# PRESENTATION DE LDAP ( Lightweight Directory Access Protocol)

## QU'EST-CE QU'UN ANNUAIRE ?

Un annuaire est une base de données spécialisée optimisée en lecture, pouvant être répartie géographiquement qui permet de partager des bases d'informations sur le réseau interne ou externe. Ces bases peuvent contenir toute sorte d'informations que ce soit des coordonnées de personnes ou des données systèmes.

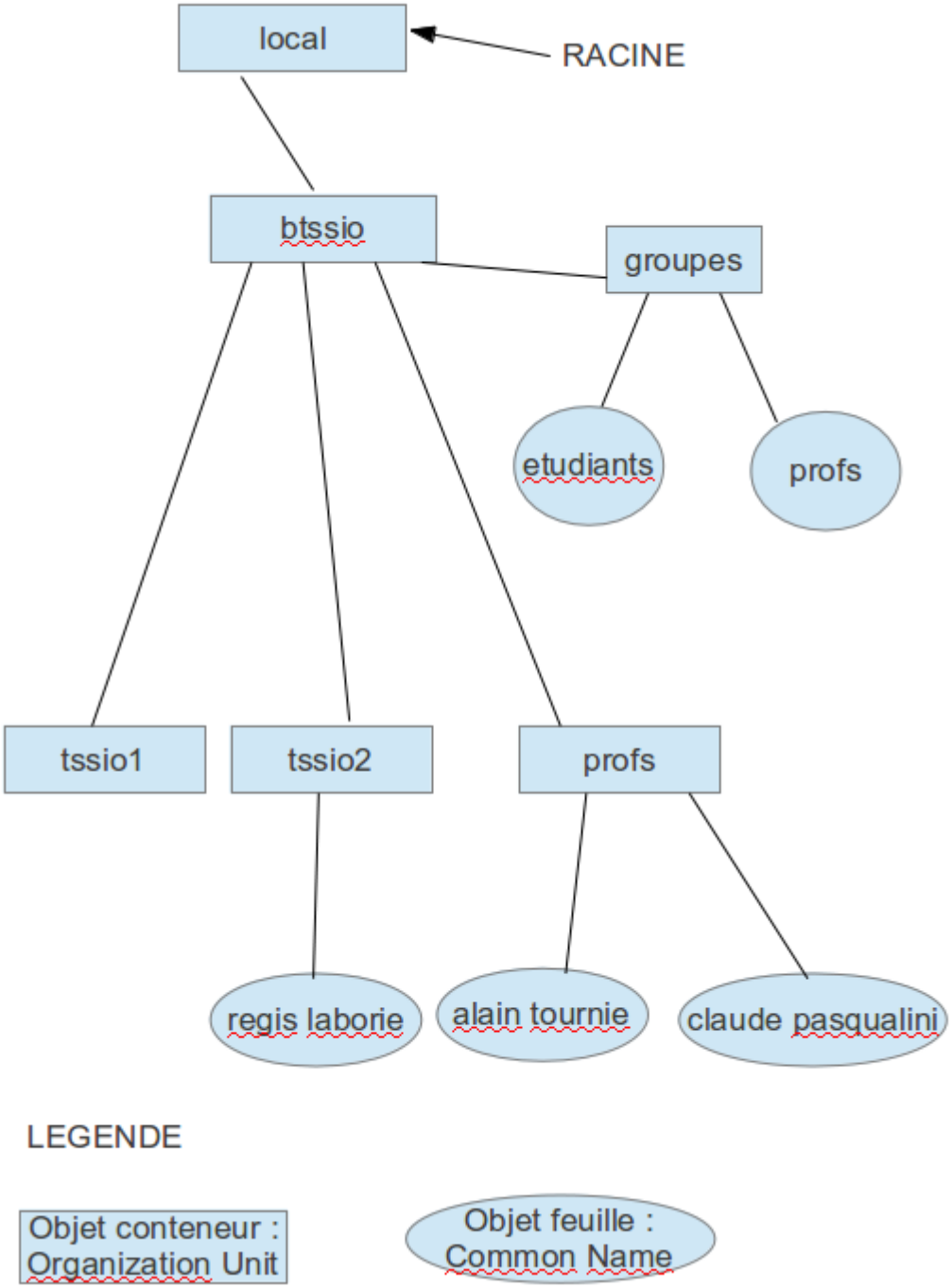
**Le protocole LDAP**

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 créer un protocole qui, fonctionnant sur TCP/IP, assurerait des requêtes simples à un annuaire X500 : c’était la naissance de LDAP (Lightweight 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.

## 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.




## SCHEMA

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).

# DESIGNATION 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.

**Exemples**

```
cn=Claude pasqualini,ou=PROFS,dc=btssio,dc=local
```

code>cn=regis laborie,ou=TSSIO2,dc=btssio,dc=local</code>

# AUTHENTIFICATION AUPRES D'UN SERVEUR 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.

# LE FORMAT LDIF (LDAP Data Interchange Format)

**LDIF** (**L**DAP **D**ata **I**nterchange **F**ormat - 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
```

**IMPORTANT :** 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.

Voir ANNEXE

# 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.

## 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. Sur l'appliance virtuelle Turnkey OpenLdap, il s'agit de :

```
/etc/init.d/slapd
```

### 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.

Sur l'appliance virtuelle Turnkey OpenLdap, il s'agit de :

```
/etc/ldap/ldap.conf
```

## LES OUTILS CLIENTS LDAP

### OUTILS EXPLOITABLES EN MODE COMMANDE

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. C'est un des objectifs du TP associé à ce chapitre !

### CLIENTS GRAPHIQUES

Ces clients sont assez nombreux et de qualités diverses.

Citons « luma » par exemple.

Dans le TP associé, nous utiliserons phpLDAPadmin 1.2.2 accessible depuis n'importe quel navigateur.

## PRESENTATION DU PROJET TURNKEY

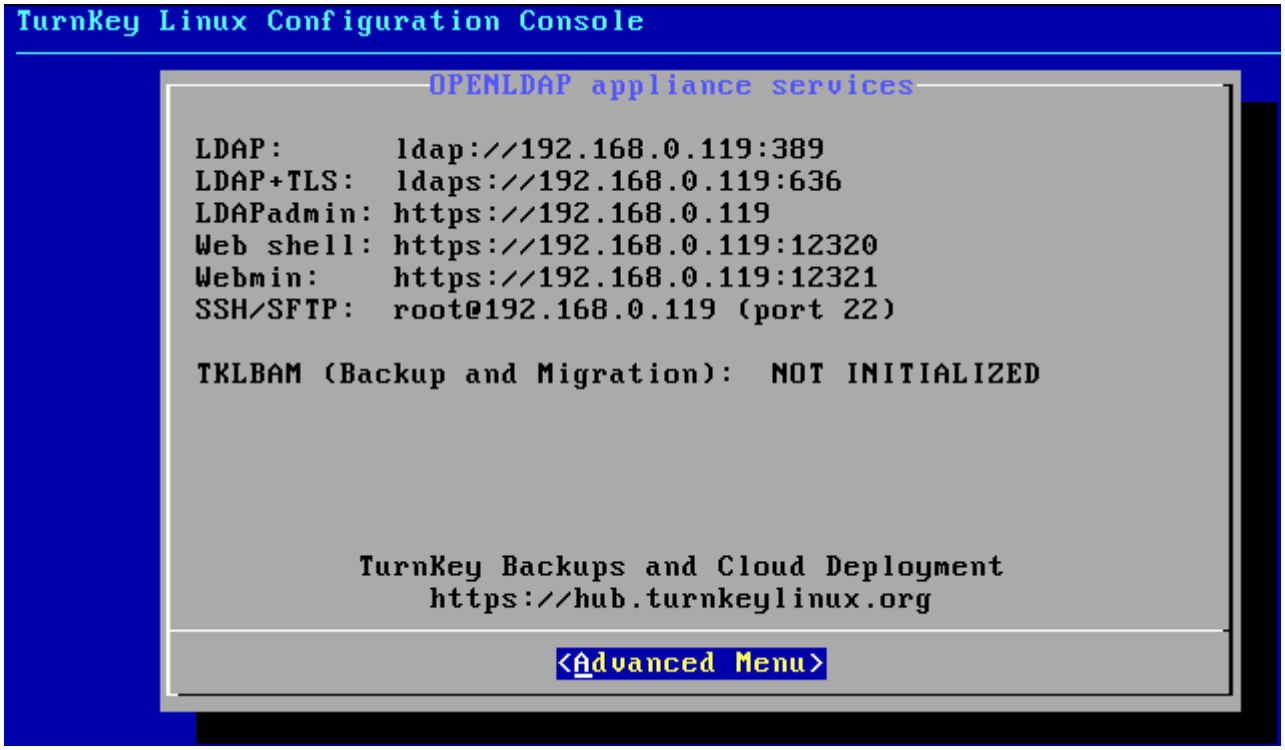
TURNKEY

Turnkey propose  plus de 45 machines virtuelles (ou ISO bootables) linux équipées de l'application web de votre choix.

Ces appliances virtuelles tournent sans problème sur Vmware, et Virtualbox mais aussi Parallels et Xen) et les ISO sont bootables. Il s'agit d'une Ubuntu 10.04.1, qui au démarrage vous posera quelques questions pour configurer la machine et qui ensuite, vous donnera les adresses d'accès à l'application, mais aussi au Webmin, Phpmyadmin, webshell et au SSH. Du 100% clé en main...

L'appliance virtuelle TURNKEY qui nous intéresse ici est « **Turnkey openladap** ».

Voilà ce que l'on obtient après lancement de la VM :




## ANNEXE : EXEMPLE DE FICHIER LDIF

```
# LDIF Export for dc=btssio,dc=local
# Server: TurnKey OpenLDAP (127.0.0.1)
# Search Scope: sub
# Search Filter: (objectClass=*)
# Total Entries: 12
#
# Generated by phpLDAPadmin (http://phpldapadmin.sourceforge.net) on January 7, 2013 10:08 am
# Version: 1.2.2

version: 1

# Entry 1: dc=btssio,dc=local
dn: dc=btssio,dc=local
dc: btssio
o: btssio.fr
objectclass: top
objectclass: dcObject
objectclass: organization

# Entry 2: cn=admin,dc=btssio,dc=local
dn: cn=admin,dc=btssio,dc=local
cn: admin
description: LDAP administrator
objectclass: simpleSecurityObject
objectclass: organizationalRole
objectclass: top
userpassword: {SSHA}EWPKqv1oKfas871TjEawcdvcxDfpGcPu

# Entry 3: cn=gestionnaire,dc=btssio,dc=local
dn: cn=gestionnaire,dc=btssio,dc=local
cn: gestionnaire
description: LDAP administrator
objectclass: simpleSecurityObject
objectclass: organizationalRole
userpassword: {SSHA}01nAXBqUd57veCeQbjOMOYPag9JIwr9B

# Entry 4: ou=Groups,dc=btssio,dc=local
dn: ou=Groups,dc=btssio,dc=local
objectclass: organizationalUnit
```

```
objectclass: top
ou: Groups

# Entry 5: cn=ETUDIANTS,ou=Groups,dc=btssio,dc=local
dn: cn=ETUDIANTS,ou=Groups,dc=btssio,dc=local
cn: ETUDIANTS
gidnumber: 503
objectclass: posixGroup
objectclass: top

# Entry 6: cn=PROFS,ou=Groups,dc=btssio,dc=local
dn: cn=PROFS,ou=Groups,dc=btssio,dc=local
cn: PROFS
cn: ETUDIANTS
gidnumber: 503
objectclass: posixGroup
objectclass: top

# Entry 7: ou=PROFS,dc=btssio,dc=local
dn: ou=PROFS,dc=btssio,dc=local
objectclass: organizationalUnit
objectclass: top
ou: PROFS

# Entry 8: cn=alain tournie,ou=PROFS,dc=btssio,dc=local
dn: cn=alain tournie,ou=PROFS,dc=btssio,dc=local
cn: alain tournie
gidnumber: 502
givenname: alain
homedirectory: /home/users/atournie
loginshell: /bin/sh
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: tournie
uid: atournie
uidnumber: 1000
userpassword: {MD5}QIg63WPx+6vH/mFY+TwSRg==

# Entry 9: cn=Claude pasqualini,ou=PROFS,dc=btssio,dc=local
dn: cn=Claude pasqualini,ou=PROFS,dc=btssio,dc=local
cn: Claude pasqualini
gidnumber: 503
givenname: Claude
homedirectory: /home/users/cpasqualini
loginshell: /bin/sh
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: pasqualini
uid: cpasqualini
uidnumber: 1002
userpassword: {MD5}QIg63WPx+6vH/mFY+TwSRg==

# Entry 10: ou=TSSIO1,dc=btssio,dc=local
dn: ou=TSSIO1,dc=btssio,dc=local
objectclass: organizationalUnit
objectclass: top
ou: TSSIO1

# Entry 11: ou=TSSIO2,dc=btssio,dc=local
dn: ou=TSSIO2,dc=btssio,dc=local
objectclass: organizationalUnit
objectclass: top
ou: TSSIO2

# Entry 12: cn=regis laborie,ou=TSSIO2,dc=btssio,dc=local
dn: cn=regis laborie,ou=TSSIO2,dc=btssio,dc=local
cn: regis laborie
gidnumber: 506
```

```
givenname: regis
homedirectory: /home/users/rlaborie
loginshell: /bin/sh
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: laborie
uid: rlaborie
uidnumber: 1001
userpassword: {MD5}QIg63WPx+6vH/mFY+TwSRg==
```

From:
/ - **Les cours du BTS SIO**

Permanent link:
**/doku.php/si5/presldap**

Last update: **2014/01/06 19:11**