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

Jean-Marc Pouchoulon

Octobre 2022

Ce TP a pour objet de vous montrer deux exemples de configuration de service ayant pour "backend" un annuaire LDAP:

- La protection d'un server web apache par l'obligation d'une authentification avec l'uid de la personne sur un annuaire.
- L'authentification, le login et la gestion des utilisateurs d'un annuaire sur une machine Linux.

Vous travaillerez individuellement sur une VM debian donc pas sur votre poste physique. Vous serez évaluez par l'enseignant au cours de la séance lors de "check" notés dans le TP.

1 Authentification Apache sur l'annuaire de l'IUT

1.1 Pré-requis:

Retrouvez le DN de votre entrée dans l'annuaire de l'IUT:

- ip: 10.255.255.200
- base: o=gouv,c=fr

Faites valider le DN récupéré par l'enseignant.(check1) Le DN permet de connaître ou se situe votre entrée dans l'annuaire de l'IUT et vous est utile à la question suivante.

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

```
apt install apache2
a2enmod authnz_ldap ldap
a2query  -m
```

On va permettre l'accès au serveur web de la VM aux utilisateurs authentifiés sur l'annuaire de l'IUT. Pour cela vous devez créer un fichier auth.conf sous /etc/apache2/conf-available/. A vous de remplir le chemin AuthLDAPURL. N'oubliez pas de redémarrer apache2.

```
<Location />
      AuthName "ldap auth"
      AuthType Basic
      AuthBasicProvider ldap
      AuthLDAPURL ldap://10.255.255.200/[A COMPLETER PAR VOS SOINS]?uid?sub?
      Require valid-user
</Location>
```

Lors de l'accès au serveur web de la VM , saisissez votre "prénom.nom" et votre mot de passe IUT. Faites valider par l'enseignant (check2).

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

Dans une machine virtuelle Debian, installez votre annuaire.

```
apt-get install slapd ldap-utils
```

Configurez le pour avoir un domaine `iutbeziers.fr`. Si vous avez fait une erreur, vous pouvez refaire votre configuration avec la commande:

```
dpkg-reconfigure slapd
```

Editez le fichier /etc/ldap/ldap.conf.

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

Redémarrez le service:

```
service slapd restart
```

Vérifiez que votre serveur est opérationnel et vous renvoie sa configuration en tapant la commande

```
slapcat
```

Récupérez le fichier `iutbeziers-central.ldif`, puis importez le dans votre annuaire

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

A cette étape, vous devoir la liste des comptes créés (39 dans l'ou people).

Requêtez ("ldapsearch -x dn") votre annuaire et faites valider par l'enseignant (check3)

3 Configuration des clients linux

Il s'agit maintenant de permettre l'authentication des utilisateurs de l'annuaire sur votre VM.

Dans le fichier /etc/nsswitch.conf, on trouve les lignes suivantes:

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

1. Quelle est la signification de ces lignes ?
2. Installez les paquets sur le clients
   `apt-get install libnss-ldap libpam-ldap ldap-utils`
   Si vous faites une erreur, vous pouvez reconfigurer à nouveau en lançant les commandes:
   `dpkg-reconfigure libpam-ldap`
   `dpkg-reconfigure libnss-ldap`
   Les fichiers concernés sont :
   `/etc/pam_ldap.conf`
   `/etc/pam_ldap.secret` *#contient le mot de passe admin*

   `/etc/libnss-ldap.conf`
   `/etc/libnss-ldap.secret` *#contient le mot de passe admin*

   `/etc/pam.d/common-account`
   `/etc/pam.d/common-auth`
   `/etc/pam.d/common-password`

`/etc/pam.d/common-session`
`/etc/pam.d/common-session-non-interactive`

3. Indiquez au client que l'authentification se fera d'abord avec les infos système (compat) puis avec les infos de l'annuaire LDAP

   `/etc/nsswitch.conf`

   ```
   passwd:     compat ldap
   group:      compat ldap
   shadow:     compat ldap
   gshadow:    files ldap
   ```

4. Gérez les mots de passe de l'annuaire.

   Pour que le mot de passe puisse être changé et mis a jour dans l'annuaire, allez dans /etc/pam.d/common-password.Vérifiez que cette ligne soit présente (suppression des use_authok)

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

5. Création automatique du HOME

   Quand on crée un utilisateur sur une machine par la commande adduser, le HOME est créé aussi. Dans notre cas, Les utilisateurs sont créés dans l'annuaire, pas sur une machine, donc il faudra que les dossiers se créent (si nécessaire) sur la machine ou l'utilisateur va s'authentifier.

   Dans /etc/pam.d/common-session, ajoutez :

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

   a) à quoi sert l'option `skel=/etc/skel`

   b) à quoi sert l'option `umask=077`

6. Faites valider les points suivants par l'enseignant (check4) :

   ```
   # la liste des utilisateurs ldap doit s'afficher
   getent passwd
   getent group
   # vous devez pouvoir changer le mot de passe pour un utilisateur LDAP via passwd
   passwd DCOUDUR
   New password:
   Re-enter new password:
   LDAP password information changed for DCOUDUR
   passwd: password updated successfully
   # vous devez pouvoir accéder via sudo su - à l'utilisateur (ignorer l'expiration)
   sudo su - DCOUDUR
   Votre compte a expiré; veuillez contacter votre administrateur système.
   Création du répertoire ń /home/dcoudur ż.
   DCOUDUR@debian:~$
   # et via ssh
   ssh DECOUDUR@...
   ```

7. En regardant le fichier /et/pam.d/sshd, déterminez si on peut se connecter en ssh sur le poste client avec l'authentification ldap. Si oui, grâce à quels éléments de configuration ?