Julien Alleaume RT2 APP

BUT TP2 M304 (Authentification web et annuaire d'utilisateurs LDAP)

1 Authentification Apache sur l'annuaire de l'IUT

1.1 Pré-requis:

Je recherche dans l'annuaire de l'IUT mon entrée en utilisant la commande :

```
julien@julien-pc:~$ ldapsearch -x -H ldap://10.255.255.200 -b o=gouv,c=fr "uid=julien.alleaume" dr
# extended LDIF
#
# LDAPv3
# base <o=gouv,c=fr> with scope subtree
# filter: uid=julien.alleaume
# requesting: dr
#

# julien.alleaume, local, eleves, utilisateurs, 0341884N, ac-montpellier, educa
 tion, gouv, fr
dn: uid=julien.alleaume,ou=local,ou=eleves,ou=utilisateurs,ou=0341884N,ou=ac-m
 ontpellier,ou=education,o=gouv,c=fr

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

1.2 Installez le serveur web apache sur votre VM et activez les modules ldap et authnz_ldap

```
apt install apache2
#Installation sans problème

a2enmod authnz_ldap ldap
#a2enmod est considéré comme non installer
```

Résolution de probleme lié à l'initialisation des module Apache2 via a2enmod ;

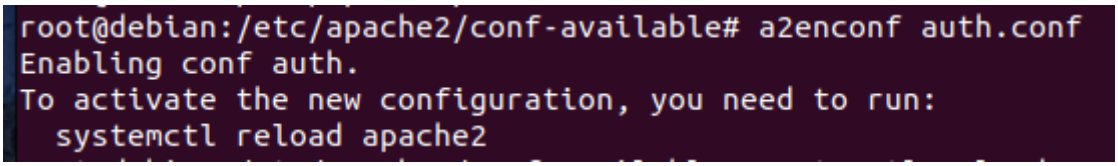
```
echo $PATH
export PATH=$PATH:/usr/sbin
#a2enmod fonctionne et me permet de continuer

a2enmod authnz_ldap ldap
a2query -m
#Activation réussie
```

Ensuite je crée le fichier auth.conf dans `/etc/apache2/conf-available/` qui va me permettre l'authentification LDAP dans une interface web Apache2 et le configure en ajoutant `o=gouv,c=fr` :

```
<Location />
        AuthName "ldap auth"
        AuthType Basic
        AuthBasicProvider ldap
        AuthLDAPURL ldap://10.255.255.200:389/o=gouv,c=fr?uid?sub?
        Require valid-user
</Location>
```

J'active le fichier `auth.conf` en faisant :

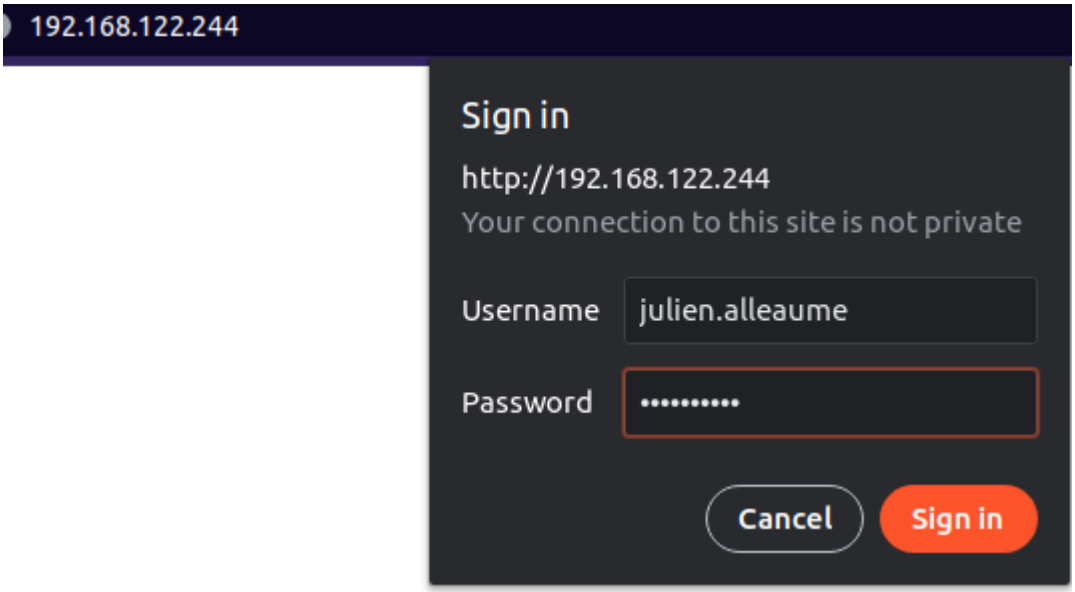
```
a2enconf auth.conf
#Commande réussie sans problème
```



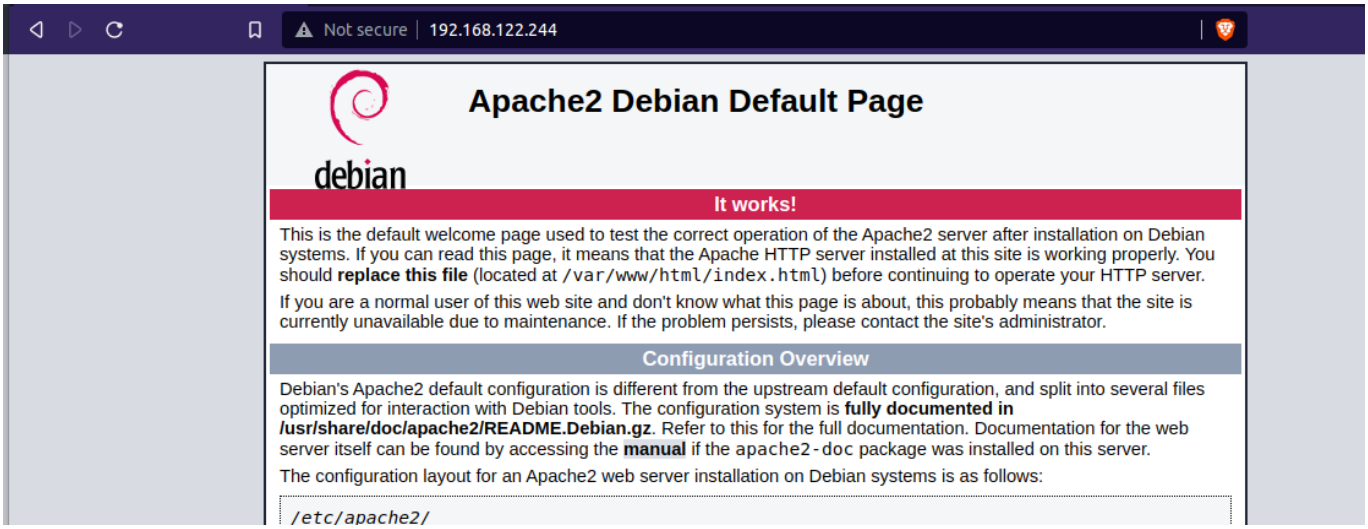
Enfin pour que les changement soit pris en compte je redémarre Apache2:

```
sudo systemctl restart apache2
```

Enfin j'essaie ma configuration en me connectant au site web via l'ip de ma VM:



Je renseigne mes identifiants et comme vu ci-dessous l'authenfication est une reussite :



2 Préparation d'un l'annuaire sur la VM afin d'avoir une BASE LDAP des utilisateurs

Installation de `slapd` et `ldap-utils`

```
apt-get install slapd ldap-utils
#Je met le mots de passe root pour administrateur

#Installation réussie sans problème
```

Ensuite j'édite le fichier `/etc/ldap/ldap.conf` et ajoute les deux ligne :

```
BASE dc=iutbeziers,dc=fr
URI ldap://localhost/
```

Puis je redémarre le service pour prendre en compte les changements:

```
service slapd restart
```

Test pour vérifier si le serveur fonctionne comme prévus : (Dans cette capture j'ai déjà importé le fichier iutbeziers-central.ldif)

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: Melanie.Zethofrais
sn: Zethofrais
givenName: Melanie
uid: MZETHOFR
uidNumber: 1039
gidNumber: 300
homeDirectory: /home/mzethofr
loginShell: /bin/bash
shadowExpire: 0
userPassword:: e1NTSEF9ZE9ES2NRTkJNSERqYmRsWS9IaEVYVEV5Q1gzSXY2Kzc=
mail: Melanie.Zethofrais@domain.tld
mail: MZETHOFR
initials:: TS7CoFou
structuralObjectClass: inetOrgPerson
entryUUID: fe4f4078-f94f-103c-9d75-0dc94f383233
creatorsName: cn=admin,dc=iutbeziers,dc=fr
createTimestamp: 20221115164044Z
entryCSN: 20221115164044.197863Z#000000#000#000000
modifiersName: cn=admin,dc=iutbeziers,dc=fr
modifyTimestamp: 20221115164044Z
```

Importation du fichier contenant toute les données d'un annuaires, transféré via scp de mon pc à ma VM :

```
ldapadd -x -D cn=admin,dc=iutbeziers,dc=fr -W -f iutbeziers-central.ldif
```

J'effectue la requetes pour pouvoir afficher la liste des comptes crée par l'importation :

```
ldapsearch -x -b dc=iutbeziers,dc=fr -s sub -
D"cn=admin,dc=iutbeziers,dc=fr" -w test "(objectClass=inetOrgPerson)"
```

En sortie de la commande :

```
# MZETHOFR, people, iutbeziers.fr
dn: uid=MZETHOFR,ou=people,dc=iutbeziers,dc=fr
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: Melanie.Zethofrais
sn: Zethofrais
givenName: Melanie
uid: MZETHOFR
uidNumber: 1039
gidNumber: 300
homeDirectory: /home/mzethofr
loginShell: /bin/bash
shadowExpire: 0
userPassword:: e1NTSEF9ZE9ES2NRTkJNSERqYmRsWS9IaEVYVEV5Q1gzSXY2Kzc=
mail: Melanie.Zethofrais@domain.tld
mail: MZETHOFR
initials:: TS7CoFou

# search result
search: 2
result: 0 Success

# numResponses: 40
# numEntries: 39
```

Comme ci dessus j'ai bien les 39 entrées prévues.

3 Configuration des clients linux

1. :

```
/etc/nsswitch.conf

passwd: compat
group: compat
shadow: compat
gshadow: compat
```

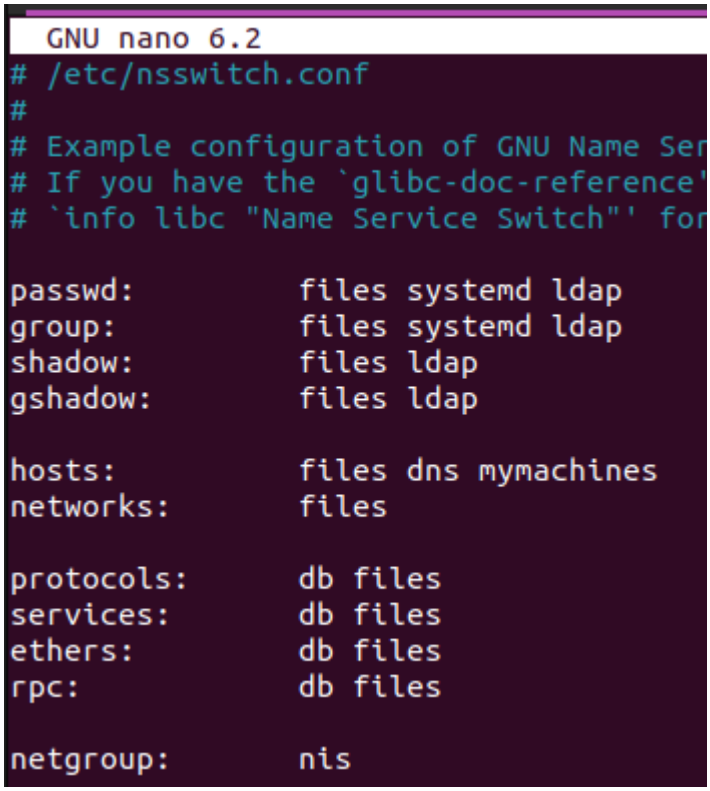
1. : C'est lignes signifient les mots de passe possible à utiliser pour la connection sur la machine.
   Ici `compat` est utilisé pour les bases de données passwd, shadow et group.

2. :

```
apt-get install libnss-ldap libpam-ldap ldap-utils
#Installation des paquets sans problemes.
```

```
#De plus je configure l'Host, le mot de passe, etc... durant
l'installation.
```

3. : J'ajoute dans `/etc/nsswitch.conf` ldap au ligne `passwd,group,shadow,gshadow` pour pouvoir utilisé les identifiants ldap comme moyen de connection à cette VM:



4. : Suppressions de `use_authok` pour pouvoir mettre à jour les mots de passe dans le fichier `/etc/pam.d/commonpassword` Et je vérifie que la ligne soit bien présente :

```
password [success=1 user_unknown=ignore default=die] pam_ldap.so
try_first_pass
```

5. : Pour crée les fichiers Home localement je change la ligne dans le fichier `/etc/pam.d/common-session`, et ajoute :

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

a) `/etc/skel` permet de crée des squelettes, c'est à dire un modèle pour les répèrtoire `Home` de manière automatique et ainsi d'avoir la même structure sur tout les utilisatuers qui s'authentifie sur la machine. b) `umask=077` permet d'affecter ds droits automatique au répertoire crée pour les utilisateurs en questions qui sont authentifier sur la machine. 6. : Validé 7. : La connection en ssh est possible même avec une changement de mots de passe et peut le vérifier grâce aà ces deux commande :

```
# Standard Unix session setup and teardown.
@include common-session
```

```
# Standard Unix password updating.
@include common-password
```

On peut aussi activer les logs et essayer de ce connecter pour voir un quelconque problèmes.