OpenLDAP

notes LDAP

Table des matières

1. Présentation

C'est une implémentation "libre" du protocole LDAPv3. Elle implémente la plupart des spécifications de l'IETF que l'on peut consulter dans différentes RFC. On dispose d'un serveur, d'un agent de réplication, et de clients permettant de consulter, créer, modifier, effacer les données un annuaire. Les clients sont accéssibles par la ligne de commande, et

2. Manipulation d'un annuaire

- Créer la zone
  Il faut d'abord identifier la zone qui sera couverte par le serveur, c'est à dire créer une entrée du type dcObject (domain component):
  ```
  dc: cp.finance.gouv.ci
  description: Direction Générale du Trésor et de la Comptabilité Publique
  objectClass: dcObject
  objectClass: organization
  o: DGTCP
  ```
  Dans ce cas, cet object représente aussi une organisation, donc "organization" est également superclasse de l'objet. Il faut également créer une entrée pour un utilisateur avec lequel on réalisera les manipulations ultérieure, pour que le système puisse associer un utilisateur aux dites modifications
  ```
  dn:
  cn=Manager,dc=cp,dc=finances,dc=gouv,dc=ci objectClass:
  organizationalRole
  cn: Manager
  ```
  le nom du gestionnaire de la zone est indiqué au serveur (slapd) dans le fichier /etc/openldap/slapd.conf
- Insérer une entrée
  ```
  >iconv --from-code=8859_1 --to-code=UTF-8 change.ldif | \
  ldapadd -x -D'cn=Manager,dc=cp,dc=finances,dc=gouv,dc=ci' -w secret
  ```
- Insérer une entrée binaire (base64)
  ```
  >uuencode -m eric_small.jpg eric_small.jpg | \
  sed -n -e '1 {;i\' -e 'dn: cn=BURGHARD
  Éric,ou=Personnes,dc=cp,dc=finances,dc=gouv,dc=ci\' \
                          -e 'changetype: modify\' -e 'replace:
  jpegPhoto' \
                          -e 'b;};2 {;s/.*/jpegPhoto:: &/p;b;};$q;s/.*/
  &/p' | \
  iconv --from-code=8859_1 --to-code=UTF-8 | \
  ldapmodify -x -D'cn=Manager,dc=cp,dc=finances,dc=gouv,dc=ci' -w secret
  ```
- Modifier une entrée
  ```
  >iconv --from-code=8859_1 --to-code=UTF-8 change.ldif | \
  ldapmodify -x -D'cn=Manager,dc=cp,dc=finances,dc=gouv,dc=ci' -w secret
  ```

3. Consulter un annuaire

La consultation d'un annuaire se fait en formulant une requête d'un client vers un serveur. De nombreux paramètres font partie de la requête:

- le point de départ de la recherche
- la profondeur de la recherche
- le comportement de la recherche vis-à-vis des liens
- l'utilisateur LDAP avec lequel faire la recherche (avec mot de passe)
- les attributs demandés
- le filtre associé à la recherche

- Intérogation du serveur
  LDAP founit un mecanisme permettant de récupérer les paramètres associés à un serveur via les mecanismes standards de requête. Cette requête se fait en anonyme sur le serveur avec un point de départ " et une profondeur de 0, en demandant les attributs administratifs '+'.
  ```
  >ldapsearch -x -s base -b'' +
  ```
  Exemple:
  ```
  namingContexts: dc=cp,dc=finances,dc=gouv,dc=ci
  supportedControl: 2.16.840.1.113730.3.4.2
  supportedExtension: 1.3.6.1.4.1.4203.1.11.1
  supportedExtension: 1.3.6.1.4.1.1466.20037
  supportedFeatures: 1.3.6.1.4.1.4203.1.5.1
  supportedLDAPVersion: 2
  supportedLDAPVersion: 3
  subschemaSubentry: cn=Subschema
  ```
  - namingContexts est une liste de zone couvertes par le serveur
  - supportedLDAPVersion est une liste regroupant les versions du protole supporté par le serveur.
  - subschemaSubentry représente le dn sous lequel intérroger le serveur pour obtenir tous les paramètre du schéma supporté par le serveur

- Format d'URL
  LDAP est accéssible en consultation à partir d'un navigateur si celui supporte les URLs LDAP (ie,konqueror). Le format est le suivant:
  ```
  "ldap://"[hostport] ["/"[dn["?"[attributes]["?"[scope]["?"[filter]["?"
  extensions]]]]]]
  ```
  Exemples:
  ```
  hostport: localhost:389
  dn: cn=Administrateur,dc=cp,dc=finances,dc=gouv,dc=ci
  attributes: +,*
  scope: base|one|sub
  filter: (&(objectClass=*)(o=SDI))
  ```
- Lister toutes les entrées
  ```
  >ldapsearch -x -b 'dc=cp,dc=finances,dc=gouv,dc=ci' '(objectclass=*)'
  ```