BUT TD1 M304 Annuaires Unifiés (Manipulation de LDAP avec le CLI (Command Line Interface))

Jean-Marc Pouchoulon

Octobre 2022

Ce TD a pour objet de manipuler les composantes d'un annuaire LDAP à l'aide de la ligne de commandes. (ldapsearch ldapmodify ldapdelete...) Les requêtes en lecture vont porter sur l'annuaire microsoft de production de l'IUT de Béziers. Active Directory est en effet capable de supporter le standard LDAP v3 ce qui permet de l'interroger avec des outils clients standards. Vous vous authentifierez avec l'utilisateur authldap (mot de passe authldap). Les URL suivantes peuvent vous aider :

- `http://msdn.microsoft.com/en-us/library/ms675881(v=vs.85).aspx`
- `http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx`
- `http://ldapwiki.willeke.com/wiki/Active%20Directory%20Computer%20Related%20LDAP%20Query`

1 L'Active Directory un LDAP presque comme les autres ....

1.1 TIPS : Amélioration de l'affichage des entrées de l'annuaire

1. *Tips , Tricks et installation des outils nécessaires au TD :* Installez le package ldap-utils.
   Afin de pouvoir utiliser la couche TLS qui permet le chiffrement de la connexion en restant sur le même port d'écoute (port 389).Il peut être nécessaire de désactiver la vérification des certificats SSL côté client. A cette fin modifiez le fichier ldap.conf (/etc/openldap/ldap.conf) en rajoutant la ligne TLS_REQCERT never.
   Nb : *l'option -d 1 dans un ldapsearch permet de débugger le dialogue LDAP.*
   Le oneliner Perl suivant :

   ```
   perl -p00e 's/\r?\n //g'|egrep -v '(\|^$)'
   ```

   permet de remettre les sorties au format LDIF de la commande ldapsearch sur une seule ligne et l' egrep enlève les lignes vides ou de commentaires. Cette autre oneline Perl :

   ```
   perl -pne 's/(\d{11})\d{7}/"DATE-AD(".scalar(localtime($1-11644473600)).")"/e'
   ```

   permet d'afficher les dates en mode "human readable" d'une entrée LDIF. Une regex utilisée par grep permettent de filter les lignes blanches et les commentaires du LDIF)

   ```
   egrep -v "(^$|^#)"
   ```

1.2 Environnement AD

1. Connectez-vous avec Apache Directory Studio `http://directory.apache.org/studio/downloads.html` à l'AD.
2. Interrogez le DNS (10.6.0.1 de l'IUT afin de retrouver les serveurs Active Directory de l'IUT. (C'est un enregistrement de type SRV)

1.3 Requêtes LDAP

1. Un ldapsearch typique sur l'AD va ressembler à ca :

```
ldapsearch -LLL   \
           -x  \
           -D 'iutbeziers\authldap'  \
           -w 'authldap'  \
           -H ldap://server-rt.iutbeziers.fr \
           -b 'dc=iutbeziers,dc=fr' dn
```

   a) Détaillez les différentes options de cette commande à partir du man.

   b) Recherchez à quoi sert l'option "+" de la commande ldapsearch ?

   c) A quoi sert l'option "-ZZ" de la commande ldapsearch ?

   d) A quoi sert l'option "-LLL" de la commande ldapsearch ?

   e) Pour information l'option "-E pr=200/noprompt" de la commande ldapsearch permet de contourner la limite du nombre maximum d'enregistrements retournés et paramétré côté serveur.

   f) Modifiez le fichier /etc/ldap/ldap.conf pour ne pas renseigner l'option -b.

2. Analysez l'organisation de l'annuaire de l'IUT de Béziers via ApacheDS. Dans quelles Organizational Units se situent majoritairement :

   a) les comptes utilisateurs ?

   b) les comptes machines ?

   c) les comptes enseignants ?

   d) les comptes étudiants ?

3. Retrouvez votre entrée dans l'annuaire en utilisant la commande ldapsearch.

   a) A quoi correspondent les différents attributs de votre entrée LDAP ?

   b) De quel(s) groupe(s) faites-vous partie ? Recherchez l'entrée correspondante à votre groupe dans l'annuaire.

   c) Donnez un exemple d'attribut multivaluée dans cette entrée ?

   d) Dans l'entrée de votre groupe, comment le lien est-il-fait avec une entrée utilisateur ?

   e) Faite une recherche sur l'overlay OpenLDAP memberOf et expliquez l'intérêt d'un tel mécanisme.

   f) Recherchez l'objectCategory présent dans votre fiche. Que représente-t-il ?

   g) Est-il obligatoire d'avoir un mot de passe ou un numero de téléphone dans une entrée de type utilisateur ?

4. PC et Humains unis par l'ObjectClass :

   a) Comparez votre entrée à une entrée relative à un ordinateur. Quels sont les objectClasses en commun avec les deux types d'entrée ?

   b) Faites une recherche sur l'objectClasse Person depuis la racine du D.I.T. Le résultat ne contient-il que des entrées de type utilisateur ?

   c) Comment obtenir uniquement des entrées de type utilisateur ?

5. Combien y a-t-il d'entrées dans l'annuaire relatives à des postes de travail ?

6. Quel est le nombre d'étudiants dans l'A.D de l'IUT ?

7. Récupérez la liste des mails de tous les étudiants de l'IUT.

8. Ecrivez en cinq lignes un guide de la recherche dans un annuaire LDAP Active Directory :

9. A l'aide ldapsearch interrogez le root DN de l'A.D. (il faut interroger l'annuaire avec une base vide). Qu'est ce que SASL ?

10. Interrogez l'AD avec ldapsearch afin de connaitre la version du système d'exploitation. Retrouvez le dn et l'attribut operatingSystem de chaque contrôleur de domaine. (regardez les exemples fournis par les documents cités en début de TD)

2 Analyse du protocole Ldap au niveau réseau

1. Lancez un ldapsearch avec l'option -x afin de retrouver votre entrée
   a) Quelles sont les phases du dialogue ldap (Liste des différents ldapMessages)
   b) Quel champ fait le lien entre une requête et une réponse ldap ?
   c) L'option -x est-t-elle sécurisée ?
   d) Utilisez l'option -ZZ afin de faire du TLS : est-elle sécurisée ? y a t-il changement de port vers le 636 ?