

<http://www-adele.imag.fr/users/Didier.Donsez/cours>

# Annuaire (Directory)

---

**Didier Donsez**

*Université Joseph Fourier - Grenoble 1*

*PolyTech'Grenoble - LIG/ADELE*

`Didier.Donsez@imag.fr`

`Didier.Donsez@ieee.fr`

# Sommaire

---

- Concept de Nommage
- Concept d 'Annuaire
- LDAP
- API
  - ASDI
  - JNDI

# Concept de Nommage (i)

- Nommage (Naming)
  - Association d'un nom à un objet
    - objet : fichier, usager, machine, service distant ...
    - Liaison (binding)
      - terme pour désigner une association
  - Exemples:
    - DNS
      - www.sun.com vers 192.9.48.5
    - FileSystem DOS
      - c:\bin\autoexec.bat vers un fichier
    - CORBA, RMI, ...

# Concept de Nommage (ii)

- Convention du nommage
  - règles de représentation des noms
    - DNS : identifiants séparés par des . (dot)
    - FS Unix : identifiants séparés par des /
    - FS Dos : nom d 'unité :\ puis identifiants séparés par des \
    - LDAP : cn=Rosanna Lee, o=Sun, c=US
- Contexte
  - sous-ensemble de liaison
    - sun.com; /usr; o=Sun, c=US sont des contextes
- Naming System
  - ensemble de contextes connectés utilisant la même convention de nommage
- NameSpace
  - ensemble de noms utilisés par un Naming Service

# Concept de Nommage (iii)

## Exemple de NameSpace

---

- DNS Related RFCs
  - <http://www.dns.net/dnsrd/rfc>
- RFC 1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
  - <http://www.ietf.org/rfc/rfc1035.txt>
- Uniform Resource Name
  - <http://www.ietf.org/html.charters/urn-charter.html>
- URN assigned name-spaces
  - <http://www.iana.org/assignments/urn-name-spaces>
- RFC 2141 URN Syntax
  - <http://www.ietf.org/rfc/rfc2141.txt>
- Naming and Addressing: URIs, URLs, ...
  - <http://www.w3.org/Addressing>
- International Domain names
  - <http://www.i-dns.net/technology/howidns/howidns.html>
- AMC-ACE-Z draft
  - <http://www.ietf.org/internet-drafts/draft-ietf-idn-amc-ace-z-01.txt>
- Internationalized Domain Name Conversion Tool
  - <http://mct.verisign-grs.com>
- Preparation of Internationalized Host Names
  - <http://www.i-d-n.net/draft/draft-ietf-idn-nameprep-03.txt>

# Concept d 'Annuaire (i)

- Annuaire (Directory)
  - extension du nommage
    - les objets ont aussi des attributs
      - une imprimante peut avoir des attributs vitesse, resolution, couleur
      - une personne peut avoir un attribut bureau, email
  - organisation généralement hiérarchique
- Exemple
  - Systèmes centralisés ou hiérarchisés
    - Novell NDS, Solaris NIS, ISO X500, OMG CosNaming, LDAP, ...
  - Systèmes spontanés et P2P
    - JINI, UPnP, ...
    - SLP, DNS-SD, ...
    - JXTA PDP (Peer Discovery Protocol), ...

## Concept d 'Annuaire (ii)

- Recherche (query) dans l 'Annuaire
  - expression logique
  - sur le nom
    - sur une partie du nom
  - sur la valeur des attributs
    - search filter
      - (appelé aussi reverse lookup ou content-based searching)

# Exemple d 'Annuaire : LDAP Lightweight Directory Access Protocol

---

- Proposé par l 'IETF en 1995
  - LDAP v3 (RFC 2251)
    - <http://www.ietf.org/rfc/rfc2251.txt>
- Simplification de ISO X500
  - même convention de nommage
  - mais basé sur TCP/IP (plutôt que les couches ISO)
  - Première implantation de l'Univ. Michigan
  - Produits commerciaux : IBM, Microsoft, Netscape, Oracle, Sun, ...
  - Voir <http://www.innosoft.com>



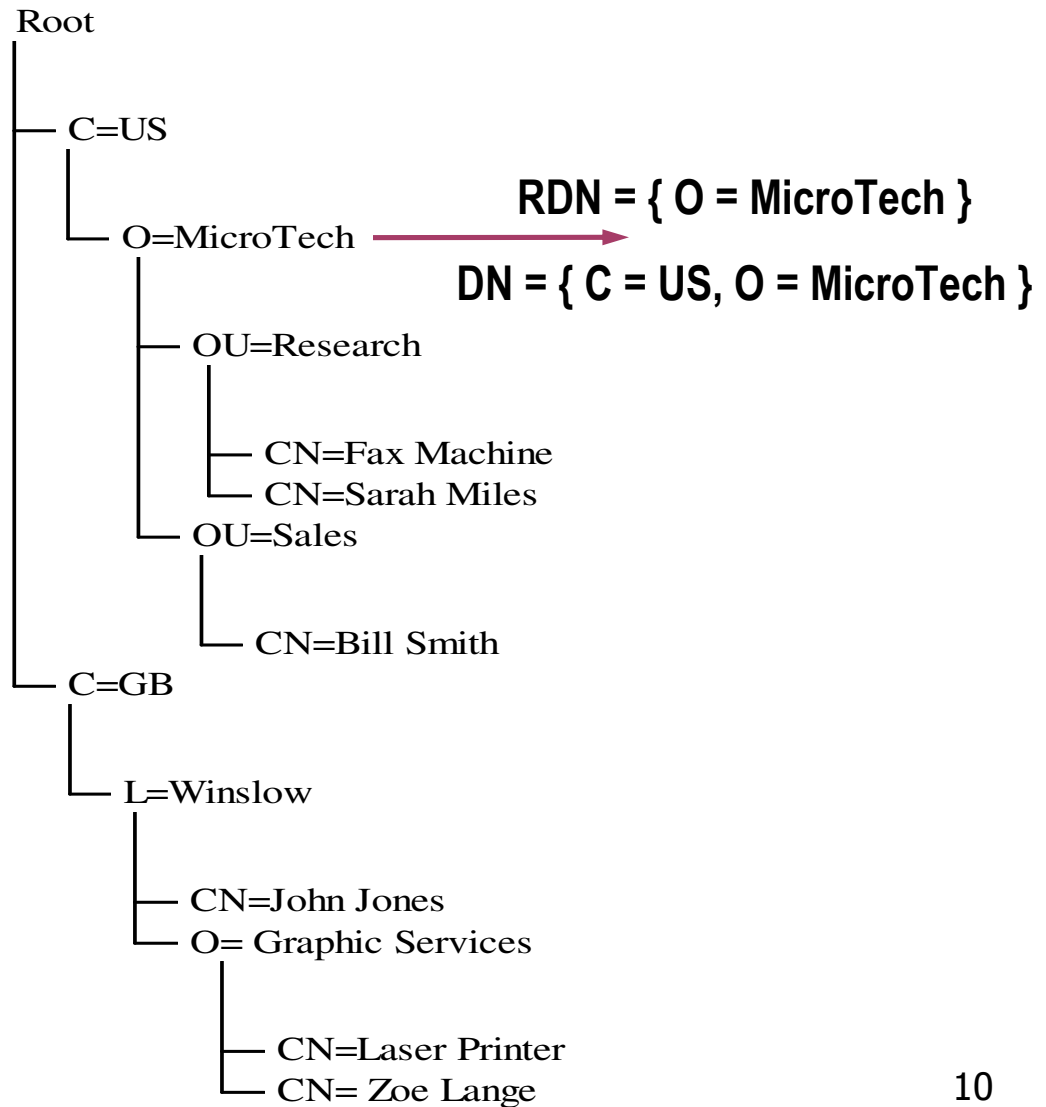
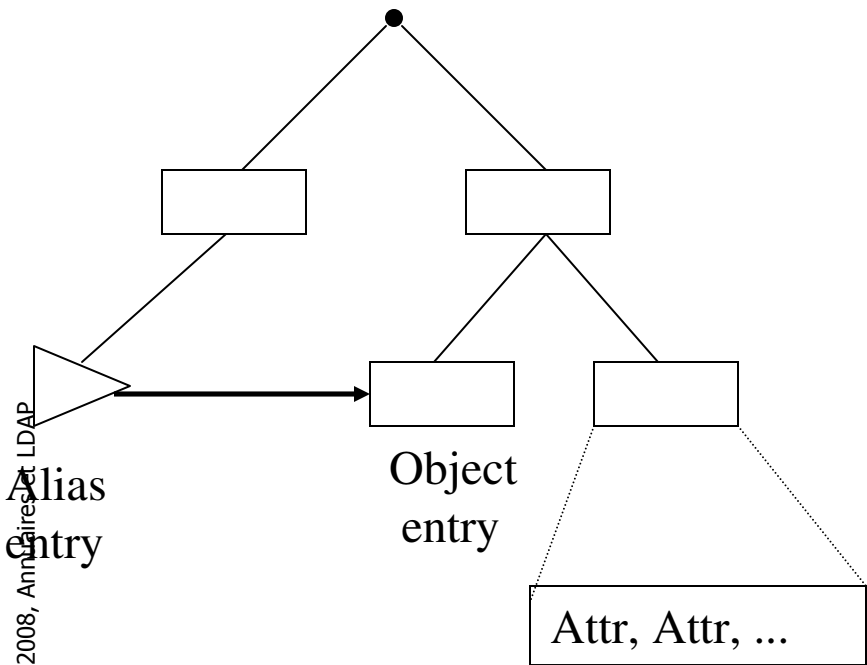
# Modèle de données LDAP

---

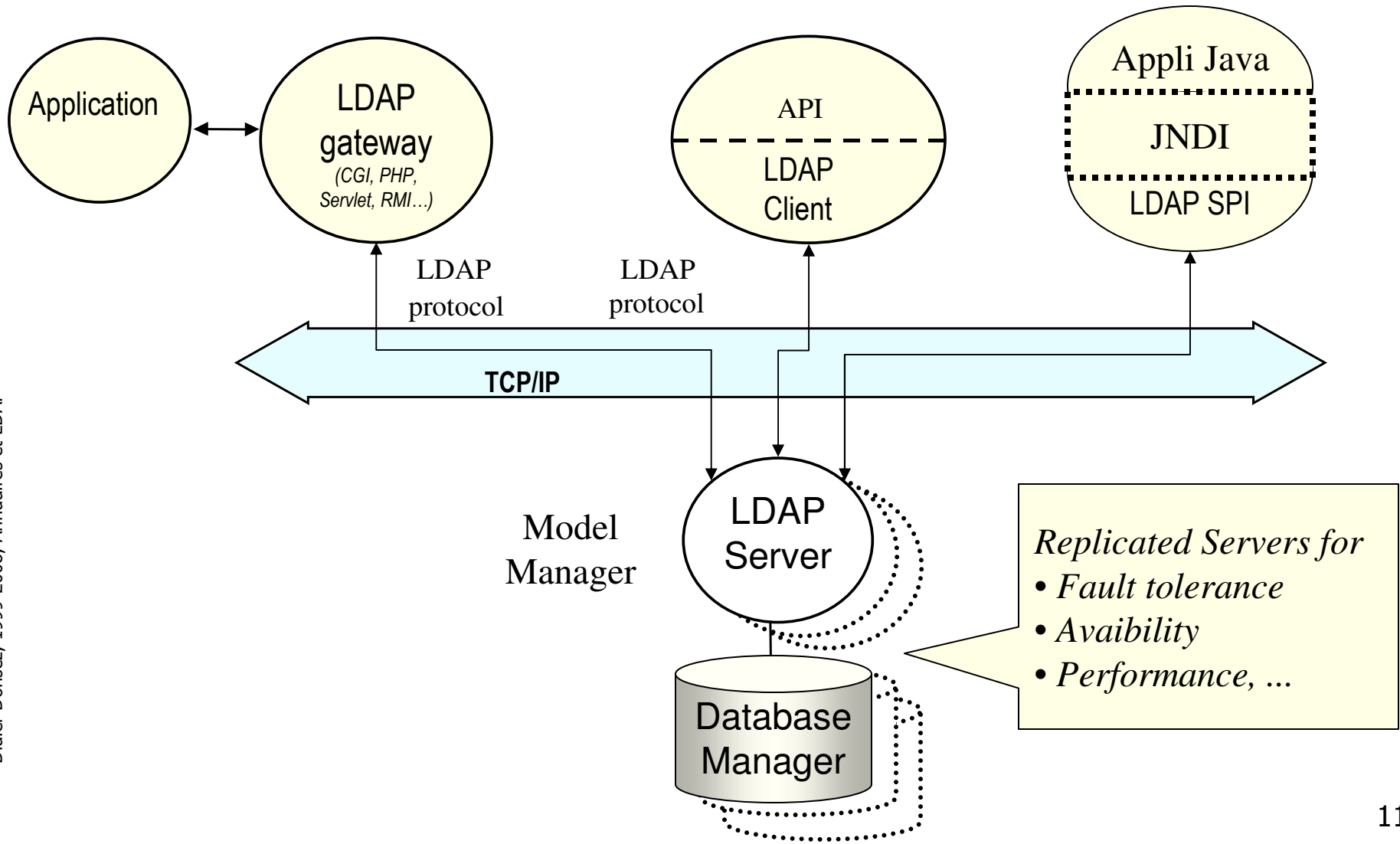
- Directory Information Tree (DIT)
  - arbre d'entrées (entries)
  - chaque entrée est composé d'un ou de plusieurs attributs typés et multivalués
    - String, données binaires comme JPEG...
- Espace de nommage hiérarchique
  - Chaque entrée du DIT est nommée
    - Relative Distinguished Name (RDN)
    - Distinguished Name (DN)

# Modèle de données LDAP

Didier Donsez, 1999-2008, Annuaire LDAP



# Architecture LDAP



# LDIF (*LDAP Data Interchange Format*)

## *RFC 2849*

---

- Format texte de représentation des données contenues dans l'annuaire
  - Opérations (ajout, suppression, modification) sur les données de l'annuaire.
- Exemple
  - dn: uid=donsezd,ou=users,ou=system
  - cn: Didier Donsez
  - sn: Donsez
  - givenname: Didier
  - objectclass: top
  - objectclass: person
  - objectclass: organizationalPerson
  - objectclass: inetOrgPerson
  - ou: Teacher
  - ou: People
  - l: Grenoble
  - uid: donsezd
  - mail: donsezd@grenoble.org
  - telephonenumber: +33 476 12 34 56
  - facsimiletelephonenumber: +33 476 12 34 00
  - roomnumber: 211
  - userpassword: catarinabellatchitchi

# DSML

## Directory Services Markup Language

---

- Représentation XML (DTD) des données d'annuaire <http://www.dsml.org>

# DSML

## Directory Services Markup Language

dn: uid=scarter, ou=People, o=mcom.com  
 cn: Sam Carter  
 sn: Carter  
 givenname: Sam  
 objectclass: top  
 ou: Accounting  
 l: Sunnyvale  
 uid: scarter  
 mail: scarter@mcom.com  
 telephonenumber: +1 408 555 4798

```
<dsml:dsml xmlns:dsml="http://www.dsml.org/DSML">
  <dsml:directory-entries>
    <dsml:entry dn="uid=scarter, ou=People, o=mcom.com">
      <dsml:attr name="cn"><dsml:value>Sam Carter</dsml:value></dsml:attr>
      <dsml:attr name="sn"><dsml:value>Carter</dsml:value></dsml:attr>
      <dsml:attr name="givenname"><dsml:value>Sam</dsml:value></dsml:attr>
      <dsml:objectclass>top</dsml:objectclass>
      <dsml:objectclass>person</dsml:objectclass>
      <dsml:objectclass>organizationalPerson</dsml:objectclass>
      <dsml:objectclass>inetOrgPerson</dsml:objectclass>
      <dsml:attr name="ou">
        <dsml:value>Accounting</dsml:value>
        <dsml:value>People</dsml:value>
      </dsml:attr>
      <dsml:attr name="l"><dsml:value>Sunnyvale</dsml:value></dsml:attr>
      <dsml:attr name="uid"><dsml:value>scarter</dsml:value></dsml:attr>
      <dsml:attr name="mail"><dsml:value>scarter@mcom.com</dsml:value>
      </dsml:attr>
      <dsml:attr name="telephonenumber"> <dsml:value>+1 408 555 4798</dsml:value>
      </dsml:attr>
    </dsml:entry>
  </dsml:directory-entries>
</dsml:dsml>
```

# Syntaxe LDAP des filtres (RFC1960)

A String Representation of LDAP Search Filters, RFC 1960, UMich, 1996,  
<http://www.ietf.org/rfc/rfc1960.txt>

```

filter ::= '(' filter-comp ')'
filter-comp ::= and | or | not | item
and ::= '&' filter-list
or ::= '|' filter-list
not ::= '!' filter
filter-list ::= filter | filter filter-list
item ::= simple | present | substring
simple ::= attr filter-type value
filter-type ::= equal | approx | greater | less
equal ::= '='
approx ::= '~='
greater ::= '>='
less ::= '<='
present ::= attr '=*'
substring ::= attr '=' initial any final
initial ::= () | value
any ::= '*' star-value
star-value ::= () | value '* star-value
final ::= () | value

```

# Acteurs et Produits LDAP

---

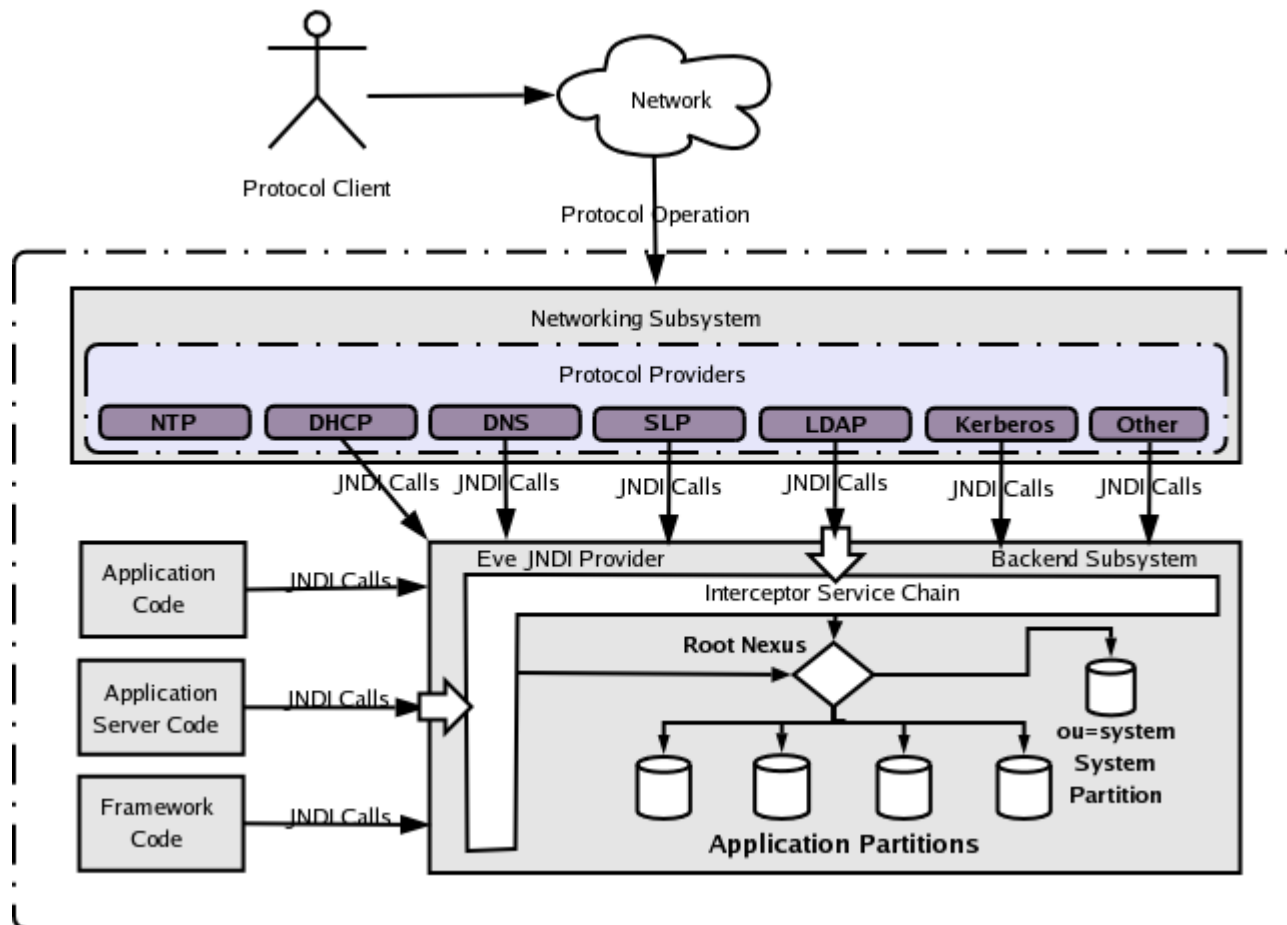
- Acteurs et Produits
  - Netscape, Microsoft, IBM, Sun, Oracle ...
- Serveur OpenSource
  - Serveur LDAP de l'Université du Michigan <http://www.umich.edu/~dirsvcs/ldap/ldap.html>
  - Serveur LDAP en OpenSource (<http://www.openldap.org>) écrit en C
  - Apache Directory Server (Java) <http://directory.apache.org/>
- Clients OpenSource
  - JXplorer <http://pegacat.com/jxplorer/>
  - Apache Directory Studio
  - <http://www.iit.edu/~gawojar/ldap/index.html>
- Autres Sites
  - An LDAP Roadmap FAQ
    - <http://www.kingsmountain.com/ldapRoadmap.shtml>
  - Introduction to slapd and slurpd
    - <http://www.umich.edu/~dirsvcs/ldap/doc/guides/slapd/1.html#RTFToC1>
  - Intranet Design: RFC-1777 (LDAP)
    - <http://idm.internet.com/RFC/rfc-1777.html>
  - Tips for LDAP Users
    - <http://java.sun.com/products/jndi/tutorial/ldap/index.html>
  - Searching the Directory
    - <http://curiac.acomp.usf.edu/db/ldap/sdk/search.htm#2839729>



# Apache Directory Server

<http://directory.apache.org/>

- LDAP server (Java)



# JXplorer

<http://pegacat.com/jxplorer/>

The screenshot shows the JXplorer web interface. The search query is `cn=*donsez*`. The search results are displayed in a table with the following columns: attribute type and value.

attribute type	value
<b>cn</b>	Didier Donsez
<b>objectclass</b>	inetOrgPerson
<b>objectclass</b>	organizationalPerson
<b>objectclass</b>	person
<b>objectclass</b>	top
<b>sn</b>	Donsez
facsimiletelephonenumber	+33 476 12 34 00
givenname	Didier
l	Grenoble
mail	donsezd@grenoble.org
ou	People
ou	Teacher
roomnumber	211
telephonenumber	+33 476 12 34 56
uid	<b>donsezd</b>
userpassword	[B@b80017
audio	
businessCategory	
carLicense	
departmentNumber	
description	
destinationIndicator	
displayName	
employeeNumber	

Buttons at the bottom: Soumettre, Ré-initialiser, Changer une Classe, Propriétés.

Connected To 'Disconnected'

# Apache Directory Studio

The screenshot displays the Apache Directory Studio interface. The main window is titled "LDAP Browser" and shows a tree view of the LDAP directory structure. The selected entry is "cn=Didier Donsez" under "ou=users, ou=system".

The "Entry Editor" pane shows the details of the selected entry:

Attribute Description	Value
<i>objectClass</i>	<i>groupOfUniqueNames (structural)</i>
<i>objectClass</i>	<i>top (abstract)</i>
<i>cn</i>	Administrators
<i>uniqueMember</i>	0.9.2342.19200300.100.1.1=admin,2.5.4.11=system

The "Modification Logs" pane shows the following log entry:

```

# !:CONNECTION ldap://localhost:10389
# !:DATE 2008-04-25T00:00:47.640
# !:ERROR [LDAP: error code 65 - failed to modify entry cn=Adminis
dn : cn=Administrators,ou=groups,ou=system
changeType : modify
  
```

The "Progress" pane shows the status of the operation:

```

Create Value (Finished)
Error While...ing value
  
```

The "Connections" pane shows the current connection to "ApacheDS Example".

# APIs

---

ADSI

JNDI

# ADSI

## Active Directory Server Interface

---

- API Plateforme Windows
  - Multi-langage (C, C++, VB, C#, ASP ...)  
via COM, .NET
- Indépendante du type d'annuaire
  - 2 connecteurs livrés en standard
    - ADS (Active Directory), Win2000
      - LDAPv3
    - Bases de Registre Windows NT

# JNDI

## Java Naming and Directory Interface

---

- API Java
- Indépendante du type d'annuaire
  - 3 SPI (Service Provider) livrés en standard
    - Lightweight Directory Access Protocol (LDAP)
    - CORBA services (COS) naming service
    - Java Remote Method Invocation (RMI) Registry
- Détails dans
  - <http://www-adele.imag.fr/~donsez/cours/jndi.pdf>

# Bibliographie

---

- Voir cours sur JNDI, JINI, SLP, DNS-SD, UPnP
  - <http://www-adele.imag.fr/~donsez/cours>
- Voir chapitre 6 et Appendix B de David N. Blank-Edelman, Perl for System Administration, O'Reilly, First edition, July 2000, ISBN 1-56592-609-9

# Bibliographie JNDI

---

- Spécifications et Tutorial JNDI
  - <http://java.sun.com/products/jndi>
  - <http://java.sun.com/products/jndi/tutorial/TOC.html>
- Rosanna Lee, Scott Seligman , "JNDI API Tutorial and Reference: Building Directory-Enabled Java Applications (The Java Series)", (May 30, 2000) , Ed Addison-Wesley Pub Co; ISBN: 0201705028



# Bibliographie LDAP

---

- David Flanagan, Jim Farley, William Crawford & Kris Magnusson, « Java Enterprise in a Nutshell, A Desktop Quick Reference », Edition Oreilly, 1st Edition September 1999, ISBN 1-56592-483-5
  - Chapter 6
- John Rhoton, «Programmer's Guide to Internet Mail : Sntp, Pop, Imap, and Ldap», October 1999, Digital Press; ISBN: 1555582125
- Mark Wilcox , « Implementing LDAP », March 1999, Wrox Press Inc; ISBN: 1861002211
- Andrew Patzer , "Programmation Java côté serveur : Servlets, JSP et EJB", Ed Eyrolles-Wrox, 2000, ISBN 1-861002-77-7 (sources des exemples sur [www.wroxfrance.com](http://www.wroxfrance.com))
  - chapitres 21 et 22
- Marcel Rizcallah, "Construire un annuaire d'entreprise avec LDAP", Ed Eyrolles, 2000, ISBN, 2-212-09154-0
  - Des études de cas
- ROB WELTMAN and TONY DAHBURA, LDAP Programming with Java, ADDISON-WESLEY, 2000, ISBN 0-201-65758-9
- D'autres livres sur <http://www.ldapzone.com/books.html>

# Bibliographie ADSI

---

- Melissa Craft, « Active Directory pour Windows 2000 Server », Edition Eyrolles, 2000, ISBN 2-212-09167-2
- Active Directory
  - <http://www.microsoft.com/windows2000/library/technologies/activedirectory>
- ADSI
  - <http://www.microsoft.com/windows2000/library/howitworks/adsilinks.asp#heading2>