

# LDAP, Authentification distante

## Administration Système et Réseaux, Sécurité

### LDAP, Authentification distante

Philippe Harrand

<sup>1</sup> Département Informatique  
Pôle Sciences et Technologies

<sup>2</sup> Direction Territoriale Sud Ouest  
France Télécom

21 octobre 2007

LDAP

Généralités

SLAPD

Client LDAP

Authentification

# LDAP ?

- ▶ Lightweight **D**irectory **A**ccess **P**rotocol
- ▶ Protocole *léger*
- ▶ Accéder un *annuaire*
- ▶ Client / Serveur

# Annuaire

- ▶ Plus souvent lu qu'écrit
- ▶ Données présentées de manière hiérarchique
- ▶ Compacts et protocole réseau léger
- ▶ Mécanismes de recherche performants
- ▶ Résultats organisés
- ▶ Annuaire répartis
- ▶ Authentification des utilisateurs
- ▶ Gestion des droits pour la consultation ou la modification

**Base de données spécialisée**

## Organisation Objet

- ▶ Généricité de la structure
- ▶ Classes structurantes  
=> définissent la structure
- ▶ Classes auxiliaires  
=> stocquent les données
- ▶ Attributs
  - ▶ Object identifiant **OID** => pour les machines
  - ▶ nom unique **DN** => pour les cyborgs
  - ▶ Syntaxe et règles de comparaison
  - ▶ Mono ou multivalué
  - ▶ Description
  - ▶ Format

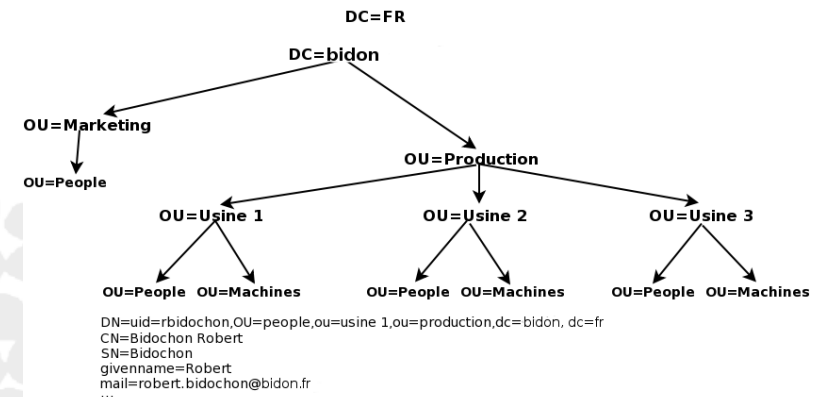
## Attributs courants

- ▶ uid (userid), identifiant présumé unique
- ▶ **cn** (common name), nom complet de la personne
- ▶ **givenname**, prénom de la personne
- ▶ **sn** (surname), nom de famille de la personne
- ▶ **o** (organization), entreprise de la personne
- ▶ **ou** (organization unit), service de l'entreprise dans laquelle la personne travaille
- ▶ **mail**, adresse de courrier électronique de la personne

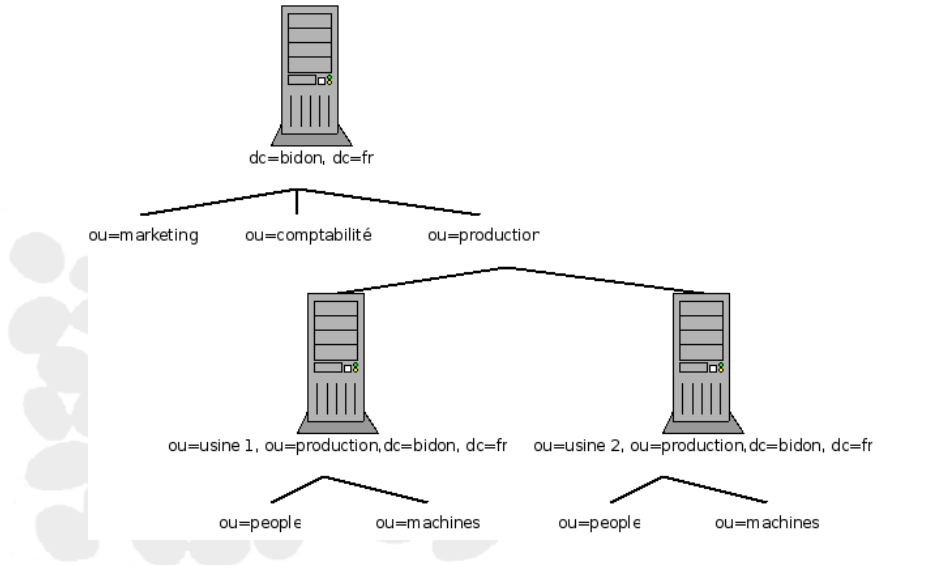
## Exemple

- ▶ Une instance d'objet => un **DN**
  - ▶ Hiérarchique
  - ▶ RDN + hiérarchie
- ▶ Les annuaires font partie de l'"annuaire mondial"
- ▶ ils s'y raccordent par le **BaseDN**
- ▶ Un annuaire peut être réparti sur plusieurs serveurs
- ▶ Semblable au DNS

## Exemple



## Exemple de répartition



## openLDAP

- ▶ Implémentation libre du protocole
- ▶ Packages
  - ▶ openldap partie commune
  - ▶ openldap-clients
  - ▶ openldap-servers
- ▶ le serveur slapd
  - ▶ /etc/openldap/slapd.conf
  - ▶ schémas standard : /usr/share/openldap/schema/ personnels /etc/openldap/schema/
- ▶ les clients
  - ▶ /etc/openldap/ldap.conf
- ▶ Attention la v2 LDAP V3 est incompatible avec la v1 LDAP V2

## Schémas

- ▶ Les schémas contiennent
  - ▶ commentaires et OID
  - ▶ définition des attributs nouveaux et leurs OID
  - ▶ définition des classes *objectclass* et leurs OID
- ▶ Il existe des schémas prédéfinis
- ▶ Vous pouvez définir les vôtres
- ▶ Mais ce n'est pas une bonne idée

## Object Identifier

OID	Assignment
1.1	Organization's OID
1.1.1	SNMP Elements
1.1.2	LDAP Elements
1.1.2.1	AttributeTypes
1.1.2.1.1	myAttribute
1.1.2.2	ObjectClasses
1.1.2.2.1	myObjectClass

FIG.: Organisation des OID

## Schémas

### ▶ Attribut

attributetype ( 0.9.2342.19200300.100.1.10 NAME 'manager'  
DESC 'RFC1274 : DN of manager'  
EQUALITY distinguishedNameMatch  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

### ▶ Objet

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 ) )

## SLAPD

- ▶ SLAPD = serveur openLDAP
- ▶ fichier de configuration : */etc/openldap/slapd.conf*  
Attention aux espaces en début de ligne
  1. Configuration générale
    - ▶ schémas
    - ▶ paramètres globaux
  2. Configuration de(s) l'annuaire(s)
    - ▶ type de fichiers de données
    - ▶ DN de base
    - ▶ identification de l'administrateur
    - ▶ indexes
    - ▶ ACL

## ACL (exemple)

access to attr=userPassword  
by self write  
by anonymous auth  
by dn="uid=root,ou=People,dc=example,dc=com" write  
by \* none

## Structure de l'annuaire

- ▶ Oubliez les SGBD
- ▶ Structure évolutive
- ▶ seul objet obligatoire :  
dn=dc=bidon,dc=fr  
objectClass : top  
objectClass : dcObject
- ▶ Instancier les noeuds de l'arbre
- ▶ Puis les feuilles
- ▶ les feuilles incluent les classes de toute l'arborescence
- ▶ et les classes définissant les attributs

## Clients

- ▶ ligne de commande
- ▶ fournis par openLDAP :
  - ▶ ldapcompare, ldapmodify, ldappasswd, ldapwhoami, ldapadd, ldapdelete, ldapmodrdn, ldapsearch
  - ▶ slapadd, slapcat, slapdn, slappasswd, slapacl, slapauth, slapindex, slaptest
- ▶ graphiques
  - ▶ GQ
  - ▶ phpLdapAdmin
  - ▶ divers clients java
  - ▶ Mozilla addresses books, Microsoft Outlook, NetMeeting, Navigateur Web : URLs LDAP

## LDIF

- ▶ Lightweight Data Interchange Format
- ▶ fichiers ASCII
- ▶ permet la population d'un annuaire, sa réplication
- ▶ les entrées sont séparées par une ligne vide

## LDIF exemple

```
dn : dc=bidon,dc=fr
dc : tp
o : bidon.fr
objectClass : top
objectClass : dcObject
objectClass : organization
ligne vide
dn : ou=people,dc=bidon,dc=fr
dc : bidon
ou : people
objectClass : top
objectClass : dcObject
objectClass : organizationalUnit
ligne vide
dn : ou=groups,dc=bidon,dc=fr
dc : bidon
ou : groups
objectClass : top
objectClass : dcObject
objectClass : organizationalUnit
```

## LDIF exemple

```
dn : uid=rbidochon,ou=people,dc=bidon,dc=fr
loginShell : /bin/bash
objectClass : top
objectClass : dcObject
objectClass : person
objectClass : posixAccount
objectClass : shadowAccount
dc : bidon
cn : Bidochon Robert
uid : rbidochon
uidNumber : 1001
homeDirectory : /home/rbidochon
sn : Bidochon
gidNumber : 1000
```

## Configuration Clients

```
/etc/openldap/ldap.conf
BASE dc=bidon, dc=fr
HOST ldap.example.com ldap-master.example.com
# SSL/TSL configuration. With CA-signed certs,
#TLS_REQCERT should be
# "demand", with the CA certificate accessible
TLS_CACERT /etc/ssl/cacert.pem
TLS_CACERTDIR /etc/ssl/openldap
# TLS_REQCERT ([demand],never,allow,try)
TLS_REQCERT allow
```

## Modes d'authentification

- ▶ Locale
  - ▶ passwd / shadow
  - ▶ tdbsam
- ▶ Distante
  - ▶ nis
  - ▶ samba / passwd
  - ▶ ldap
  - ▶ samba / ldap

## PAM

- ▶ Plugable Authentication Modules
- ▶ Utilisés par de nombreuses applications
- ▶ Chaque application définit une pile
- ▶ Modules génériques
  - ▶ dont /etc/pam.d/system-auth
  - ▶ et pam\_ldap

## principes de PAM

- ▶ Type de module
  - ▶ auth : authentifie l'utilisateur
  - ▶ account : restriction du compte
  - ▶ password : Gestion des mots de passe
  - ▶ session : Tout ce qui concerne l'ouverture d'une session, avant et après
- ▶ Contrôle
  - ▶ required : Doit réussir, on continue
  - ▶ requisite : Doit réussir, on ne continue pas
  - ▶ optimal : Ignoré
  - ▶ sufficient : Si le test est correct, on obtient immédiatement une acceptation
- ▶ Module et options éventuelles

## login

auth	required	pam_securetty.so
auth	required	pam_nologin.so
auth	include	system-auth
account	include	system-auth
password	include	system-auth
session	optional	pam_console.so
session	include	system-auth

## system\_auth

auth	required	pam_env.so
auth	sufficient	pam_unix.so likeauth nullok
auth	required	pam_deny.so
account	sufficient	pam_unix.so
account	required	pam_deny.so
password	required	pam_cracklib.so retry=3 minlen=2 dcredit=0 ucredit=0
password	sufficient	pam_unix.so nullok use_authtok md5 shadow
password	required	pam_deny.so
session	optional	pam_keyinit.so revoke
session	required	pam_limits.so
session	required	pam_unix.so

## Configuration de l'authentification

- ▶ A la main, modifier
  - ▶ /etc/pam.d/system\_auth
  - ▶ /etc/openldap/ldap.conf
  - ▶ /etc/nsswitch.conf
- ▶ Au clickodrôme
  - ▶ drakauth chez Mandriva
  - ▶ authconfig chez Fedora