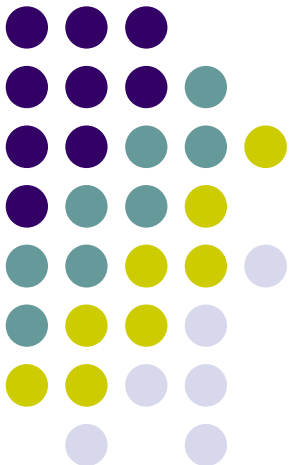
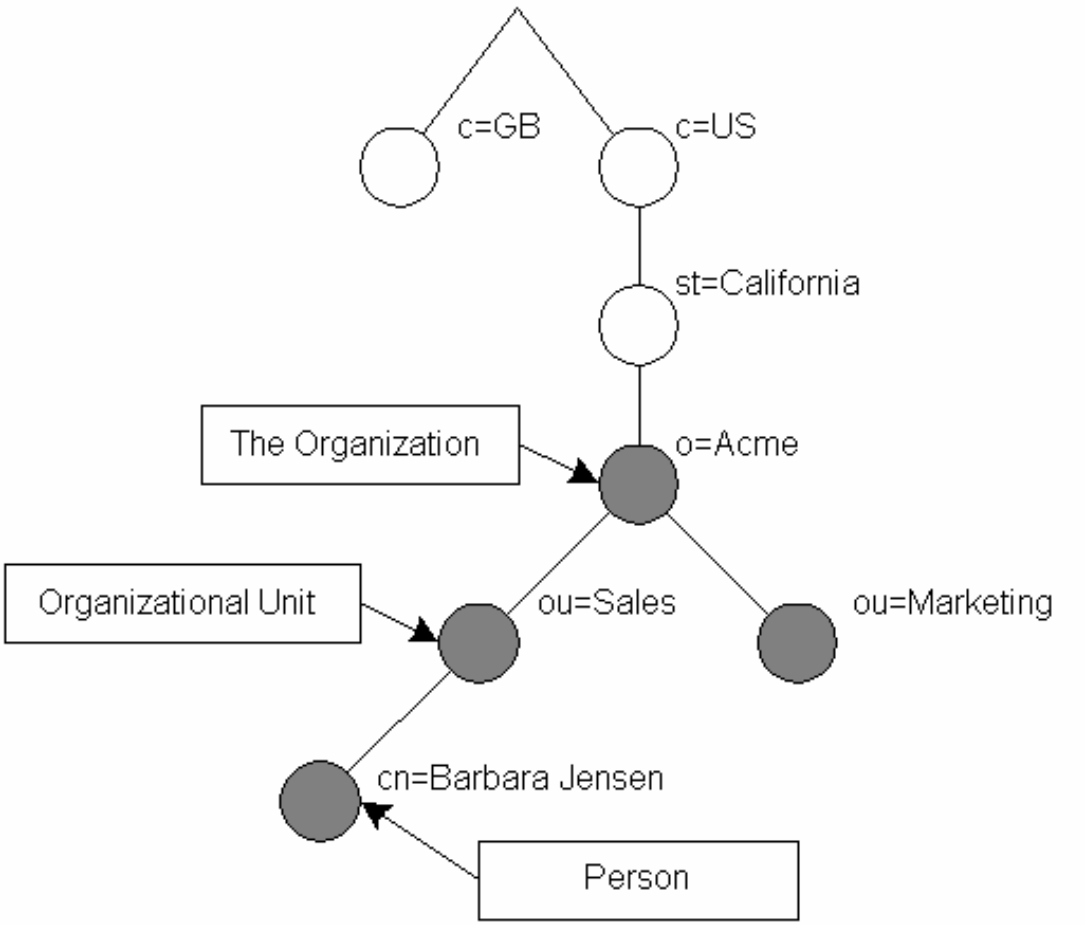
Υλοποίηση Δικτυακών Υποδομών και Υπηρεσιών: Ρύθμιση Εξυπηρετητή LDAP σε Ubuntu Linux

Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης & Τεχνολογίας Τηλεπικοινωνιών

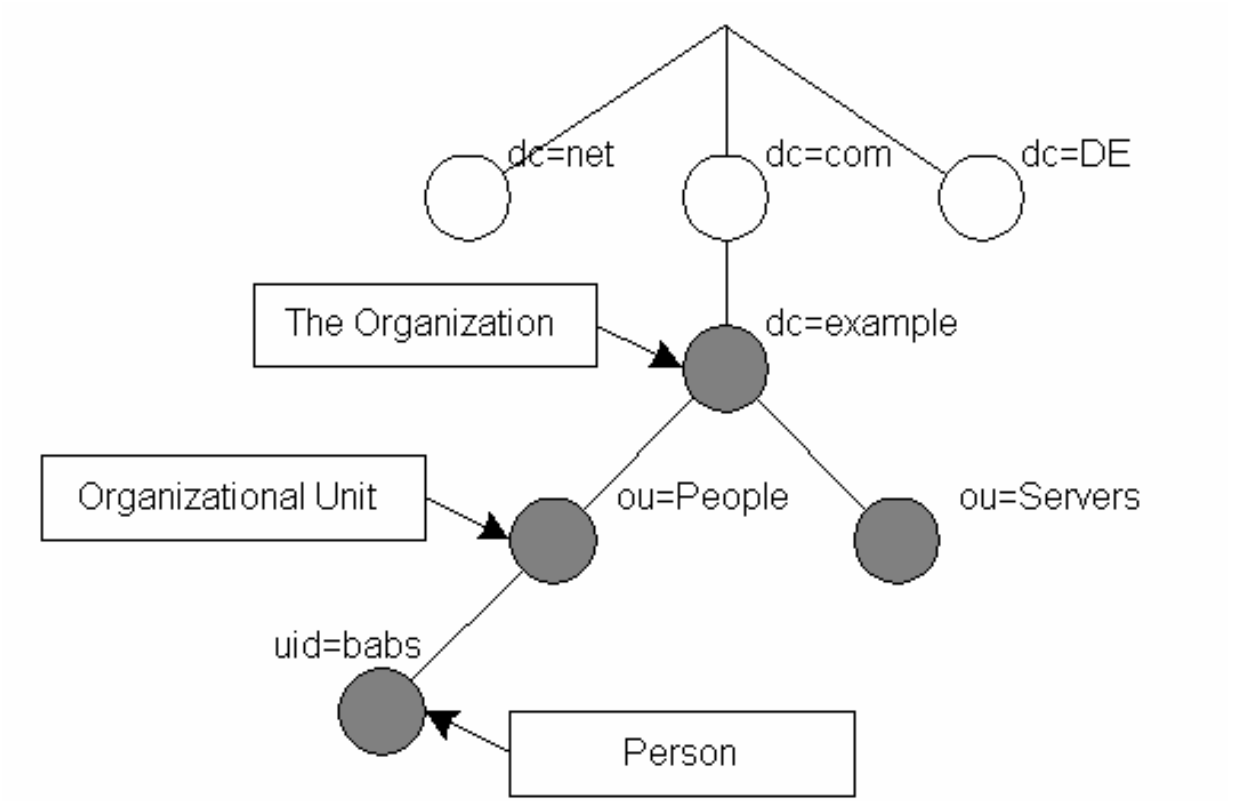
Ευάγγελος Α. Κοσμάτος



LDAP Δέντρο (φυσική οργάνωση)



LDAP Δέντρο (internet domain)



Πρόσβαση σε πληροφορία στον LDAP

- Αναφερόμαστε με την χρήση distinguished name, τα οποία συνθέτονται από το όνομα του entity (το οποίο ονομάζεται Relative Distinguished Name - RDN) και από τα ονόματα των προγόνων του.
  - Για παράδειγμα για την εγγραφή Barbara Jensen στο προηγούμενο σχήμα έχουμε RDN uid=babs και DN τα uid=babs, ou=People, dc=example,dc=com.
- Το πλήρες format του DN ορίζεται στο RFC2253, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names."

OpenLDAP (slapd)

- LDAPv3
- Transport Layer Security (TLS/SSL)
- Έλεγχος τοπολογίας (Topology control)
- Έλεγχος πρόσβασης (Access control)
- Επιλογή από βάσεις δεδομένων
- Γενικό API
- Υποστήριξη Threads
- Υποστήριξη Replication
- Υποστήριξη Proxy Cache
- Ευέλικτο Configuration

OpenLDAP Configuration (1)

- Βασικά αρχεία ρυθμίσεων του Openldap είναι στον κατάλογο /etc/ldap.
  - Κυριότερο αρχείο ρυθμίσεων το **slapd.conf**
- Εισάγουμε τα βασικά LDAP schemes

```
# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
```

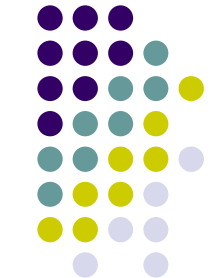
OpenLDAP Configuration (2)

- Καθορίζουμε την βάση που θα χρησιμοποιήσουμε:
  database hdb

- Καθορίζουμε τον βασικό κατάλογο:
  suffix “dc=corelab”

- Καθορίζουμε τον βασικό χρήστη του καταλόγου, ο οποίος έχει όλα τα δικαιώματα:
  rootdn "cn=admin,dc=corelab"
  rootpw {MD5}xxxxxxxxxxxxxxxxxxxxxxxxxxxx

OpenLDAP Configuration (3)



- Τον κωδικό του admin τον βάζουμε σε μορφή MD5 για λόγους ασφαλείας. Για να βρείτε την MD5 κωδικοποίηση του κωδικού που θα χρησιμοποιήσετε εκτελείτε την εντολή:

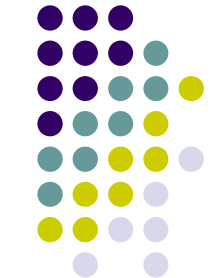
  slappasswd –h {MD5}

OpenLDAP Configuration (4)

- Καθορίζουμε τα δικαιώματα πρόσβασης:

```
access to attrs=userPassword
by dn="cn=admin,dc=corelab" write
by anonymous auth
by self write
by * none
```

OpenLDAP Configuration (5)



- Πρόσβαση ανάγνωσης σε όλους:
  access to dn.base="" by * read

- Απόλυτα δικαιώματα μόνο στον admin
  **access to *
  by dn="cn=admin,dc=corelab" write
  by * read**

Κείμενο σε ASN.1

Παράμετροι της εντολής slapd (1)

- start: Starts with default configuration
- stop: Stops the slapd
- -f <filename>: This option specifies an alternate configuration file for slapd. The default is normally /usr/local/etc/openldap/slapd.conf.
- -h <URLs>: This option specifies alternative listener configurations.The default is ldap:/// which implies LDAP over TCP on all interfaces on the default LDAP port 389. You can specify specific host-port pairs or other protocol schemes (such as ldaps:// or ldapi://). For example, -h "ldaps:// ldap://127.0.0.1:666" will create two listeners: one for LDAP over SSL on all interfaces on the default LDAP/SSL port 636, and one for LDAP over TCP on the localhost (loopback) interface on port 666. Hosts may be specified using IPv4 dotted-decimal form or using host names. Port values must be numeric.

- -n <service-name>: This option specifies the service name used for logging and other purposes. The default service name is slapd.

Παράμετροι της εντολής slapd (2)

- -l <syslog-local-user>: This option specifies the local user for the syslog(8) facility. Values can be LOCAL0, LOCAL1, LOCAL2, ..., and LOCAL7. The default is LOCAL4. This option may not be supported on all systems.
- -u user -g group: These options specify the user and group, respectively, to run as. user can be either a user name or uid. group can be either a group name or gid.
- -r directory: This option specifies a run-time directory. slapd will chroot(2) to this directory after opening listeners but before reading any configuration files or initializing any backends.
- -d <level> | ?: This option sets the slapd debug level to <level>. When level is a `?' character, the various debugging levels are printed and slapd exits, regardless of any other options you give it.

Βοηθητικό πρόγραμμα slapcat

- Για να δούμε τα περιεχόμενα της βάσης, εκτελούμε την εντολή:
  slapcat

- Το πρόγραμμα slapcat χρησιμοποιείται για να εξάγει την βάση δεδομένων σε ένα LDIF αρχείο:
- **slapcat -l <filename> -f <slapdconfigfile> [-d <debuglevel>] [-n <databasenumber>|-b <suffix>]** where -n or -b is used to select the database in the slapd.conf(5) specified using -f. The corresponding LDIF output is written to standard output or to the file specified using the -l option.

Δημιουργία νέας Βάσης

- Σταματάμε τον OpenLDAP server
  /etc/init.d/slapd stop
- Διαγράφουμε την βάση
  rm –r /var/lib/ldap/*
- Εκκινούμε τον OpenLDAP server
  /etc/init.d/slapd start
- Πηγαίνουμε στο home directory του root και δημιουργούμε το ldif αρχείο με τα περιεχόμενα που θέλουμε.
- Εισάγουμε το ldif αρχείο στη βάση
  ldapadd -x -D "cn=admin,dc=corelab" -W -f mydb.ldif

Αρχείο ldif (1)

```
dn: dc=corelab
objectClass: top
objectClass: dcObject
objectClass: organization
o: Core Lab
dc: corelab

dn: cn=admin,dc=corelab
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: {MD5}xxxxxxxxxxxxxxxxxxxxx
```

Αρχείο ldif (2)

dn: DN

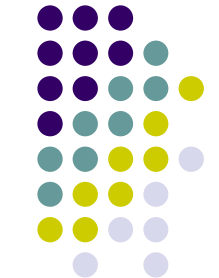
- **Η dn directive ορίζει ένα Distinguished Name (DN) και χρησιμοποιείται για να ορίσει ένα entry (ακολουθούν και άλλες directives για το entry).**
- **Θα πρέπει να υπάρχει κενή γραμμή πριν την dn directive**
  - **(εκτός εάν είναι η πρώτη directive του αρχείου)**

Αρχείο ldif (3)

objectclass: objectclassname

- **Η objectclass directive επιτρέπει ένα objectclass να προστεθεί στο entry.**
- **Θα πρέπει να υπάρχει τουλάχιστον ένα objectclass ανά entry.**
- **Παράδειγμα**
  - **objectClass: top Αποτελεί μια ιδιαίτερη, αφηρημένη κλάση, από την οποία όλες οι άλλες άμεσα ή έμμεσα κληρονομούν χαρακτηριστικά της.**

Βοηθητικό πρόγραμμα slapsearch



- Αναζήτηση σε ldap κατάλογο
- Παράδειγμα αναζήτησης
  ldapsearch -x -h localhost –b 'dc=corelab' uid=admin

Δημιουργία user και group (1)

- Για λόγους ασφάλειας προτείνεται ο OpenLDAP server να μην εκτελείται από τον χρήστη root. Συνίσταται η δημιουργία ενός νέου χρήστη (π.χ. ldap) και μιας νέας ομάδας (π.χ. ldap), για αποκλειστική χρήση στην εκτέλεση του OpenLDAP server.
- Για την δημιουργία τους εκτελείτε τις ακόλουθες εντολές:

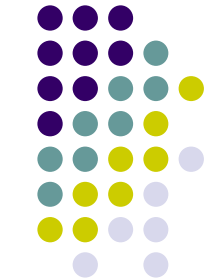
  adduser ldap

Δημιουργία user και group (2)

- Επίσης, ο νέος χρήστης και group θα πρέπει να δηλωθεί και στο σύστημα. Στο Ubuntu τα παραπάνω καθορίζονται στο αρχείο /etc/default/slapd:

```
SLAPD_USER=ldap
SLAPD_GROUP=ldap
SLAPD_PIDFILE=/var/run/slapd/slapd.pid
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_OPTIONS="-4"
```

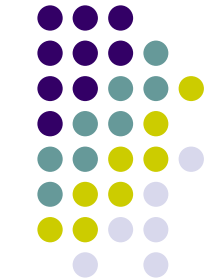
Δημιουργία user και group (3)



- Τέλος θα πρέπει να αλλάξετε τα δικαιώματα πρόσβασης στα ακόλουθα αρχεία:

```
chgrp ldap /etc/ldap/slapd.conf
chmod 640 /etc/ldap/slapd.conf
chown –R ldap.ldap /var/run/slapd
chmod 750 /var/run/slapd
chmod 644 /var/run/slapd/*
chown –R ldap.ldap /var/lib/ldap
chmod 750 /var/lib/ldap
chmod 600 /var/lib/ldap/*
```

Εκτέλεση slapd



slapd -h 'ldap://127.0.0.1:389/ ldaps:/// ldapi:///' -g ldap –u ldap -4

- Αναλυτικά το παραπάνω περιγράφει τα εξής:
  - Έχει σηκωθεί επιτυχώς ο OpenLDAP server daemon (slapd)
  - Ο οποίος ακούει για αιτήσεις που προέρχονται από το ίδιο μηχάνημα (ldap://127.0.0.1:localhost)
  - Ο slapd daemon τρέχει με δικαιώματα χρήστη ldap και group ldap (-g ldap –u ldap)
  - Απαντάει σε αιτήσεις που έρχονται από IPv4 διευθύνσεις (-4)

Configuration ldap.conf

- Client side configuration
  - Αρχείο /etc/ldap/ldap.conf

```
BASE dc=corelab
URI ldap://127.0.0.1:389
```

Backup Configuration files

Ubuntu:

```
sudo cp /etc/ldap/slapd.conf /etc/ldap/slapd.conf_old

sudo cp /etc/default/slapd /etc/default/slapd_old
```

Πρόγραμμα phpldapadmin (1)

- Γραφικό περιβάλλον για LDAP Server
- Εκτέλεση στο browser
  http://127.0.0.1/phpldapadmin
- Αν εμφανιστεί λάθος λόγω μικρού μεγέθους μνήμης php
  sudo vim /etc/php5/apache2/php.ini
  memory_limit = 50M
  sudo /etc/init.d/apache2 restart

Πρόγραμμα phpldapadmin (2)