LDAP

RES, Lecture 10

Olivier Liechti

heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Agenda

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- Introduction
  - LDAP: history, objectives and overview
  - Tools: servers, browsers, APIs and libraries
- LDAP: the data model
  - Hierarchical organization, naming
  - Core concepts: DIT, entry, attribute, class, schema
- LDAP: the protocol
  - Principles, operations and the LDIF data format
- LDAP: the infrastructure
  - Distribution and replication
  - Commands, filters, etc.
- LDAP with Java: Java Naming & Directory Interface (JNDI)
  - Authentication, query, data manipulation

Références

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- LDAP for Rocket Scientists (ZYTRAX, Inc.)
  - http://www.zytrax.com/books/ldap/
- Redbook IBM
  - http://www.redbooks.ibm.com/abstracts/sg244986.html
- Tutorials and presentations
  - http://quark.humbug.org.au/publications/ldap/
  - http://www.it-sudparis.eu/s2ia/user/procacci/ldap/
  - http://www.hawaii.edu/its/brownbags-trainings/ldap/
- RFCs
  - http://www.mozilla.org/directory/standards.html
- OpenDJ
  - http://forgerock.com/products/open-identity-stack/opendj/
  - http://opendj.forgerock.org/
- LDAP Clients
  - http://directory.apache.org/studio/
  - http://www-unix.mcs.anl.gov/~gawor/ldap/

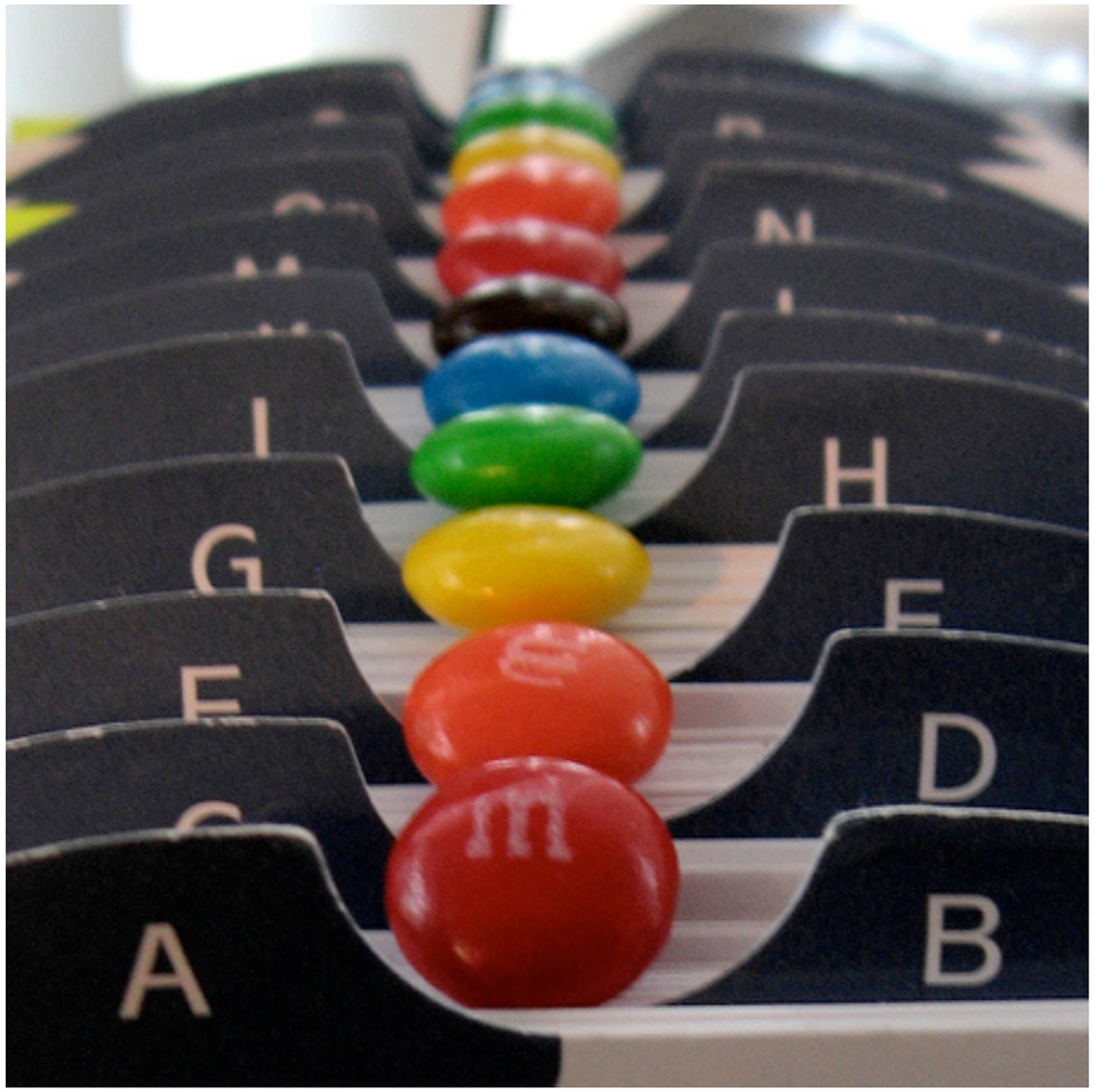
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Introduction

LDAP: a Directory Service

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

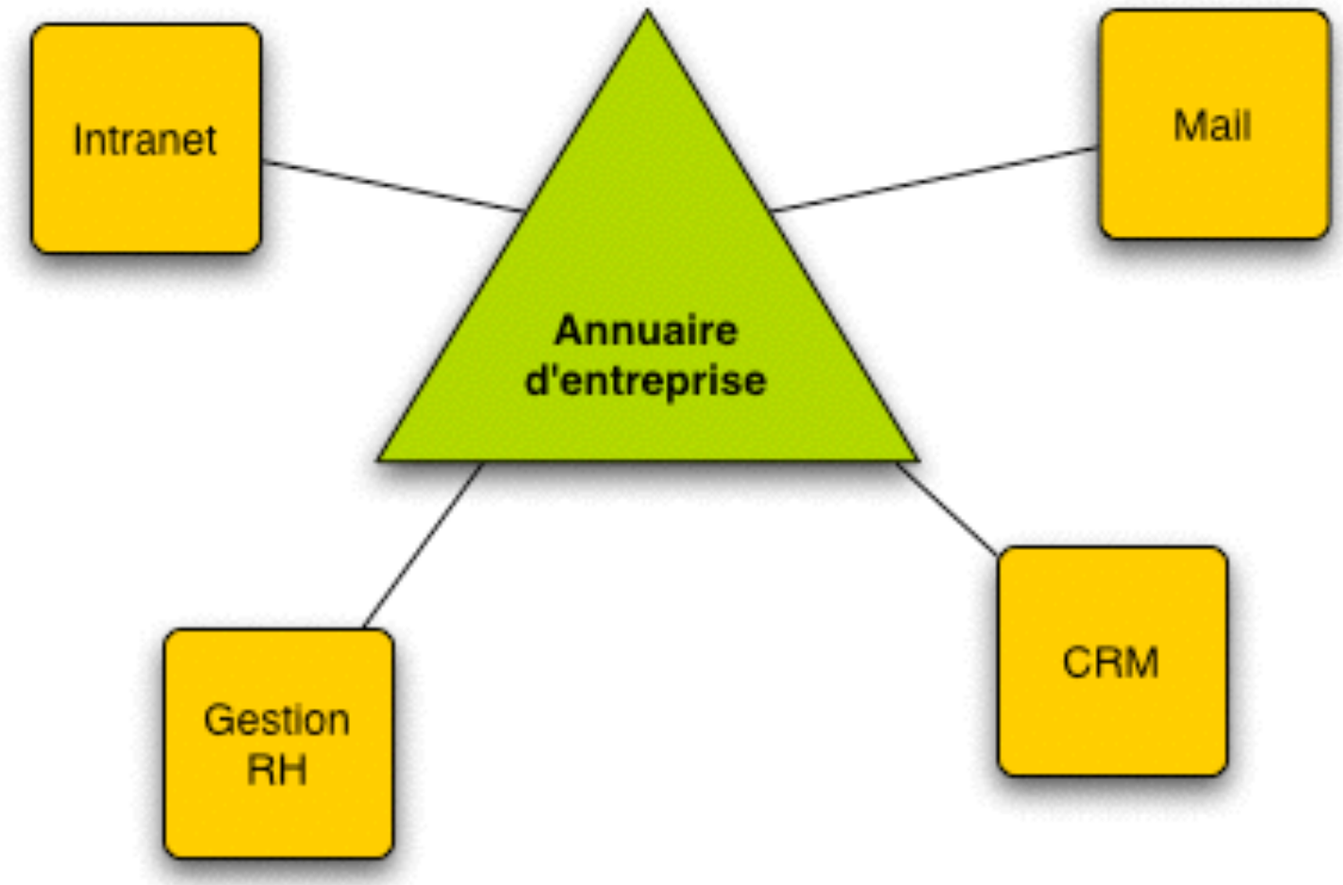
- Late 70's
  - Standardisation of directory service by the UIT (X.500).
  - Related to the growing adoption of electronic messaging protocols.
  - Directory Access Protocol (DAP).
- Late 90's
  - Lightweight (simplified) version of the protocol, based on the TCP/IP stack.
  - University of Michigan, IETF
- Key functions
  - Fast information lookup
  - Authentication



http://flickr.com/photos/gehmflor/375334958/sizes/m/#cc_license

LDAP: Sharing Data in the Enterprise

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

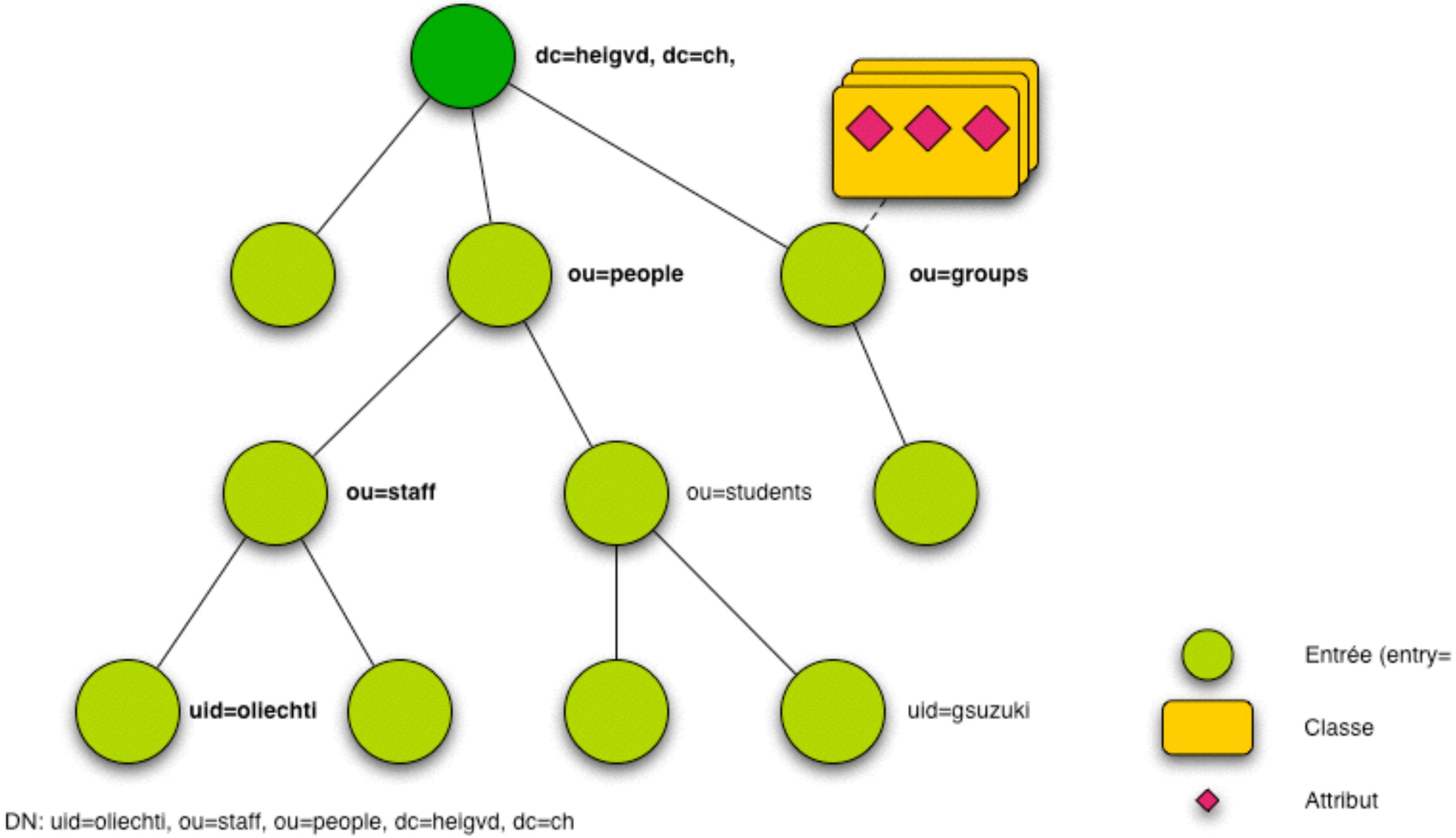


heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

LDAP: the Data Model

LDAP: the Data Model

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

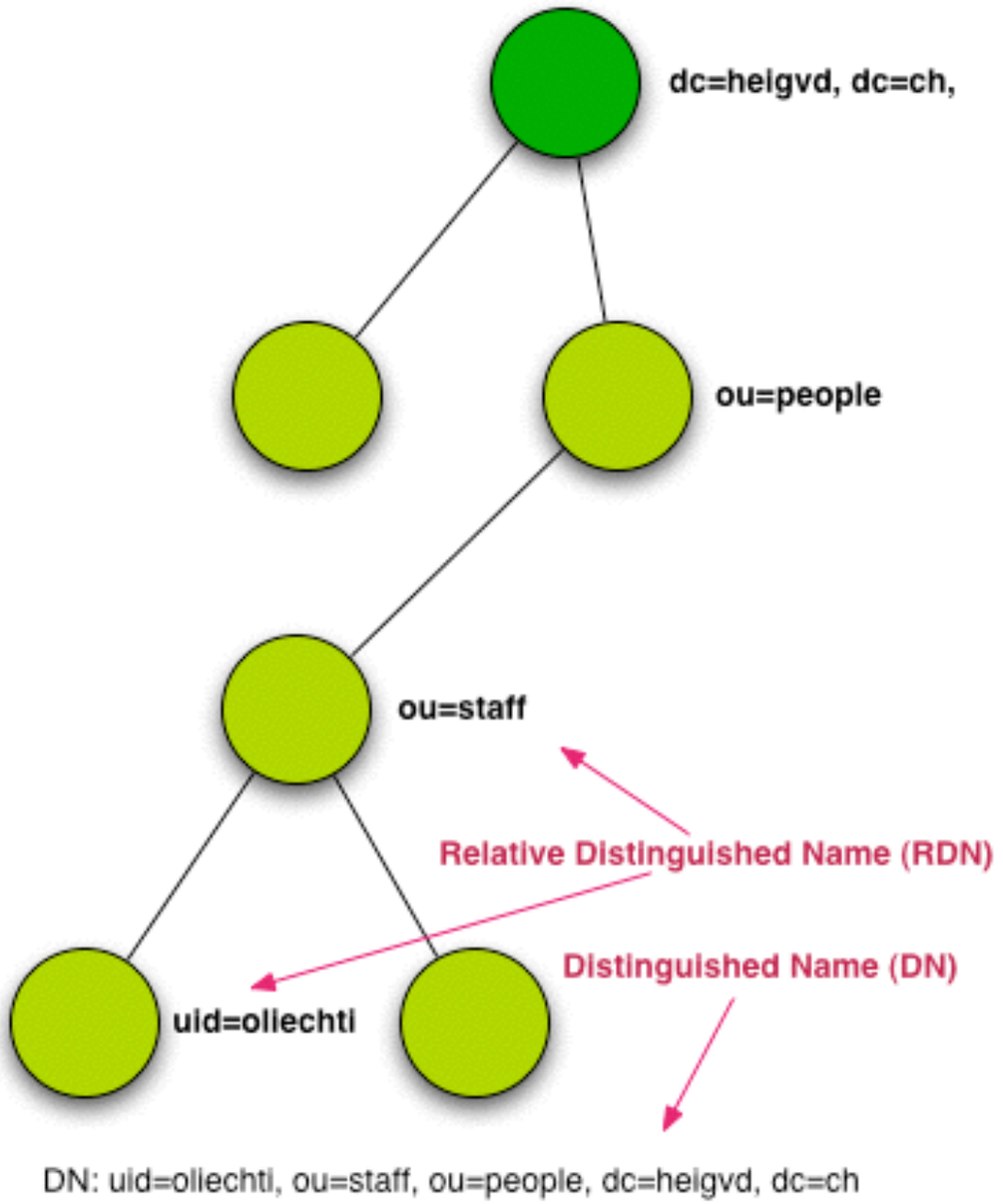


DN: uid=ollechti, ou=staff, ou=people, dc=heigvd, dc=ch

The Directory Information Tree (DIT)

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

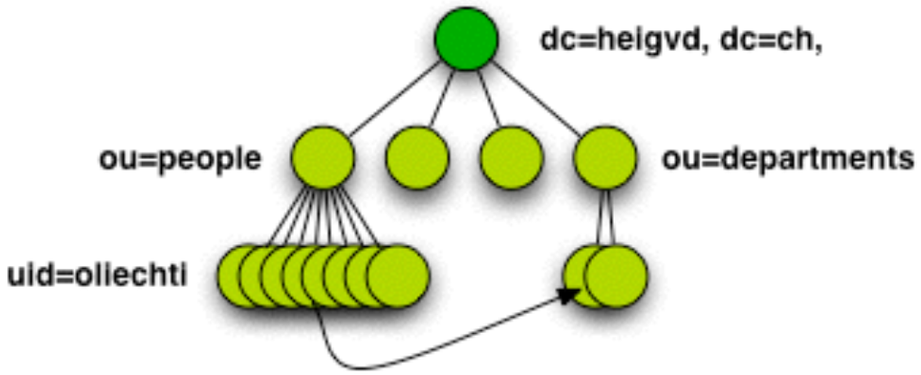
- Data is organized hierarchically, in a tree:
  - The “root” is also called “suffix” or “base”.
  - Each node in the tree is an LDAP “entry”.
  - The intermediate nodes are “container” nodes.
- LDAP entries are named:
  - The **Distinguished Name (DN)** is used to identify and locate an entry in the tree.
  - The DN provides the path from the root to the entry.
  - The **Relative Distinguished Name** (RDN) uniquely identifies an entry among siblings (nodes that are children of the same node)

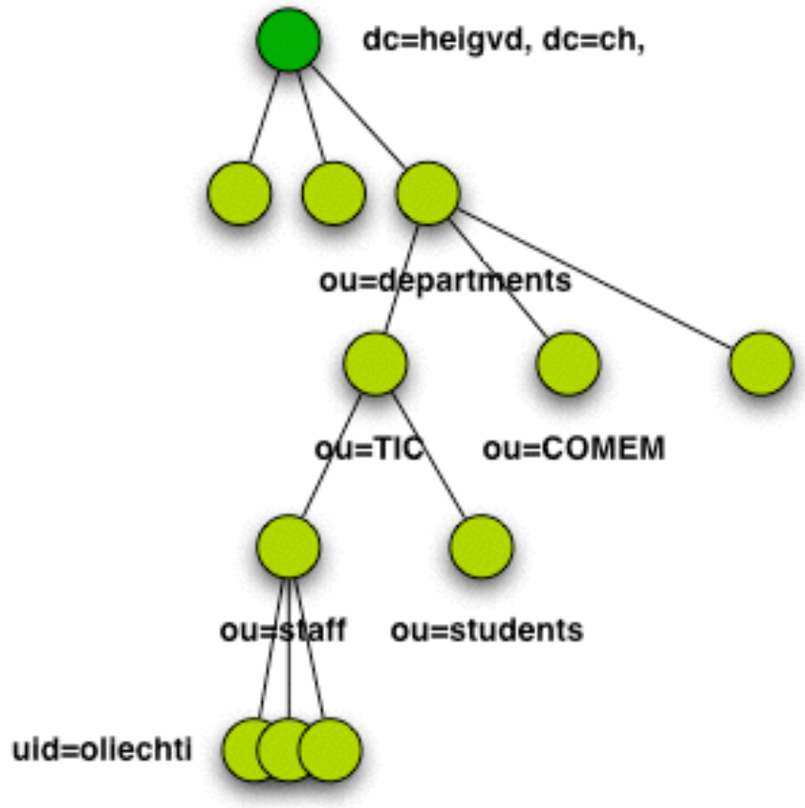


How to Structure the DIT

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- What can we store in a directory?
  - People (e.g. employees, customers, partners, etc.)
  - Equipment (e.g. printers, file servers, etc.)
  - Software services (e.g. web services, etc.)
  - Configuration parameters (e.g. of the server itself)
- When storing people, how do we structure the DIT?
  - Do we reflect the org chart, by department?
  - Do we structure by country?
- Recommendation
  - A flat structure is much move convenient, flexible and evolvable than a deep one.





http://docs.sun.com/app/docs/doc/820-2488/fpqzx?a=view
http://docs.sun.com/source/816-6679-10/dit.htm#1015250

The Notion of Entry

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- An LDAP "**entry**" LDAP is an object stored in the directory.
- It is a **node** in the DIT.
- An entry is uniquely identified by its **Distinguished Name** (DN)
- An entry is locally (among siblings) identified by its **Relative Distinguished Name** (RDN).
- The state of an entry is defined by a list of **attributes and attribute values**.
- The **structure** of an entry (i.e. the list of attributes) is defined in one or more **classes**. The multi-valued **ObjectClass attribute** of an entry is used to specify which classes it is an instance of.
- Examples of entries:
  - A person, a group, a department, a printer, an online service, a configuration parameter, etc.

The Notion of Object Class

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- The notion of LDAP object class is similar to the notion of class in an **object-oriented programming language**.
- A class is defined by a list of **attributes**
  - some of which are **mandatory**
  - some of which are **optional**
  - some of which are **multivalued**
- A class can **extend** another one (inheritance)
- The **RFC 2252** (LDAPv3 Attribute Syntax Definitions) provides the **syntax** to define classes.
- Many classes have been standardized and specified in RFCs, for example:
  - `inetOrgPerson, OrganizatinalPerson, Person`
  - `organizationalUnit`
  - `groupOfUniqueNames`

Syntax to Define a Class

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

```
ObjectClassDescription = "(" whsp
     numericoid whsp       ; ObjectClass identifier
     [ "NAME" qdescrs ]
     [ "DESC" qdstring ]
     [ "OBSOLETE" whsp ]
     [ "SUP" oids ]        ; Superior ObjectClasses
     [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
                           ; default structural
     [ "MUST" oids ]       ; AttributeTypes
     [ "MAY" oids ]        ; AttributeTypes
whsp ")"
```

Example: inetOrgPerson

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

```
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
  SUP organizationalPerson STRUCTURAL MAY ( audio $ businessCategory $
  carLicense $ departmentNumber $ displayName $ employeeNumber $ employeeType $
  givenName $ homePhone $ homePostalAddress $ initials $ jpegPhoto $
  labeledURI $ mail $ manager $ mobile $ o $ pager $ photo $ roomNumber $
  secretary $ uid $ userCertificate $ x500UniqueIdentifier $
  preferredLanguage $ userSMIMECertificate $ userPKCS12 ) X-ORIGIN 'RFC 2798' )
```

The Notion of Attribute

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- **Attributes** define that state of an entry.
- Attributes are **referenced in classes**.
- Attributes have a **type** (String, Binary, etc.).
- Attributes can be **multivalued**.

```
attributeTypes: ( 0.9.2342.19200300.100.1.41
  NAME ( 'mobile' 'mobileTelephoneNumber' ) EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.50
  X-ORIGIN 'RFC 4524' )
```

The Notion of Schema

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- When deploying an LDAP directory service, one has to specify the **schema** that defines the rules governing the structure of managed data:
  - What are the classes that are supported and that can be used to create entries?
  - What are the attributes that are supported and used to define classes?
  - etc.
- There are **standard schemas** and when you install an LDAP server, a default one is available to you. Very often, you do not need more and can create entries based on the standard classes and attributes (InetOrgPerson, OrganizationalUnit, etc.).
- If you have special needs, then you can **extend the schema** with:
  - custom classes (e.g. heigvdPerson)
  - custom attributes (e.g. gapsIdNumber)
- The procedure for extending the schema depends on the actual LDAP server (OpenDJ, OpenLDAP, Active Directory, etc.)

Object IDentifier (OID)

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- An OID is an **alphanumeric value** that **uniquely identifies** a particular element in a directory schema, such as a **class** or an **attribute**.
- There are **different ways to obtain an OID** for a schema element:
  - If the schema and directory data is used only for internal purposes, then you can freely define the OID value (as an analogy, think of a private IP network where you can decide for the addressing scheme yourself).
  - If the data is shared with external organizations, then a globally unique OID must be obtained (think of public IP addresses).
- OIDs are managed by the IANA; the procedure to obtain an OID is easy and simple.

https://www.opends.org/wiki/page/HowToExtendTheLDAPSchema#section-HowToExtendTheLDAPSchema-WorkingWithObjectIdentifiersOIDs

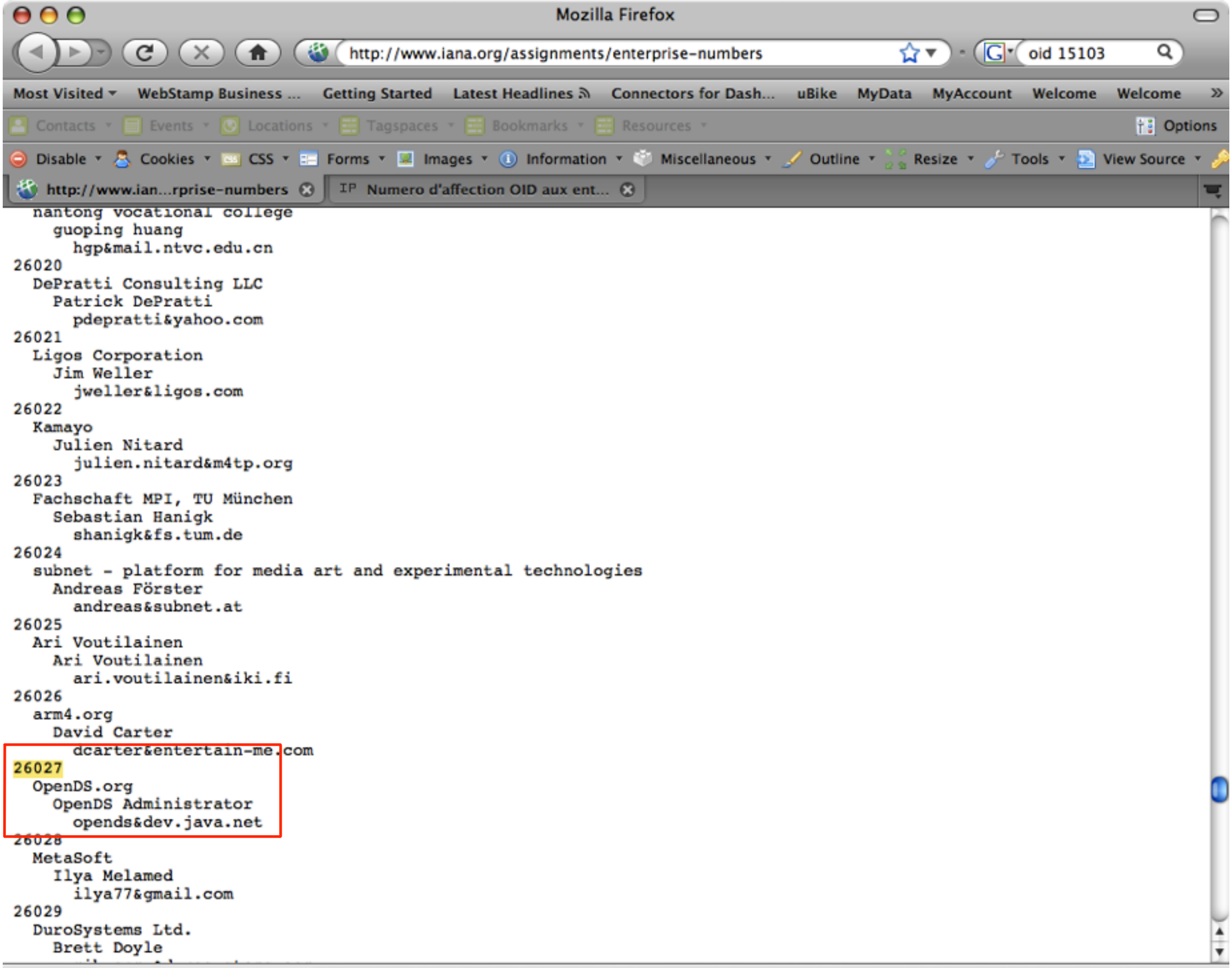
LDAP object classes and attributes require a base object identifier (OID) that must be unique within your organization to avoid naming conflicts in the directory. If you plan to use your directory internally within your organization, use the OIDs provided in the OpenDS directory server. If you plan to export your schema or publicly expose your schema in any way, you should consider entering a request for a unique OID for your organization (see Obtaining a Base OID).

After you have obtained a base OID, you can add branches to it for your organization's object classes and attributes. For example, the OpenDS project uses an assigned base OID of `1.3.6.1.4.1.26027`. For each component type, OpenDS provides unique branch numbers to the base OID for each schema component.

> **Note:** OpenDS provides a comprehensive set of OIDs that should be sufficient for most applications. You can also request OIDs for addition to the OpenDS repository.

For example, OpenDS uses the following base OIDs for each schema component:

OID Value	Type
1.3.6.1.4.1.26027.1.1	Attribute
1.3.6.1.4.1.26027.1.2	Object classes
1.3.6.1.4.1.26027.1.3	Attribute syntaxes
1.3.6.1.4.1.26027.1.4	Matching rules
1.3.6.1.4.1.26027.1.5	Controls
1.3.6.1.4.1.26027.1.6	Extended operations
1.3.6.1.4.1.26027.1.9	General use (Currently, no OIDs are assigned for OpenDS.)
1.3.6.1.4.1.26027.1.999	Experimental use


Mozilla Firefox
http://www.iana.org/assignments/enterprise-numbers
oid 15103
Most Visited
WebStamp Business ...
Getting Started
Latest Headlines
Connectors for Dash...
uBike
MyData
MyAccount
Welcome
Welcome
Contacts
Events
Locations
Tagspaces
Bookmarks
Resources
Options
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
http://www.ian...rprise-numbers
IP Numero d'affection OID aux ent...
nantong vocational college
guoping huang
hgp&mail.ntvc.edu.cn
26020
DePratti Consulting LLC
Patrick DePratti
pdepratti&yahoo.com
26021
Ligos Corporation
Jim Weller
jweller&ligos.com
26022
Kamayo
Julien Nitard
julien.nitard&m4tp.org
26023
Fachschaft MPI, TU München
Sebastian Hanigk
shanigk&fs.tum.de
26024
subnet - platform for media art and experimental technologies
Andreas Förster
andreas&subnet.at
26025
Ari Voutilainen
Ari Voutilainen
ari.voutilainen&iki.fi
26026
arm4.org
David Carter
dcarter&entertain-me.com
26027
OpenDS.org
OpenDS Administrator
opends&dev.java.net
26028
MetaSoft
Ilya Melamed
ilya77&gmail.com
26029
DuroSystems Ltd.
Brett Doyle
Find:
26027
Next
Previous
Highlight all
Match case
Done

```
PRIVATE ENTERPRISE NUMBERS

(last updated 2008-07-11)

SMI Network Management Private Enterprise Codes:

Prefix: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

This file is http://www.iana.org/assignments/enterprise-numbers

Decimal
| Organization
| | Contact
| | | Email
| | | |
0
  Reserved
    Internet Assigned Numbers Authority
      iana&iana.org
1
  NxNetworks
    Michael Kellen
      OID.Admin&NxNetworks.com
2
  IBM
    Bob Moore
      remoore&us.ibm.com
3
  Carnegie Mellon
    Mark Poepping
      host-master&andrew.cmu.edu
4
  Unix
    Keith Sklower
      sklower&okeeffe.berkeley.edu
5
  ACC
    Art Berggreen
      art&SALT.ACC.COM
6
  TWG
    John Lunny
```

Private Enterprise Number (PEN) Application Form

http://pen.iana.org/pen/PenApplication,$Form.sdirect

oid 15103

Most Visited | WebStamp Business ... | Getting Started | Latest Headlines | Connectors for Dash... | uBike | MyData | MyAccount | Welcome | Welcome

Contacts | Events | Locations | Tagspaces | Bookmarks | Resources | Options

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline | Resize | Tools | View Source | Op

Private Enterprise Number (PEN... | Haute Ecole d'Ingénierie et de ...

Application Information Confirmation

Please verify that the information you have provided is correct and click the "Confirm" button to submit the application for IANA review. If you would like to make corrections to the application you are submitting, click "Make Changes". Click "Cancel" to exit without submitting the information to IANA.

Organization

Organization Name:	Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud (HEIG-Vd)
Organization Address:	Av. des Sports 20
Organization Phone:	+41 24 55 77584

Contact

Contact Name:	Olivier Liechti
Contact Address:	Av. des Sports 20
Contact Phone:	+41 24 55 77584
Contact Fax:	
Contact Email:	olivier.liechti@heig-vd.ch

http://pen.iana.org/pen/PenApplication.page

Confirm | Make Changes | Cancel

Find: 26027 | Next | Previous | Highlight all | Match case

Done

How to Manage Your OIDs?

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

1.3.6.1.4.1.xxx.n.n.n

Prefix: iso.org.dod.internet.private.enterprise (1.3.6.1.4.1)

Prefix assigned by the IANA to the HEIG-Vd

You define the rules for the suffix of the OIDs

```
.1.*: test
.2.*: teaching .2.1.*: PDA  2.2.*: RES
.3.*: research
.4.*: prod
```

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

LDAP: the Protocol

LDAP: the Protocol

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- LDAP is a client-server protocol
  - Operates on top of TCP
  - Standard port: 389
- Main LDAP commands
  - **Bind** (authentication and session establishment)
  - **Search** - search for and/or retrieve directory entries
  - **Add** a new entry
  - **Delete** an entry
  - **Modify** an entry
  - **Modify** Distinguished Name (DN) - move or rename an entry
  - **Unbind** (session termination)

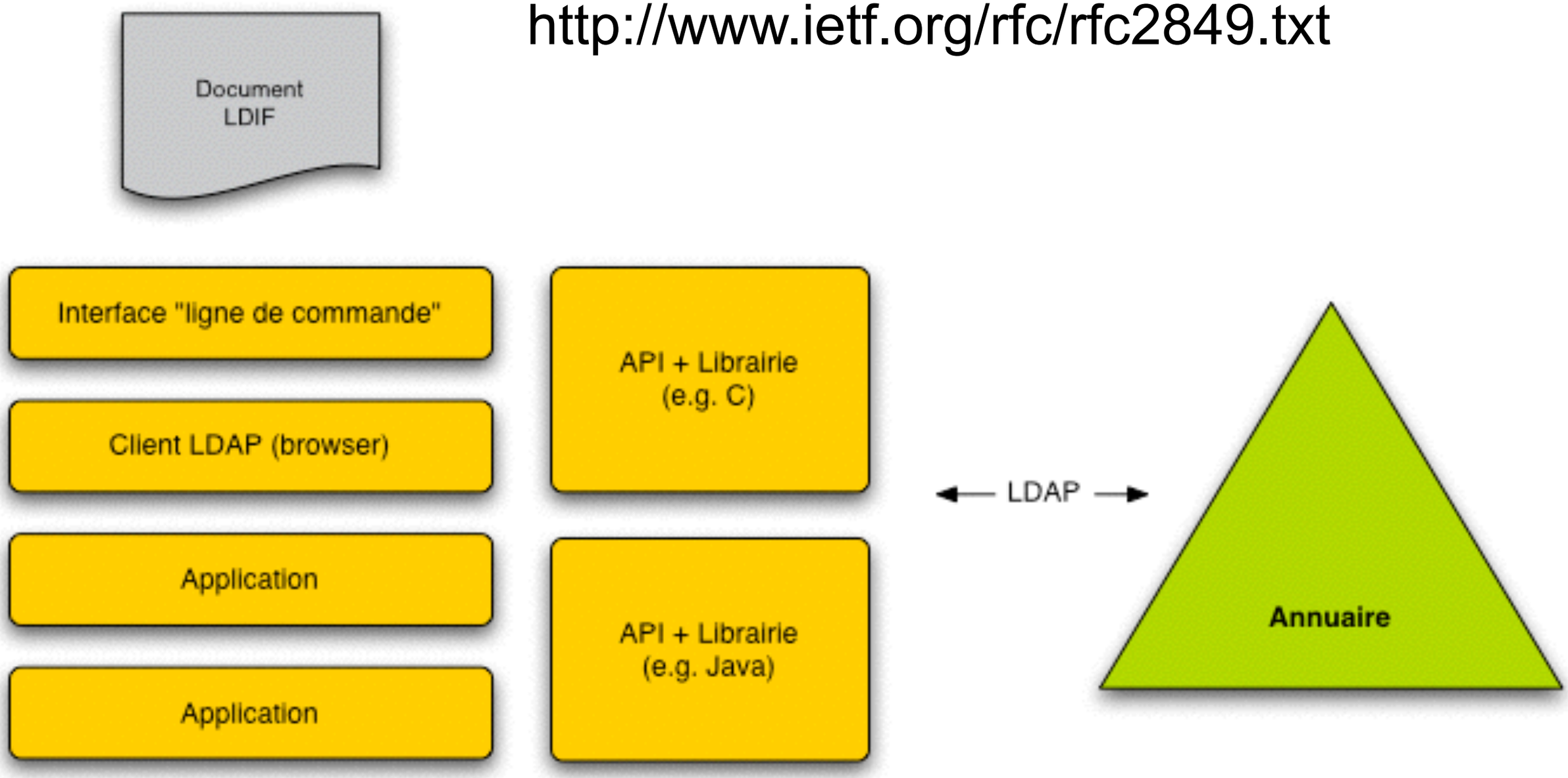
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

LDAP: the Infrastructure

LDAP: Components

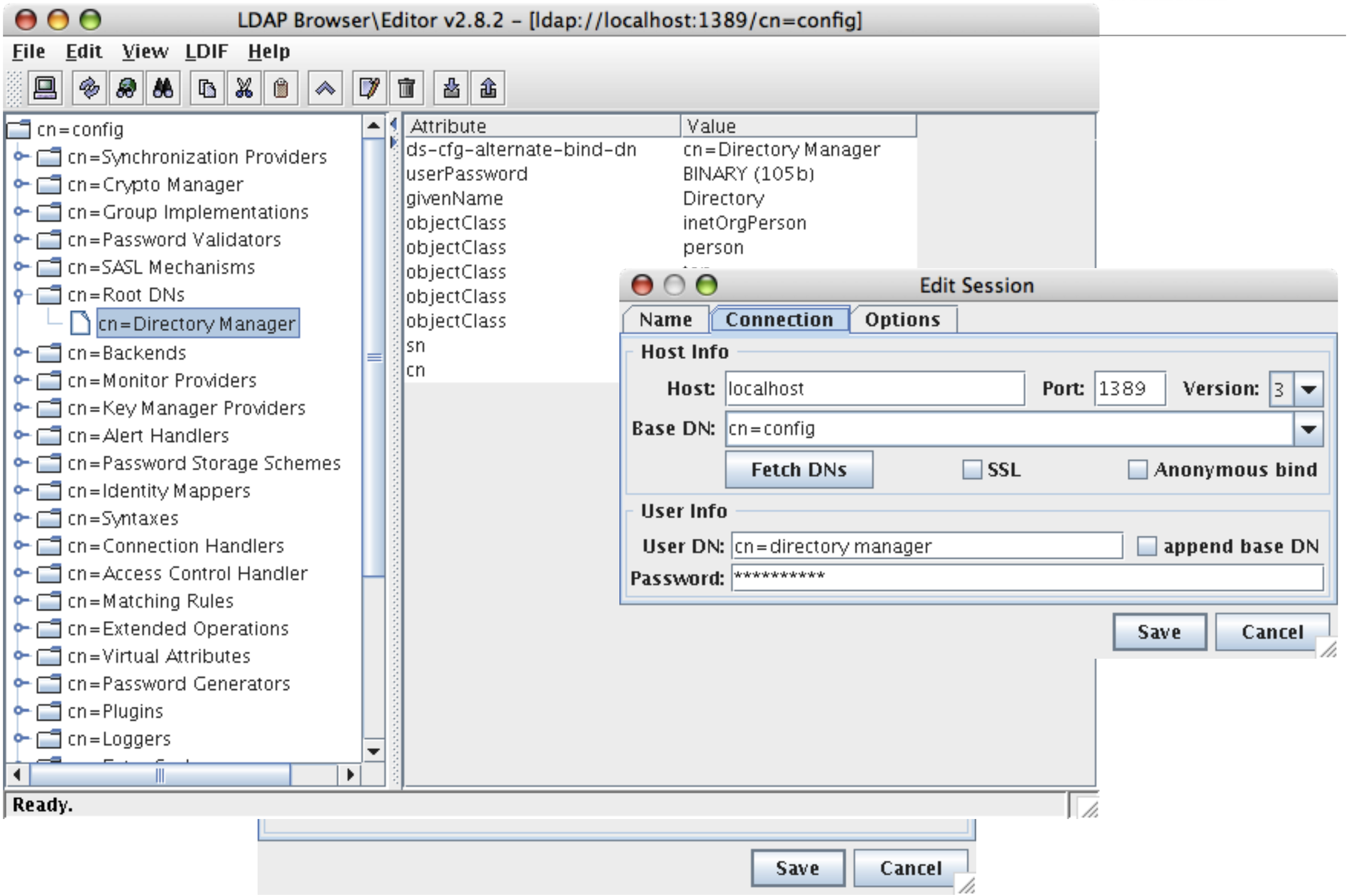
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

http://www.ietf.org/rfc/rfc2849.txt



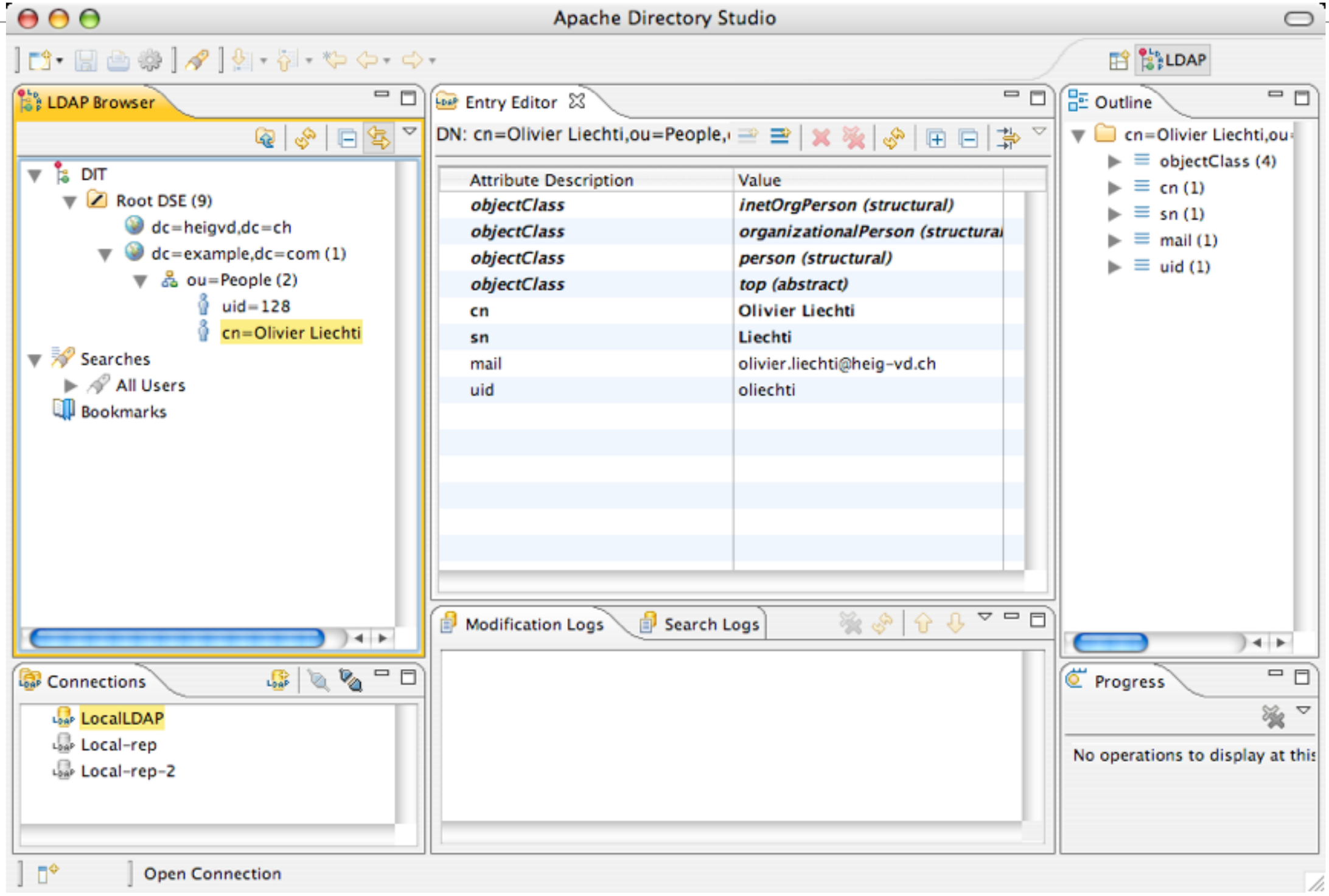
LDAPBrowser

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud



Apache Directory Studio

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud



heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

OpenDS & OpenDJ

OpenDS

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- OpenDS is an LDAP server:
  - developed in Open Source, with the support of Sun Microsystems (now Oracle)
  - 100% Java
  - “Embeddable" in applications
- Installation and setup is very easy
  - via Java WebStart
  - File structure is straightforward
- Yet, OpenDS is “enterprise-ready”
  - replication
  - performance
- OpenDS makes it possible to quickly and easily experiment with LDAP
- http://www.opends.org/

OpenDJ

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

OpenDJ
Congregate - Locate

- OpenDJ is a fork of OpenDS:
  - developed in Open Source, by ForgeRock
  - 100% Java
- Two web sites:
  - Open source project page: http://opendj.forgerock.org
  - ForgeRock product page: http://forgerock.com/products/open-identity-stack/opendj/

Warning!

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- Many operating systems (Mac OS, Solaris, Linux, etc.) include LDAP commands natively:
  - Example: Mac OS provides `/usr/bin/ldapsearch`
  - These commands are typically in the path
- LDAP servers, such as OpenDJ, provide their own commands. They may use the same name (e.g. ldapsearch) but accept different options and their own syntax!!!
  - Exemple: `${OPEN_DJ_INSTALL_PATH}/bin/ldapsearch`
  - These commands are not in the path by default
- For that reason, when you use LDAP commands:
  - Be careful of which command you are using:
    - `cd ${OPEN_DJ_INSTALL_PATH}/bin/`
    - `./ldapsearch`
  - Is different from:
    - `cd ${OPEN_DJ_INSTALL_PATH}/bin/`
    - `ldapsearch`

ldapsearch (1)

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- This command is used to submit queries and extract data from the directory
- Syntax:
  - `ldapsearch [options] [filter] [attributes]`
- Key options:
  - `-h, --host` à quel serveur veut-on se connecter?
  - `-p, --port` sur quel port écoute-t-il?
  - `-D, --bindDN` avec quel identité veut-on se connecter?
  - `-w, --bindPassword` avec quel mot de passe (à éviter, penser à `ps`!!)
  - `-b, --baseDN` à partir d'où veut-on faire la recherche?
  - `-a, --searchScope` avec quelle profondeur?
  - `-T, --dontWrap` pour éviter les ruptures de lignes (LDIF)
  - `--propertiesFilePath` pour éviter de saisir toutes les options
- Documentation:
  - http://opendj.forgerock.org/opendj-server/doc/admin-guide/index/ldapsearch-1.html

ldapsearch (2)

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- Syntax for LDAP filters
  - Defined in RFC 2254
  - Operators for filters: `&`, `|`, `!`
- Examples:
  - Entries for which the attribute **cn** is equal to “Babs Jensen”:
    - `(cn=Babs Jensen)`
  - Entries for which the attribute **cn** is different from “Tim Howes”:
    - `(!(cn=Tim Howes))`
  - People whose **family name** is “Jensen” **or** whose first name is “Babs” and **family name** starts with “J”:
    - `(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*))`

ldapsearch (3)

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

- Return all entries
  - `ldapsearch -h hostname -p 389 -b dc=example,dc=com "(objectclass=*)"`

```
dn: dc=example,dc=com
objectClass: domain
objectClass: top
dc: example

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalunit
objectClass: top
ou: Groups

dn: cn=Directory
Administrators,ou=Groups,dc=example,dc=com
objectClass: groupofuniquenames
objectClass: top
ou: Groups
cn: Directory Administrators
uniquemember: uid=kvaughan, ou=People, dc=example,dc=com
uniquemember: uid=rdaugherty, ou=People,
dc=example,dc=com
uniquemember: uid=hmiller, ou=People, dc=example,dc=com
```

```
dn: uid=scarter,ou=People,dc=example,dc=com
telephonenumber: +1 408 555 4798
```

- **Return only some attributes:**
  - `ldapsearch -h hostname -p 389 -b dc=example,dc=com "(cn=Sam Carter)" telephoneNumber`

ldapmodify (1)

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- This command is used to update data in the directory
- Syntax:
  - `ldapmodify [options] [filter] [attributes]`
- Key options:
  - `-h, --host` what is the IP address of the server?
  - `-p, --port` on which port is it listening?
  - `-D, --bindDN` what is the DN of the user connecting to the server?
  - `-w, --bindPassword` and his password? (bad practice!! think about the `ps` command!!)
  - `-f, --filename` the file containing the LDIF data
- Two ways to provide LDIF data to the server
  - provide LDIF via the command line + CTRL-D (*nix) ou CTRL-Z (Win)
  - Use the `-f` option and capture the LDIF data in a file (strongly recommended)
- Documentation:
  - http://opendj.forgerock.org/opendj-server/doc/admin-guide/index/ldapmodify-1.html

Example: LDIF to add an entry

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

```
dn: uid=john.doe,ou=People,dc=example,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password
```

Example: LDIF to modify an entry

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

```
dn: uid=john.doe,ou=People,dc=example,dc=com
changetype: modify
replace: description
description: This is the new description for John Doe
-
add: mailAlternateAddress
mailAlternateAddress: jdoe@example.com
```

Example: LDIF to delete an entry

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

```
dn: uid=john.doe,ou=People,dc=example,dc=com
changetype: delete
```

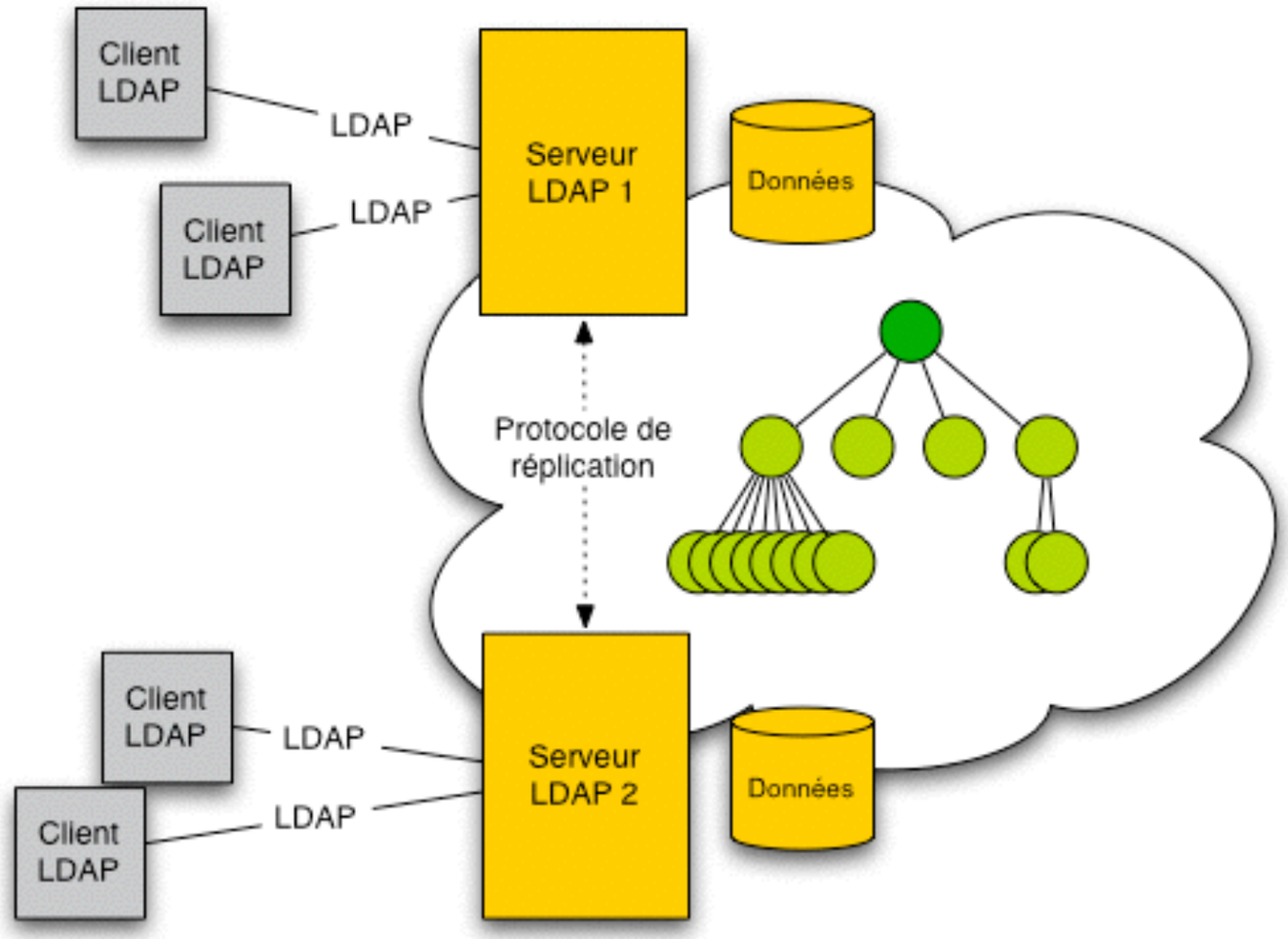
heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Replication

Principles

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

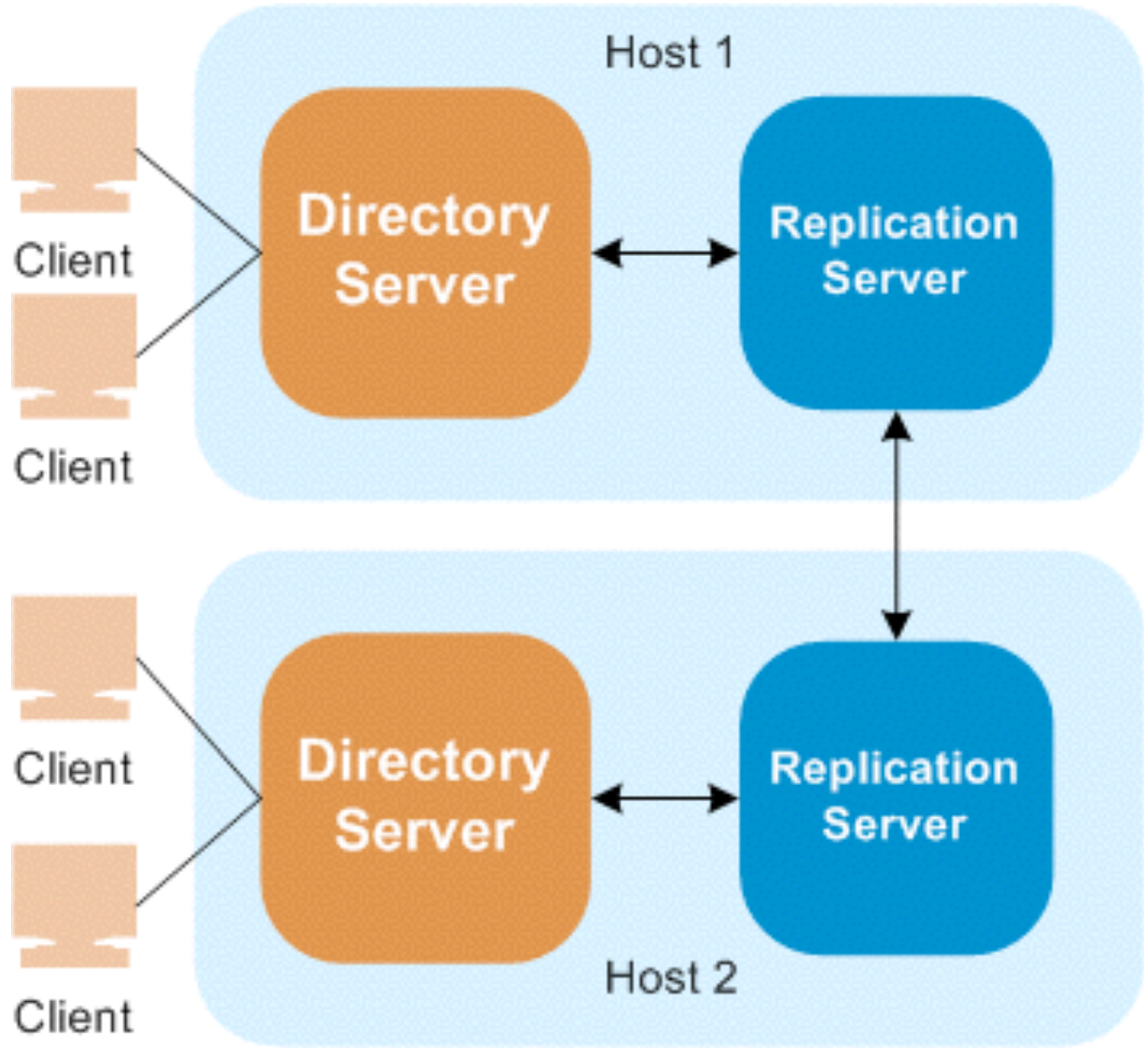
- What is LDAP “replication”?
  - Several LDAP servers are deployed to provide the directory service:
    - ➔ in the same data center (scalability, availability)
    - ➔ in different data centers, possibly in different countries (performance, latency)
  - Data are replicated (copied when updated) between the servers.
  - Clients can connect to the “most appropriate” server (either directly or via an LDAP proxy)



Principles

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

- Reasons for using LDAP replication
  - To ensure systemic qualities!
  - Performance
  - Scalability
  - Availability
- Different topologies are possible:
  - Single Master (1 server accepts write operations)
  - Muli Master (write operations can be submitted to multiple servers)



https://www.opends.org/wiki/page/SmallTopologies

http://www.sun.com/bigadmin/features/articles/dsee6_multimaster.jsp

OpenDS Status Panel

Server Status

Server Run Status: Started Stop Restart

Open Connections: 2

Server Details

Host Name:	olivier-liechtis-computer.local
Administrative Users:	cn=Directory Manager
Installation Path:	/Users/oliechti/OpenDS-rep-2
OpenDS Version:	OpenDS Directory Server 1.1.0-build001
Java Version:	1.5.0_07

Connection Handlers

Address:Port	Protocol	Stat
0.0.0.0:161	SNMP	Disa
0.0.0.0:1689	JMX	Disa
0.0.0.0:3389	LDAP	Ena
0.0.0.0:636	LDAPS	Disa

Data Sources

Base DN	Backend ID	Entries	Replication	Missing C
dc=example,dc=com	userRoot	2002	Enabled	0

OpenDS Quit

OpenDS Status Panel

Server Status

Server Run Status: Started Stop Restart

Open Connections: 3

Server Details

Host Name:	olivier-liechtis-computer.local
Administrative Users:	cn=Directory Manager
Installation Path:	/Users/oliechti/OpenDS-rep
OpenDS Version:	OpenDS Directory Server 1.1.0-build001
Java Version:	1.5.0_07

Connection Handlers

Address:Port	Protocol	State
0.0.0.0:161	SNMP	Disabled
0.0.0.0:1689	JMX	Disabled
0.0.0.0:2389	LDAP	Enabled
0.0.0.0:636	LDAPS	Disabled

Data Sources

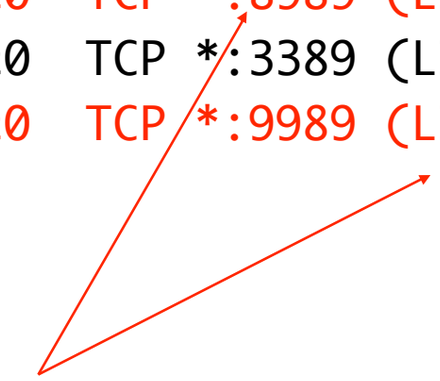
Base DN	Backend ID	Entries	Replication	Missing Changes	Age of Oldest Missing Change
dc=example,dc=com	userRoot	2002	Enabled	0	<not available>

OpenDS Quit

Replication in OpenDS

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

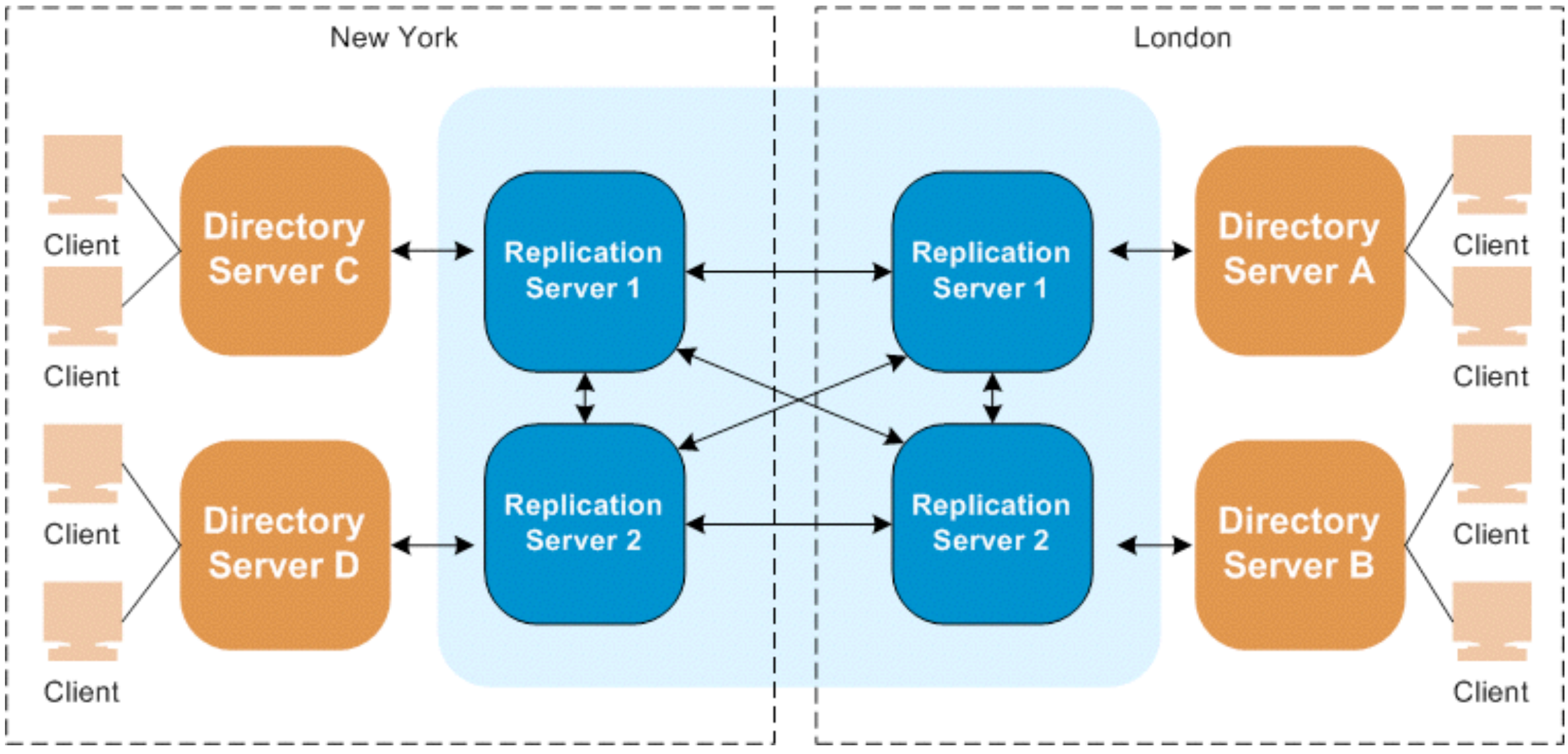
```
$ lsof -P -i TCP | grep 89 | grep LISTEN
java      6145 oliechti   33u  IPv6 0x7a4c46c      0t0  TCP *:1389 (LISTEN)
java      9527 oliechti   40u  IPv6 0x798da24      0t0  TCP *:2389 (LISTEN)
java      9527 oliechti   46u  IPv6 0x79beaf0      0t0  TCP *:8989 (LISTEN)
java      9617 oliechti   41u  IPv6 0x7a2f174      0t0  TCP *:3389 (LISTEN)
java      9617 oliechti   46u  IPv6 0x7a2dde8      0t0  TCP *:9989 (LISTEN)
```



replication ports

Multi-Site Topology

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud



heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

LDAP with Java

Java Naming & Directory Interface (JNDI)

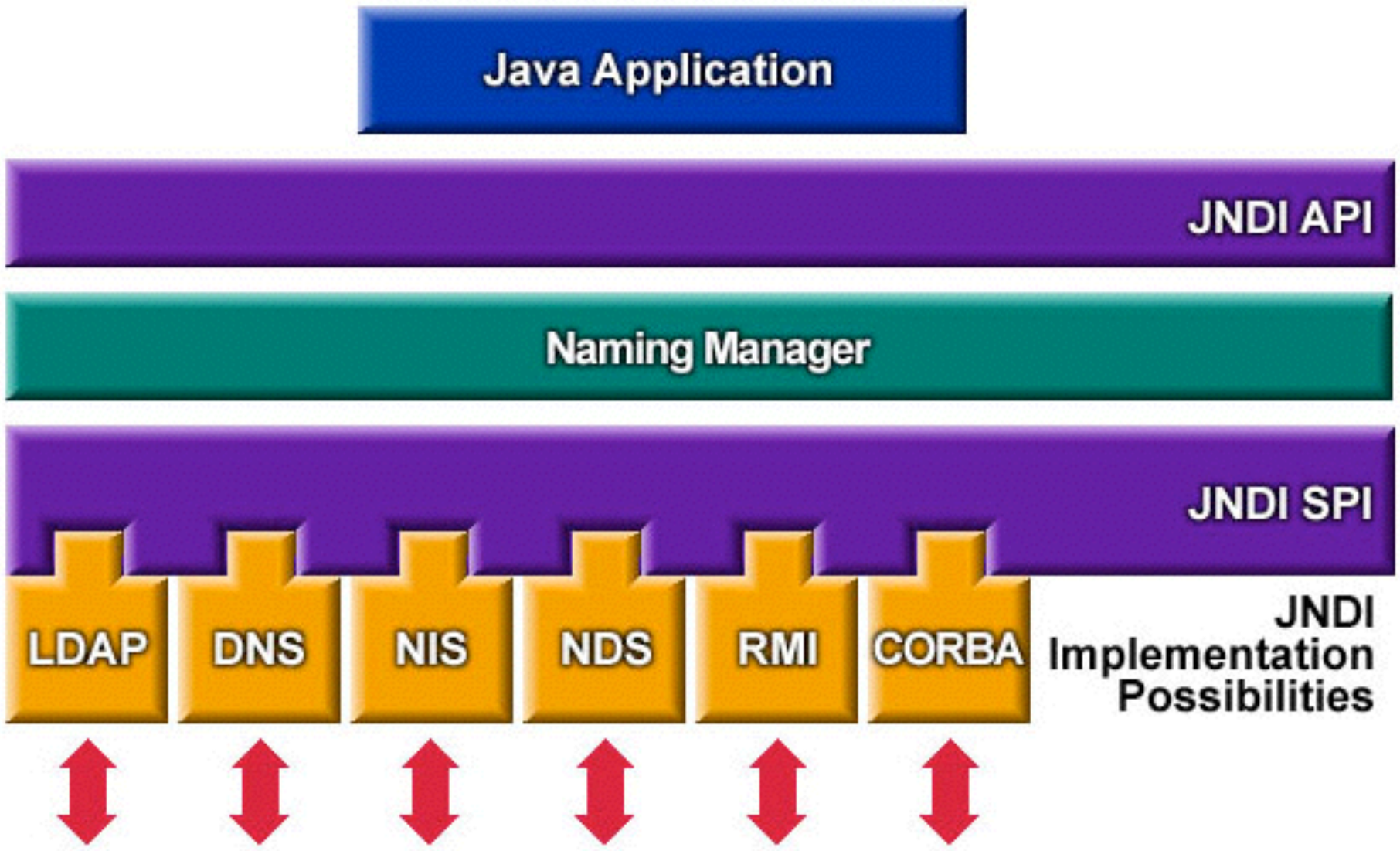
Java Naming and Directory Interface (JNDI)

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud

- LDAP is one of the application-level protocols that deals with data organized in a hierarchical data structure.
- Java developers would like:
  - a standard API that they can use for any protocol used to access hierarchical data (LDAP and others)
  - to be able to use this API to interact with any of the LDAP implementation (Active Directory, OpenDJ, OpenLDAP, etc.)
- In other words, they would like to have **the equivalent of JDBC** (used to talk to different relational database management systems in the same way), but for LDAP servers.
- JNDI is an answer to this need. The API provides a standardized API to interact with naming and directory services.

Java Naming and Directory Interface (JNDI)

heig-vd
Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud



http://java.sun.com/products/jndi/tutorial/getStarted/overview/index.html

How do I use JNDI?

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- The first step consists of establishing a connection with the directory server.
- This is done with the `InitialDirContext` class:

```
// Set up the environment for creating the initial context
Hashtable env = new Hashtable();

env.put(Context.INITIAL_CONTEXT_FACTORY,
  "com.sun.jndi.ldap.LdapCtxFactory");

env.put(Context.PROVIDER_URL,
  "ldap://localhost:389/o=JNDITutorial");

DirContext ctx = new InitialDirContext(env);
```

How do I use the API?

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

- Once connected, the API provides abstractions to interact with the naming service.
- It is possible to navigate in the hierarchy, to access the entries and their attributes. It is also possible to submit LDAP filters via the API.

```
// Create the default search controls
SearchControls ctls = new SearchControls();

// Specify the search filter to match
// Ask for objects that have the attribute "sn" == "Geisel"
// and the "mail" attribute
String filter = "(&(sn=Geisel)(mail=*))";

// Search for objects using the filter
NamingEnumeration answer = ctx.search("ou=People", filter, ctls);
```

How do I use the API?

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

> Here is an example for iterating over all attributes of an entry, and then over all values of each attribute (remember that LDAP attributes can be **multivalued**).

```
// Search for objects using the filter
NamingEnumeration answer = ctx.search("ou=People", filter, ctls);

for (NamingEnumeration ae = answer.getAll(); ae.hasMore();) {
    Attribute attr = (Attribute)ae.next();
    System.out.println("attribute: " + attr.getID());

    /* Print each value */
    for (NamingEnumeration e = attr.getAll(); e.hasMore();
         System.out.println("value: " + e.next()));
}
```