authentication failure for "/": Password Mismatch
```

Om te zien wat er precies aan de hand is kun je in het systeem-log voor authenticatie kijken:

tail /var/log/auth.log