Responsable du cours (ARIR81/M1-APP-RS) : Yousfi Souheib

TP4 : Authentification Apache avec OpenLDAP

Introduction

Ce TP vise à vous familiariser avec la configuration d'une authentification sur un serveur Apache, en employant OpenLDAP comme mécanisme d'authentification unifié. Durant ce TP, vous apprendrez comment ajuster les paramètres d'Apache pour qu'il sollicite un annuaire OpenLDAP lors de la vérification des credentials des utilisateurs désirant accéder à des contenus sécurisés.

Configuration de Apache

Suite à l'installation du paquet apache2, il est nécessaire d'activer le module authnz_ldap.

```
ubuntu@Efrei:~$ sudo apt-get install apache2
[sudo] password for ubuntu:
Reading package lists ... Done
```

```
ubuntu@Efrei:~$ sudo a2enmod auth
auth_basic       authn_core       authn_socache    authz_dbd        authz_owner
auth_digest      authn_dbd        authnz_fcgi      authz_dbm        authz_user
auth_form        authn_dbm        authnz_ldap      authz_groupfile
authn_anon       authn_file       authz_core       authz_host
ubuntu@Efrei:~$ sudo a2enmod authnz_ldap
Considering dependency ldap for authnz_ldap:
Enabling module ldap.
Enabling module authnz_ldap.
To activate the new configuration, you need to run:
  systemctl restart apache2
ubuntu@Efrei:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: ubuntu
Password:
==== AUTHENTICATION COMPLETE ====
ubuntu@Efrei:~$
```

Dans le fichier de configuration HTTP du serveur web Apache, la configuration présentée ci-dessous est fournie sans les commentaires :

```
ubuntu@Efrei:~$ grep .  /etc/apache2/sites-available/000-default.conf | grep -v '#'
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

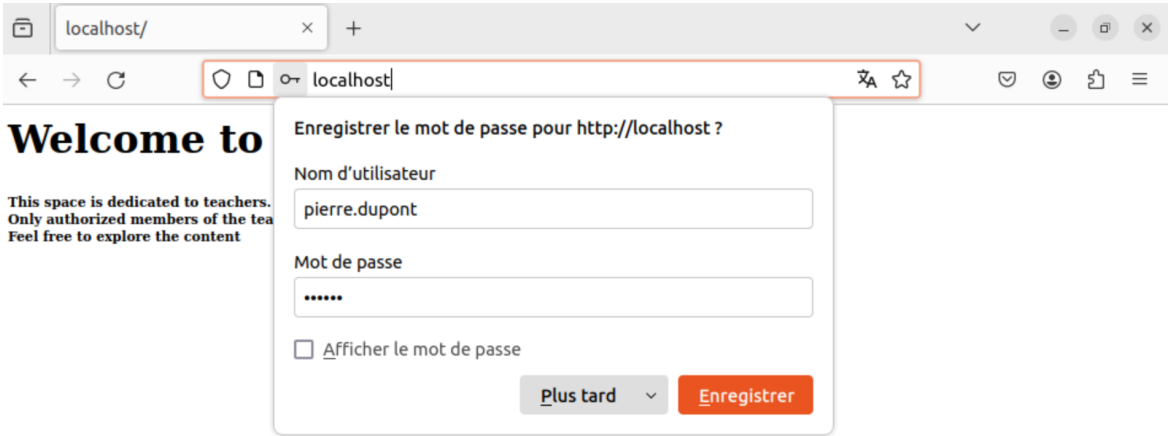
Nous configurons une page d'accueil pour notre site qui s'affichera lors de l'accès à localhost de la manière suivante :

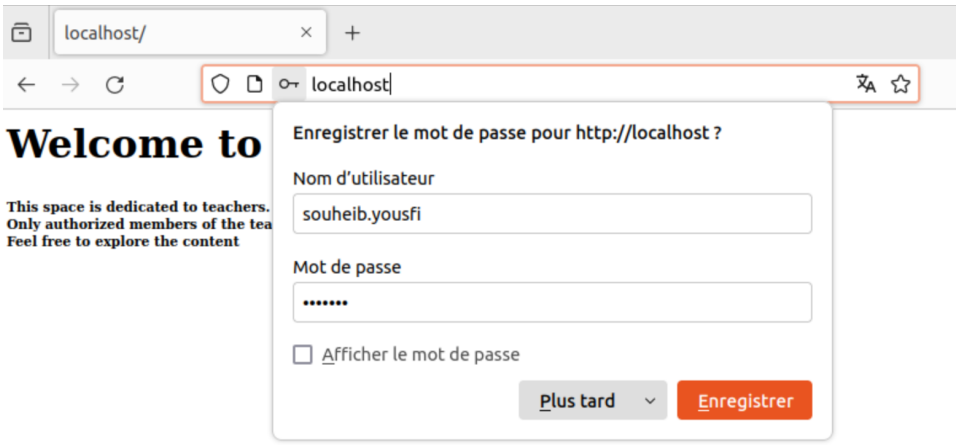
```
ubuntu@Efrei:~$ cat /var/www/html/index.html
<h1> Welcome to the Teachers' Space :) </h1>
<h6> This space is dedicated to teachers. <Br>
Only authorized members of the teachers group have been access. <Br>
Feel free to explore the content
 </h6>
```

Pour incorporer l'authentification LDAP dans Apache, modifiez le fichier /etc/apache2/sites-available/000-default.conf en y ajoutant une directive qui désigne votre serveur LDAP comme source d'authentification. Cette configuration permettra à Apache de se connecter au serveur LDAP pour l'authentification des utilisateurs, basée sur les données présentes dans ce dernier. Avant d'apporter cette modification, vérifiez que l'utilisateur dédié à Apache a été préalablement créé pour éviter des problèmes d'accès au serveur LDAP. Après avoir réalisé ces changements, il est nécessaire de redémarrer le service Apache2 pour que les nouvelles configurations prennent effet. Ce processus active l'authentification LDAP sur votre serveur web, renforçant la sécurité par une gestion centralisée des identités et des accès.

```
ubuntu@Efrei:~$ grep . /etc/apache2/sites-available/000-default.conf | grep -v '#'
<AuthnProviderAlias ldap myldap>
        AuthLDAPURL  "ldap://Efrei.fr/ou=users,dc=Efrei,dc=fr" STARTTLS
</AuthnProviderAlias>
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
<Directory "/var/www/html">
        AuthType Basic
        AuthName "Top Secret"
        AuthBasicProvider myldap
        Require valid-user
        LogLevel trace1
</Directory>
</VirtualHost>
```

Il est observé que tous les utilisateurs répertoriés dans notre annuaire bénéficient d'un accès à notre site web.



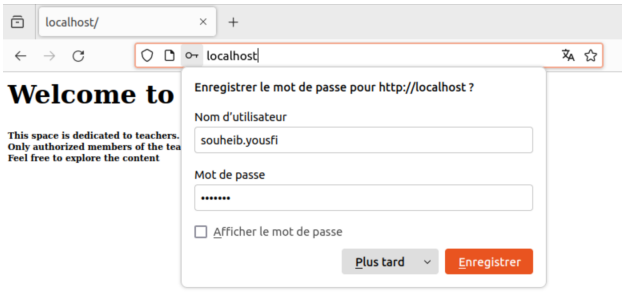


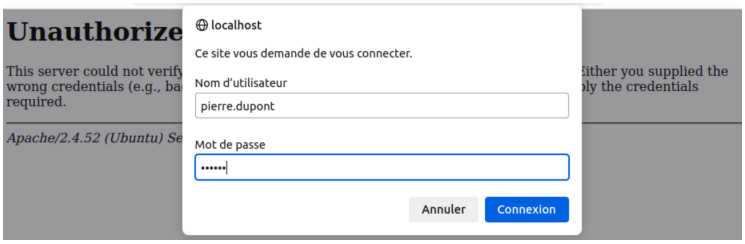
Restriction de l'accès à la page au groupe teachers

Pour limiter l'accès au site web, il est nécessaire d'incorporer un filtre dans l'URL LDAP de manière à autoriser uniquement les membres du groupe "teacher". Après cette modification, un redémarrage du service Apache2 est requis pour appliquer la nouvelle configuration.

```
ubuntu@Efrei:~$ grep . /etc/apache2/sites-available/000-default.conf | grep -v '#'
<AuthnProviderAlias ldap myldap>
        AuthLDAPURL  "ldap://Efrei.fr/ou=users,dc=Efrei,dc=fr?uid?sub?(gidNumber=3001)" STARTTLS
</AuthnProviderAlias>
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
<Directory "/var/www/html">
        AuthType Basic
        AuthName "Top Secret"
        AuthBasicProvider myldap
        Require valid-user
        LogLevel trace1
</Directory>
</VirtualHost>
```

Et nous testons les accès pour l'enseignant et pour tout autre utilisateur qui n'appartient pas au groupe teacher :





♣ **S.Y.** ♣
Bon travail