LDAP

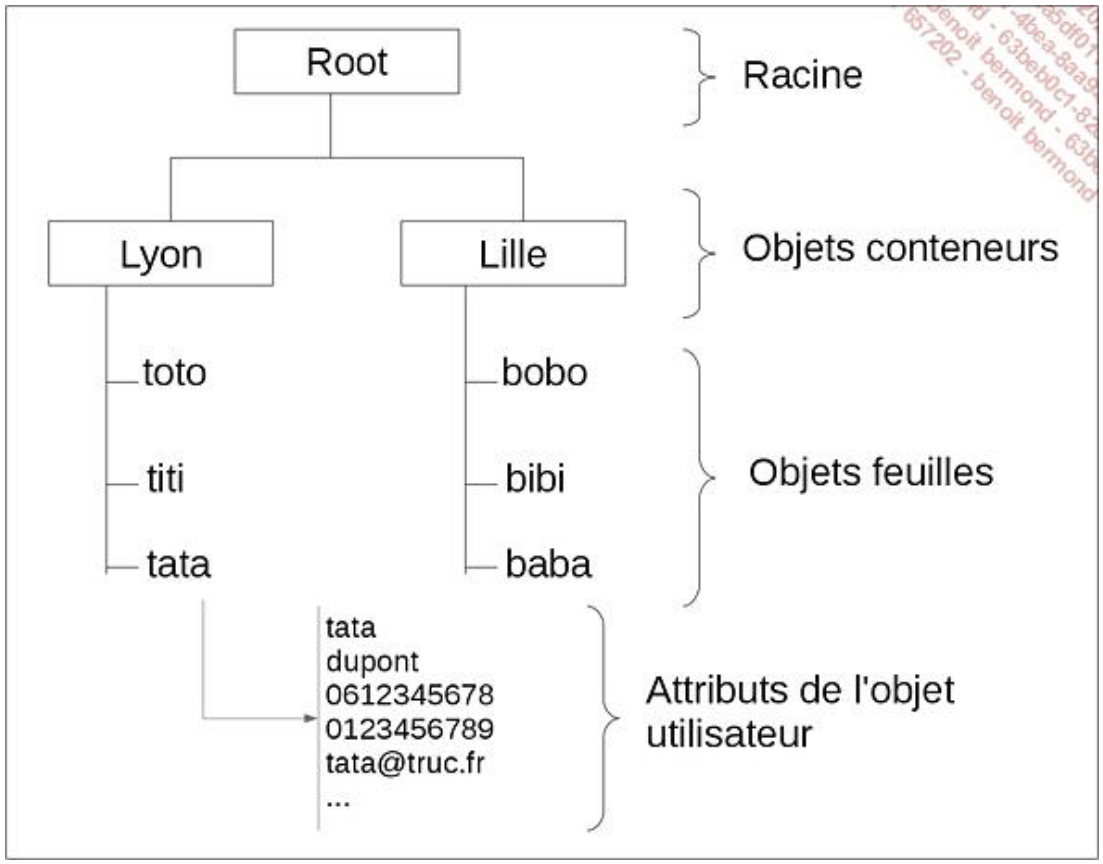
1. Généralités

a. Les annuaires

En 1990, l'ITU (*International Telecommunication Union*) propose une norme de structuration des annuaires électroniques. Cette norme, visant à proposer à tous les développeurs qui y souscrivent un cadre de fonctionnement et de référencement commun porte le nom de X500.

Les premiers logiciels à exploiter cette norme furent naturellement les messageries électroniques. La NDS (*Netware Directory Services*) célèbre en son temps, fut le premier usage marquant des technologies d'annuaires X500 au service d'un système d'exploitation réseau. Les annuaires sont aujourd'hui largement répandus, soit au sein du système d'exploitation réseau (l'Active Directory de Microsoft), soit sous forme d'annuaire « neutre », à la disposition d'autres applications. On parle alors d'annuaires « pages blanches ».

b. Structure et terminologie



Les annuaires électroniques X500 présentent des caractéristiques de structure communes. Les annuaires sont hiérarchisés, et ont forcément un point d'origine généralement appelé Root. Tout élément de l'annuaire est appelé objet ; certains éléments sont structurants et d'autres strictement informatifs. Les éléments structurants sont appelés conteneurs et sont de types divers comme l'organisation, le domaine ou encore l'unité organisationnelle.

Tout objet de l'annuaire renferme en son sein des informations de formats divers. Ces informations sont appelées attributs de l'objet.

c. Schéma

Les annuaires sont à l'origine prévus pour stocker et gérer des identités, et on y trouvera naturellement des objets représentant des personnes, et des attributs permettant d'identifier et de définir la personne, comme le nom, le prénom, le téléphone et l'adresse de messagerie. L'ensemble des types d'objets possibles dans l'annuaire, et pour chaque objet l'ensemble des attributs utilisables est défini dans le schéma de l'annuaire.

Toutefois, il est naturel pour un éditeur ou un utilisateur de vouloir stocker dans son annuaire des informations de nature particulière pour les besoins propres de ses applications. Si le schéma d'origine ne le permet pas, on peut alors réaliser une extension de schéma. L'extension de schéma consiste à définir pour un annuaire de nouveaux types d'objets, ou de nouveaux attributs pour un type d'objet existant. Par exemple, si une entreprise dispose d'un annuaire recensant l'ensemble de son personnel, et que ledit personnel doit porter des chaussures de sécurité, on aura intérêt à étendre le schéma pour ajouter aux objets utilisateur l'attribut « pointure » plutôt que de gérer une liste plus ou moins à jour sur un tableur.

Le type de chaque objet (unité organisationnelle, utilisateur, groupe, etc.) est appelé classe. Une classe d'objets se définit par l'ensemble des attributs qui la compose. Parmi ces attributs, un aura une importance particulière dans la dénomination de l'objet, c'est le CN (*Common Name*).

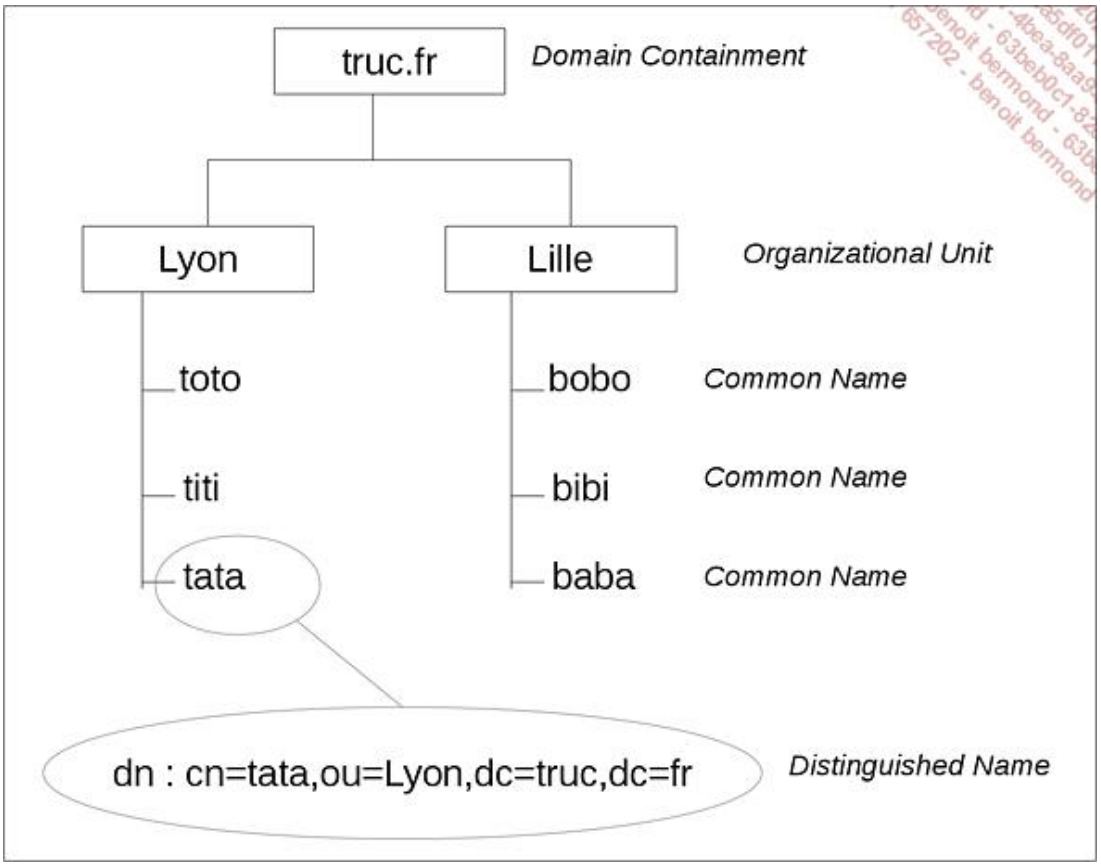
d. Le protocole LDAP

La norme X500 ne prévoyant pas à l'origine de protocole d'interrogation des annuaires, une proposition de protocole a été faite en 1993 par l'université du Michigan pour un créer un protocole qui, fonctionnant sur TCP/IP, assurerait des requêtes simples à un annuaire X500 : c'était la naissance de LDAP (*Leightweight Directory Access Protocol*). Les annuaires X500 en place durent donc implémenter une couche serveur pour le protocole LDAP afin de pouvoir répondre aux requêtes des clients exploitant ce nouveau protocole.

Rapidement, le succès du protocole LDAP fut tel qu'on oublia le rôle fondateur de X500 pour ne plus parler que d'annuaires LDAP. Et on parle aujourd'hui d'annuaire LDAP pour tout annuaire capable de répondre à des requêtes LDAP. Les éléments de structure et de dénominations X500 ont néanmoins perduré et on parle toujours d'objets, de conteneurs et de schéma.

e. Désignation des objets

Nous avons vu que les objets de l'annuaire s'inséraient dans une arborescence. Pour une désignation sans ambiguïté des objets dans un annuaire, il existe une notation formelle qui reprend la position de l'objet dans l'arborescence de l'annuaire, ainsi que son type. Cette notation est le DN (*Distinguished Name*).



Format type d'un nom distinctif

```
classe1=nom_objet1,classe2=nom_objet2,...,classen=nom_objetn
```

Où les paramètres *classex* représentent la classe de l'objet décrit (cn, ou, uid, etc.), et les paramètres *objetsx*

représentent les noms des objets décrits.

Le nom distinctif reprend toute l'arborescence de l'objet référencé jusqu'à la racine de l'annuaire, chaque changement de niveau étant représenté par des virgules. Pour chaque objet cité, la classe de cet objet est obligatoirement mentionnée.

Le nom distinctif sera employé pour désigner un objet de l'annuaire, et son utilisation sera obligatoire pour les opérations d'authentification.

f. Authentification auprès d'un annuaire LDAP

Les annuaires gèrent leur propre sécurité. Si souvent les requêtes anonymes sont autorisées pour des consultations en lecture, il faudra s'authentifier auprès de l'annuaire pour les opérations d'écriture. Cette authentification se fait en fournissant le nom distinctif et le mot de passe d'un compte de l'annuaire ayant les droits nécessaires sur les éléments à gérer. En terminologie LDAP, on parle de « bind » (liaison) pour l'authentification.

g. Le format LDIF

LDIF (*LDAP Data Interchange Format - Format d'échange des données LDAP*) a pour objet de permettre l'exportation ou l'importation des données depuis ou vers un annuaire LDAP. LDIF décrit un format de fichier texte qui contient tout ou partie des données d'un annuaire LDAP. On peut y mentionner l'intégralité des objets et de leurs attributs, ou seulement une sélection. Le format LDIF est employé par de nombreux utilitaires LDAP.

Format type d'une entrée de fichier LDIF

```
dn: nom_distinctif
attribut1: valeur1
attribut2: valeur2
...
attributn: valeurn
```

Il est tentant de considérer LDIF comme un format privilégié pour échanger des données d'un annuaire vers un autre, en cas de migration ou d'échanges de données. En fait, les fichiers LDIF décrivent les objets d'un annuaire conformément à son schéma, et il est bien rare que deux annuaires différents présentent rigoureusement le même schéma. Pour ces raisons, le format LDIF n'est en général utilisé que pour manipuler les données d'un même annuaire, dans le cas d'une sauvegarde par exemple. Les solutions de méta-annuaires qui permettent ce type de synchronisation exploitent généralement un format plus ouvert comme le format XML.

---

2. Le serveur OpenLDAP

OpenLDAP est l'implémentation de serveur LDAP open source la plus courante sur les systèmes Linux. Si elle manque cruellement de convivialité par rapport à ses équivalents commerciaux, elle n'en est pas moins répandue dans toutes sortes d'implémentation qui vont de la centralisation de l'authentification à la gestion de comptes et carnets d'adresses pour les messageries.

a. Gestion du Service

Le service openldap est géré par un script normalisé dans le répertoire **/etc/init.d**. Son nom est variable et dépend de la distribution. L'ambiguïté vient du fait que le protocole applicatif est LDAP, alors que le nom de l'exécutable est **slapd** et le nom du produit applicatif openldap.

b. Configuration

Dans un fonctionnement standard, la configuration initiale ne représente pas un travail considérable. Il s'agit surtout d'avoir un contexte de base : une sorte de point de départ de l'arborescence dans lequel se trouveront tous les objets créés dans l'annuaire. La configuration se trouve dans un fichier **slapd.conf**, généralement situé dans le répertoire **/etc/ldap** ou **/etc/openldap**. Ce fichier comprend aussi la déclaration de l'administrateur de l'annuaire ainsi que son mot de passe.

Déclaration du contexte de base dans le fichier slapd.conf

```
suffix      "dc=domaine"
```

Où *domaine* représente le contexte principal de l'arborescence. Cette valeur est fréquemment renseignée lors de l'installation par les scripts de post-installation des paquetages. Il est possible pour un annuaire openldap de gérer plusieurs arborescences.

Déclaration du compte administrateur dans le fichier slapd.conf

```
rootdn        "cn=compte_admin,dc=domaine"
```

Où *compte_admin* représente le compte administrateur de l'annuaire. Attention, contrairement à d'autres implémentations LDAP, il n'est pas obligatoire que le compte administrateur soit aussi un objet de l'annuaire.

Déclaration du mot de passe administrateur dans le fichier slapd.conf

```
rootpw {format_cryptage}mot_de_passe_crypté
```

Où *format_cryptage* représente l'algorithme de hachage utilisé pour crypter le mot de passe (SHA1, MD5, crypt, ou texte clair).

Pour simplifier la saisie du mot de passe, la commande **slappasswd** permet de générer la chaîne de caractères constituée du mode de cryptage et du mot de passe crypté, directement insérable dans **slapd.conf**.

Exemple d'utilisation de la commande slappasswd

La commande slappasswd envoyant son résultat sur la sortie standard, il faut ruser un peu pour l'intégrer au fichier slapd.conf.

```
[root@beta openldap]# slappasswd -s motdepasse
{SSHA}oW6wu+yUpFnaB6tg+4cMWnAa8OmDXV62
[root@beta openldap]# echo "rootpw $(slappasswd -s motdepasse)" >> slapd.conf
[root@beta openldap]#
```

À ce stade, l'annuaire est fonctionnel après redémarrage du service, mais vide. Il reste à l'alimenter avec les clients LDAP.

3. Les outils clients LDAP

On dispose pour Linux d'outils en ligne de commande permettant de réaliser des opérations sur les serveurs LDAP. Ces outils sont généralement fournis dans un paquetage applicatif appelé **ldap-utils**. Leur syntaxe peu engageante implique un petit temps d'adaptation pour les exploiter confortablement.

a. Recherche d'informations avec ldapsearch

Sans doute le plus couramment utilisé des outils clients en ligne de commande LDAP. La commande **ldapsearch** permet d'effectuer des requêtes sur un annuaire LDAP et de récupérer le résultat au format LDIF.

Le cas le plus simple consiste à demander localement (directement sur le serveur) l'export total de toutes les informations d'un annuaire et on utilise souvent cette possibilité pour vérifier la présence d'un objet ou simplement que l'annuaire répond bien aux requêtes.

Syntaxe de la commande ldapsearch pour exporter toutes les informations publiques d'un annuaire

```
ldapsearch -x -b contexte
```

Export avec ldapsearch : options et paramètres	
-x	Utilise une authentification simple (cas général).
-b *contexte*	Réalise la recherche à partir du DN du conteneur contexte.

Syntaxe de la commande ldapsearch pour récupérer des informations précises selon critères de recherche

```
ldapsearch -x -D dn_admin -W -h ip_serveur -b contexte -s sub attribut=valeur
```

Recherche avec ldapsearch : options et paramètres	
-D dn_admin	Fait l'authentification avec le nom distinctif *dn_admin*.
-W	Demande interactivement le mot de passe. Peut être remplacé par -w (minuscule) suivi du mot de passe en clair dans la ligne de commande.
-h *ip_serveur*	S'adresse au serveur dont l'adresse est *ip_serveur*.
-s sub	Réalise une recherche récursive dans tous les niveaux subordonnés au contexte de recherche.
attribut	Le nom de l'attribut qui sera le critère de recherche.
valeur	La valeur de l'attribut recherché. Le caractère « * » représente n'importe quelle valeur existante.

Exemples de recherche avec ldapsearch

On veut afficher tous les utilisateurs se trouvant dans l'annuaire dont le numéro de téléphone commence par 01.

```
user@ubuntu:~$ ldapsearch -x -D cn=admin,dc=pas,dc=net -w password
-h 172.17.7.20 -b dc=pas,dc=net -s sub telephoneNumber=01*
# extended LDIF
#
# LDAPv3
# base <dc=pas,dc=net> with scope subtree
# filter: telephoneNumber=01*
# requesting: ALL
#

# toto, lyon, pas.net
dn: cn=toto,ou=lyon,dc=pas,dc=net
objectClass: person
cn: toto
sn: toto
telephoneNumber: 0123456789

# tutu, paris, pas.net
dn: cn=tutu,ou=paris,dc=pas,dc=net
objectClass: person
cn: tutu
sn: tutu
telephoneNumber: 0178945632

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

On souhaite maintenant afficher l'ensemble des utilisateurs de l'unité organisationnelle paris. Notez le contexte de recherche (-b ou =paris,dc=pas,dc=net) et le filtre de recherche qui vise à vérifier que l'attribut téléphone est renseigné. (telephoneNumber=).*

```
user@ubuntu:~$ ldapsearch -x -D cn=admin,dc=pas,dc=net -w password
-h 172.17.7.20 -b ou=paris,dc=pas,dc=net -s sub telephoneNumber=*
# extended LDIF
#
# LDAPv3
# base <ou=paris,dc=pas,dc=net> with scope subtree
```

```
# filter: telephoneNumber=*
# requesting: ALL
#

# tata, paris, pas.net
dn: cn=tata,ou=paris,dc=pas,dc=net
objectClass: person
cn: tata
sn: tata
telephoneNumber: 9876543210

# tutu, paris, pas.net
dn: cn=tutu,ou=paris,dc=pas,dc=net
objectClass: person
cn: tutu
sn: tutu
telephoneNumber: 0178945632

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Toutes les connexions aux serveurs LDAP sont effectuées avec l'option -x indiquant une authentification en texte clair. Cela constitue naturellement un risque en matière de sécurité. La connexion avec authentification SASL permettrait de remédier à cette situation. Toutefois, sa complexité de mise en œuvre et le fait que la plupart des consultations se font en mode anonyme font que l'authentification SASL est rarement utilisée.

b. Ajout d'objets dans un annuaire avec ldapadd

Pour l'essentiel, la commande **ldapadd** va lire le contenu d'un fichier LDIF contenant les données à modifier, et les ajouter à l'annuaire. La construction du fichier se doit d'être rigoureuse mais ne présente pas de difficulté.

Syntaxe simplifiée de la commande ldapadd

`ldapadd -x -D dn_admin -W -h ip_serveur -f fichier_ldif`

ldappadd : options et paramètres	
-x	Utilise une authentification simple (cas général).
-D *dn_admin*	Fait l'authentification avec le nom distinctif *dn_admin*.
-W	Demande interactivement le mot de passe. Peut être remplacé par -w (minuscule) suivi du mot de passe en clair dans la ligne de commande.
-h *ip_serveur*	S'adresse au serveur dont l'adresse est *ip_serveur*.
-f *fichier_ldif*	Ajoute les objets référencés dans le fichier *fichier_ldif*.

Exemple de fichier LDIF pour ajout par la commande ldapadd

Appelons ce fichier toto.ldif

```
dn: cn=toto,dc=pas,dc=net
objectClass: person
cn: toto
sn: toto
telephoneNumber: 0123456789
```

Exemple d'utilisation de ldapadd

```
root@serveur# ldapadd -D cn=admin,dc=pas,dc=net -W -h 192.168.1.10 -f toto.ldif
root@serveur#
```

c. Modification d'objet existant avec ldapmodify

La commande **ldapmodify** va également être utilisée avec un fichier ldif comme argument, et ses paramètres d'utilisation sont les mêmes que ceux de la commande **ldapadd**.

Syntaxe simplifiée de la commande ldapmodify

```
ldapmodify -D dn_admin -W -h ip_serveur -f fichier_ldif
```

Exemple de fichier LDIF pour ajout par la commande ldapmodify

```
dn: cn=toto,dc=pas,dc=net
changetype: modify
replace: telephoneNumber
telephoneNumber: 9876543210
```

d. Suppression d'objet avec ldapdelete

La commande **ldapdelete** peut s'employer directement sans passer par un fichier ldif.

Exemple de suppression d'objet avec ldapdelete

```
root@serveur# ldapdelete -D cn=admin,dc=pas,dc=net -w password -h
127.0.0.1 -x cn=toto,dc=pas,dc=net
root@serveur#
```

e. Modification de mot de passe avec ldappasswd

La commande **ldappasswd** permet d'affecter un mot de passe encrypté à un objet utilisateur présent dans l'annuaire.

Syntaxe simplifiée de la commande ldappasswd

```
ldappasswd -x -D dn_admin -W -h ip_serveur -s motdepasse dn_utilisateur
```

ldappasswd : options et paramètres	
-s *motdepasse*	Le mot de passe que l'on souhaite affecter au nouvel utilisateur. Peut être remplacé par -S (majuscule) pour une frappe interactive du nouveau mot de passe.
dn_utilisateur	Le nom distinctif de l'utilisateur dont il faut modifier le mot de passe.

Exemple d'utilisation de la commande ldappasswd

La première commande affecte le mot de passe à l'utilisateur tata. Notez l'usage des options -w et -s qui permettent d'inclure les mots de passe (mot de passe d'authentification et mot de passe de l'utilisateur) directement dans la ligne de commande sans avoir à les taper de façon interactive.

La deuxième commande provoque l'affichage de toutes les propriétés de l'utilisateur tata, et on voit bien le mot de passe crypté apparaître sous l'attribut userPassword.

```
user@ubuntu:~$ ldappasswd -x -D cn=admin,dc=pas,dc=net -w password
-h 172.17.7.20 -s motdepasse cn=tata,ou=paris,dc=pas,dc=net
```

```
user@ubuntu:~$ ldapsearch -x -D cn=admin,dc=pas,dc=net -w password
-h 172.17.7.20 -s sub -b dc=pas,dc=net cn=tata
# extended LDIF
#
# LDAPv3
# base <dc=pas,dc=net> with scope subtree
# filter: cn=tata
# requesting: ALL
#

# tata, paris, pas.net
dn: cn=tata,ou=paris,dc=pas,dc=net
objectClass: person
cn: tata
sn: tata
telephoneNumber: 9876543210
userPassword:: e1NTSEF9RVpNNVV6RFN1M2xKbUgwZVhDTmpVWGhacEtSOTNxSFU=

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
user@ubuntu:~$
```

f. Allègement des syntaxes pour les utilitaires clients LDAP

Chacun des utilitaires clients en lignes de commande peut trouver certains éléments de configuration dans le fichier **ldap.conf**. La syntaxe des commandes en sera allégée d'autant. Son emplacement est généralement **/etc/ldap/ldap.conf**, mais il peut varier au gré des implémentations.

Fichier ldap.conf courant

```
BASE contexte
HOST ip_serveur
```

Fichier ldap.conf : principaux paramètres	
BASE *contexte*	Réalise les recherches à partir du DN du conteneur *contexte*.
HOST *ip_serveur*	Les requêtes s'adressent au serveur dont l'adresse est *ip_serveur*.

Il est également possible de déclarer le contexte de base LDAP par la variable LDAPBASE. Le renseignement du fichier ldap.conf constitue toutefois une méthode plus universelle.

g. Clients graphiques

Les applications compatibles LDAP intègrent un client leur permettant de réaliser des requêtes auprès de l'annuaire pour assurer leur fonctionnement. Par exemple, un client de messagerie est en général capable d'aller vérifier la validité d'un compte ou de faire une recherche auprès d'un annuaire LDAP. Toutefois, si on utilise un annuaire LDAP au service d'une application, il sera souvent pratique de disposer d'un outil graphique « universel », qui permettra de vérifier le bon fonctionnement de l'annuaire et éventuellement de l'alimenter indépendamment de l'application cliente. Ces outils sont assez nombreux et de qualités diverses. On peut citer luma, gq, lat.

Exemple de visualisation depuis le client graphique luma