Cours 2
Administration des réseaux : Les Annuaires

Licence Pro RIMS

Sylvain MERCHEZ

Plan

Administration des réseaux : Les annuaires

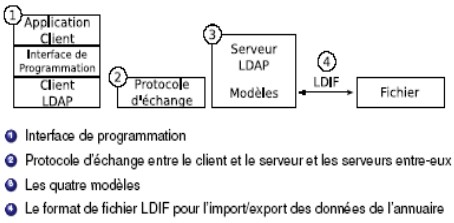
- Introduction
- LDAP
- OpenLDAP

Le protocole LDAP

- Quatre modèles
  - Le modèle de nommage : définit comment l'information est stockée et organisée
  - Le modèle fonctionnel : définit les services fournis par l'annuaire (recherche, ajout, ...)
  - Le modèle d'information : définit le type d'informations stockées
  - Le modèle de sécurité : définit les droits d'accès aux ressources

Le protocole LDAP

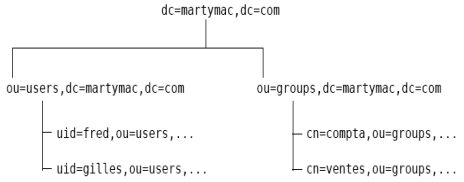
- LDAP



1. Interface de programmation
2. Protocole d'échange entre le client et le serveur et les serveurs entre-eux
3. Les quatre modèles
4. Le format de fichier LDIF pour l'import/export des données de l'annuaire

LDAP : un modèle de nommage

- Une représentation hiérarchique des données



Un élément marque son appartenance à l'élément supérieur en en reprenant le nom, qu'il complète par le sien.

Ex: "cn=ventes,ou=groups,dc=martymac,dc=com"

LDAP : un modèle de nommage

- **A SAVOIR :**
  - Chaque élément est appelé une **entrée** (an entry). Une entrée peut être un branchement (un **noeud**, a node) ou un élément terminal (une **feuille**, a leaf).
  - Chaque élément possède un **DN** (Distinguished Name). Le DN est le nom complet de l'élément qui permet de le positionner dans l'arborescence. Il est unique. Ex: "cn=ventes,ou=groups,dc=martymac,dc=com"
  - Chaque élément possède également un **RDN** (Relative Distinguished Name), partie du DN de l'élément qui est relative au DN supérieur. Exemple : "cn=ventes"
  - La racine est l'élément supérieur de tous les autres, c'est la base de l'arborescence. On l'appelle root en anglais, parfois on parle de "root DN". Exemple : "dc=martymac,dc=com"

LDAP : un modèle de nommage

- Règles :
  - La RFC 2253 normalise l'écriture des DN et conseille de ne pas ajouter d'espaces autour du signe "=", ni à la fin du DN. Les espaces sont autorisés par contre pour les valeurs des entrées.

"cn=Ganael Laplanche,cn=ventes,ou=groups,dc=martymac, dc=com" => Correct

"cn = Ganael Laplanche, cn = ventes, ou = groups, dc = martymac, dc = com" => pas correct

  - Les majuscules seront ou non prises en compte en fonction du type d'attribut utilisé et de ses particularités.

LDAP : un modèle fonctionnel

- Plusieurs types d'opérations possibles :
  - Rechercher une entrée suivant certains critères
  - S'authentifier
  - Ajouter une entrée
  - Supprimer une entrée
  - (Modifier une entrée)
  - Renommer une entrée
- Certaines de ces actions, notamment la recherche, nécessitent des outils particuliers pour nous faciliter l'accès à l'annuaire

LDAP : un modèle fonctionnel

- La base

  La base est le DN à partir duquel nous allons agir. Pour une recherche, il s'agir du noeud à partir duquel est effectuée la recherche.

- La portée

  La portée (scope) est le nombre de niveaux sur lesquels l'action va être effectuée.

  Il existe 3 niveaux différents :

  - SUB : l'action est effectuée récursivement à partir de la base spécifiée sur la totalité de l'arborescence.
  - ONE : l'action est effectuée sur un seul niveau inférieur par rapport à la base spécifiée (les fils)
  - BASE : l'action est effectuée uniquement sur la base spécifiée.

LDAP : un modèle fonctionnel

- Les filtres

  Le troisième outil à notre disposition est le filtre. Un filtre va permettre d'effectuer des tests de correspondance lors d'une recherche. Il s'agit en quelques sortes du critère de la recherche.

  Il existe 4 tests basiques, qui peuvent ensuite être combinés :

  - Le test d'égalité : X=Y
  - Le test d'infériorité : X<=Y
  - Le test de supériorité : X>=Y
  - Le test d'approximation : X~=Y

LDAP : un modèle fonctionnel

- Les filtres
  - Les autres opérateurs (<, >) ou des tests plus complexes peuvent être mis en place par combinaison, il faut alors utiliser les parenthèses ( ) et l'un des opérateurs suivants :
    - L'intersection (et) : &
    - L'union (ou) : |
    - La négation (non) : !
    - Un test d'infériorité stricte pourrait donner ceci : (&(X<=Y)(!(X=Y)))
  - On peut combiner plus de deux éléments : (&(X=Y)(Y=Z)(A=B)(B=C)(!(C=D)))

LDAP : un modèle fonctionnel

- **Les URLs LDAP**
  - En une seule ligne, il est possible de spécifier tous les éléments de notre requête. Voici le format de cette URL (RFC 2255) :

Ex : ldap[s]://serveur[:port][/[base[?[attributs à afficher][?[portée][?[filtre][?extensions]]]]]]

L'exemple ci-dessous recherche tous les uid de notre arbre, à partir de la branche users :

ldap://localhost:389/ou=users,dc=martymac,dc=com?uid?sub

LDAP : un modèle d'information

- **Les attributs**
  - Un attribut est une valeur contenue dans une entrée. Une entrée peut bien entendu contenir plusieurs attributs.

```
dn: uid=martymac,ou=users,dc=martymac,dc=com
objectClass: account
objectClass: posixAccount
cn: martymac
uid: martymac
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/martymac
userPassword:: e0NSWVBUfWJjT29IUk5SbG1HbC4=
loginShell: /bin/sh
gecos: martymac
description: martymac
```

LDAP : un modèle d'information

- **Les classes d'objets**
  - L'objectClass d'une entrée est un attribut qui permet de cataloguer cette entrée.
  - Un objectClass définit un regroupement d'attributs obligatoires ou autorisés pour une entrée.
  - Une entrée peut posséder un ou plusieurs objectClass. Ce sont ces objectClass qui définissent la présence de tous les autres attributs.

LDAP : un modèle d'information

- **Les schémas**
  - La syntaxe et la liste des attributs connus de l'annuaire sont écrits dans ce que l'on appelle les "schémas".
  - Un annuaire LDAP a la capacité de charger en mémoire plusieurs schémas. A travers ces schémas, il est possible de définir de nouveaux attributs et de nouveaux objectClass.
  - Un schéma est un fichier qui décrit un à un les attributs disponibles (leur nom, leur type, etc...), ainsi que les objectClass qui y font appel.
  - Au démarrage du serveur LDAP, le ou les fichiers de schéma spécifiés dans sa configuration seront chargés.
  - Dans notre exemple, l'objectClass posixAccount est défini dans le fichier nis.schema.

LDAP : un modèle d'information

- **Les schémas**
  - Etudions une partie de ce fichier, livré avec OpenLDAP et situé dans /etc/ldap/schema :

```
# [...]
attributetype ( 1.3.6.1.1.1.1.0 NAME 'uidNumber'
        DESC 'An integer uniquely identifying a user in a domain'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

# [...]

objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY
        DESC 'Abstraction of an account with POSIX attributes'
        MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
        MAY ( userPassword $ loginShell $ gecos $ description ) )
```

LDAP : un modèle d'information

- **Le format LDIF**
  - Les données contenues dans l'annuaire sont présentées dans un certain format : il s'agit du format LDIF (LDAP Data Interchange Format - RFC 2849).
  - Sachez que toute interaction avec un annuaire se fait par le biais de ce format : l'ajout, la modification, la suppression d'entrées, l'interrogation de l'annuaire y compris.
  - Dans ce format, chaque entrée constitue un paragraphe, et, au sein de chaque paragraphe, chaque ligne constitue un attribut.

LDAP : un modèle d'information

- **Le format LDIF**
  - Voici un exemple un peu plus complet, incluant le groupe de notre utilisateur :

```
# [...]
dn: cn=utilisateurs,ou=groups,dc=martymac,dc=com
objectClass: posixGroup
cn: utilisateurs
gidNumber: 10001

dn: uid=martymac,ou=users,dc=martymac,dc=com
objectClass: account
objectClass: posixAccount
cn: martymac
uid: martymac
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/martymac
userPassword:: e0NSWVBUfWJjT29IUk5SbG1HbC4=
loginShell: /bin/sh
gecos: martymac
description: martymac
# [...]
```

LDAP : un modèle de sécurité

- **L'authentification simple, le binding**
  - pour avoir accès aux données
  - le "binding" : Le client envoie alors le DN d'un compte contenu dans l'annuaire lui-même, ainsi que le mot de passe associé.
  - ACL pour appliquer des droits particuliers (liste rouge)
  - Possible de se connecter de manière anonyme : le client envoie alors un DN vide au serveur LDAP.

LDAP : un modèle de sécurité

- **Les ACLs**
  - Les ACLs (Access Control Lists) interviennent après la notion de binding. Il sera possible de donner des droits de lecture, d'écriture (ou d'autres droits divers) sur des branches particulières de l'annuaire au compte connecté.
  - Ceci permet de gérer finement les droits d'accès aux données.

LDAP : un modèle de sécurité

- **Le chiffrement des communications (SSL/TLS)**
  - Le chiffrement des communications, via SSL (Secure Socket Layer, ou TLS - Transport Layer Security) est également une méthode de protection de l'information.
  - Il est possible, avec la plupart des annuaires existants, de chiffrer le canal de communication entre l'application cliente et l'annuaire.

LDAP : concept avancé

- **La réplication**
  - Un annuaire dit "maître" envoie par le biais du format LDIF, toutes les modifications effectuées sur un annuaire "esclave".

  L'avantage d'une telle opération est double :
  - permettre une meilleure montée en charge pour de gros annuaires : il est possible de rediriger le client vers l'un ou l'autre des annuaires répliqués
  - disposer d'une copie conforme du premier annuaire,

LDAP : concept avancé

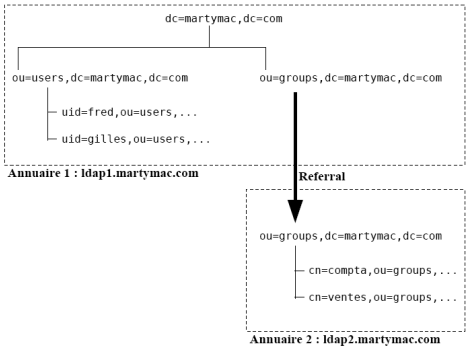
- **La distribution (les referrals)**

  La distribution est un mécanisme qui va permettre de faire pointer un lien vers un autre annuaire pour une branche particulière.

LDAP : concept avancé

- **La distribution (les referrals)**

  Ex :



LDAP : concept avancé

- **La distribution (les referrals)**

Ex :

```
dn: ou=groups,dc=martymac,dc=com
objectClass: referral
ref: ldap://ldap2.martymac.com/ou=groups,dc=martymac,dc=com
```

Plan

Administration des réseaux : Les annuaires

- Introduction
- Le protocole LDAP
- OpenLDAP

OpenLDAP

- **Liens :**

Site du projet : http://www.openldap.org

Historique des versions : http://www.openldap.org/software/roadmap.html

Historique du projet : http://www.openldap.org/conf/odd-sfo-2003/keynote.html

OpenLDAP : Outils clients

- Rechercher une entrée : ldapsearch

```
ldapsearch -x -H ldap://<serveur> -b <base> [-s portée] [filtre] [attributs]
```

Exemples :

ldapsearch -x -H ldap://localhost -b "dc=martymac,dc=com" "(uid=garf*)"

ldapsearch -x -H ldap://localhost -b dc=martymac,dc=com "(gidNumber=2000)"

ldapsearch -x -H ldap://localhost -b dc=martymac,dc=com "(&(gidNumber=2000)(objectClass=posixAccount))"

ldapsearch -x -H ldap://localhost -b dc=martymac,dc=com "(&(gidNumber=2000)(objectClass=posixAccount))" homeDirectory

OpenLDAP : Outils clients

- Supprimer une entrée : ldapdelete

```
ldapdelete -W -D <binddn> -x -H ldap://<serveur> <dn>
```

Exemples :

ldapdelete -x -H ldap://localhost -W -D "cn=Manager,dc=martymac,dc=com" "uid=odie,ou=users,dc=martymac,dc=com"

ldapdelete -x -H ldap://localhost -W -D "cn=Manager,dc=martymac,dc=com" -r "ou=users,dc=martymac,dc=com"