

Ασφάλεια Πληροφοριακών Συστημάτων

«Αυθεντικοποίηση και Εξουσιοδότηση – Παράδειγμα ελέγχου πρόσβασης με openidp»

Τμήμα Πληροφορικής

Υπ. Δρ. Β.Μάλαμας (bagmalamas@unipi.gr)
Αν. Καθηγητής Π. Κοτζανικολάου

Περιεχόμενα

1. Εισαγωγή
2. Δημιουργία εργαστηριακού περιβάλλοντος
3. Εγκατάσταση LDAP server
4. Εγκατάσταση του rhpldapadmin
5. Ρυθμίσεις του rhpldapadmin
6. Σύνδεση με rhpldapadmin
7. Δημιουργία χρηστών
8. Παραδείγματα σύνδεσης για αυθεντικοποίηση

Υπηρεσίες καταλόγου

Τι είναι ένας κατάλογος (Directory) ;

Κατάλογος:

Μια συλλογή πληροφοριών που βασικός της σκοπός είναι η αναζήτηση και η ανάγνωση των δεδομένων και σπανίως η τροποποίηση τους.

Υπηρεσία καταλόγου:

Παρέχει πρόσβαση σε πληροφορίες καταλόγου

Εξυπηρετητής καταλόγου :

Πρόγραμμα το οποίο παρέχει την Υπηρεσία καταλόγου.

Εισαγωγή (1) – Υπηρεσίες καταλόγου

Τύποι δεδομένων καταλόγου

- Λογαριασμοί
- Ψευδώνυμα ηλεκτρονικού ταχυδρομείου και λίστες
- Κλειδιά κρυπτογράφησης
- Διευθύνσεις IP
- Hostnames
- Εκτυπωτές

Γνωστές υπηρεσίες καταλόγου

- DNS
- LDAP
- NIS

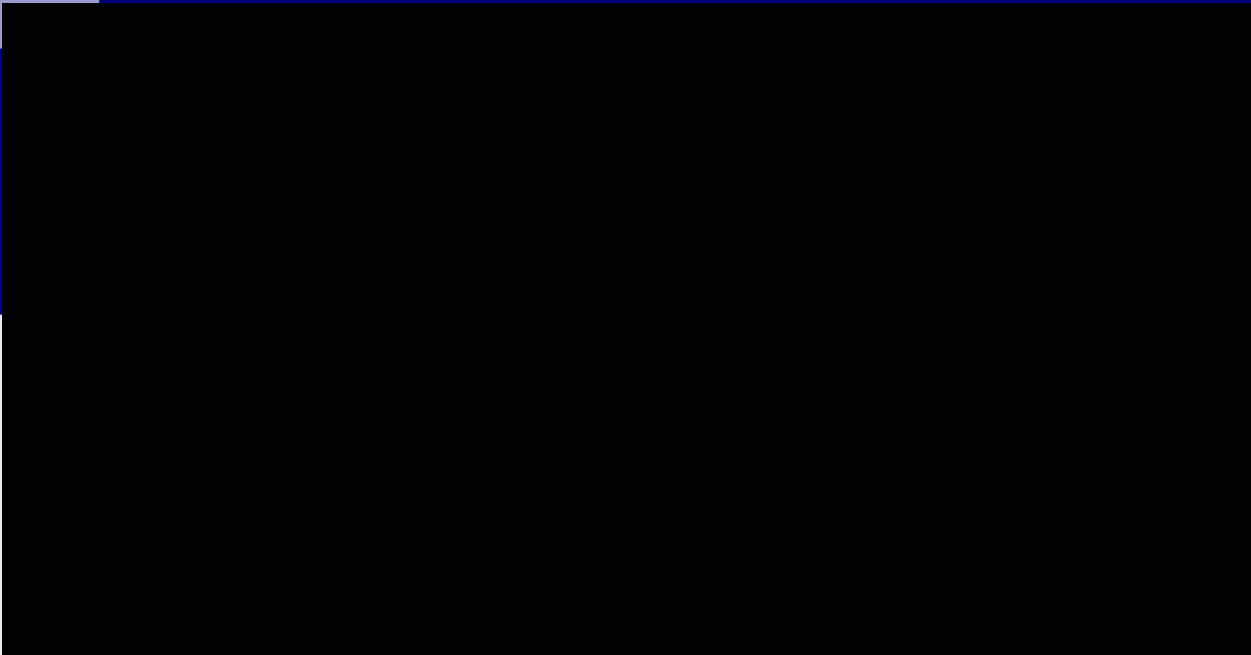
Εισαγωγή (2) - γενικά για το LDAP

LDAP (Lightweight Directory Access Protocol)

- Όπως λέει και ο τίτλος του πρόκειται για ένα πρωτόκολλο που χρησιμοποιείται από εφαρμογές για να αποκτήσουν πρόσβαση σε πληροφορίες καταλόγου
- Πρόκειται για μια συλλογή πληροφοριών που έχει σαν βασικό σκοπό την αναζήτηση και την ανάγνωση των δεδομένων
- Στην πραγματικότητα πρόκειται για μια υπηρεσία καταλόγου που προσφέρει γρήγορη αναζήτηση (πιο γρήγορη από τις συμβατικές βάσεις δεδομένων) προσφέροντας ενοποιημένη πρόσβαση σε πόρους του δικτύου, βελτίωση της διαχείρισης των δεδομένων

Εισαγωγή (3)- Η δομή του LDAP

Η δομή που ακολουθεί ο LDAP είναι ιεραρχική δεντρική σε αντίθεση με την σχεσιακή δομή που ακολουθούν οι βάσεις δεδομένων



Εισαγωγή (4) - Ενέργειες στον LDAP

Μερικές βασικές ενέργειες που μπορεί μια εφαρμογή να πραγματοποιήσει με έναν LDAP server είναι:

- Αναζήτηση
- Προσθήκη χρήστη
- Διαγραφή χρήστη
- Αλλαγή δεδομένων χρήστη
- Bind: ανταλλαγή πληροφοριών αυθεντικοποίησης μεταξύ server και client
(μας ενδιαφέρει ιδιαίτερα για την τελική εργασία όπου τον ρόλο του server θα παίζει ο LDAP και τον ρόλο του client η εφαρμογή μας)

Εισαγωγή (5)

- Ένας κατάλογος LDAP αποτελείται από εγγραφές (entries) – οι εγγραφές είναι συνήθως τα στοιχεία των εργαζομένων/χρηστών
- Κάθε εγγραφή αποτελείται από χαρακτηριστικά (attributes)
π.χ. Τέτοια χαρακτηριστικά θα μπορούσαν να είναι το όνομα ή ο αριθμός τηλεφώνου ενός χρήστη
- Κάθε καταχώρηση είναι μια συλλογή χαρακτηριστικών που έχει ένα μοναδικό όνομα (Distinguished Name – DN), το οποίο χρησιμοποιείται ως αναφορά της κάθε καταχώρησης και προσδιορίζει με μοναδικό τρόπο μια εγγραφή LDAP

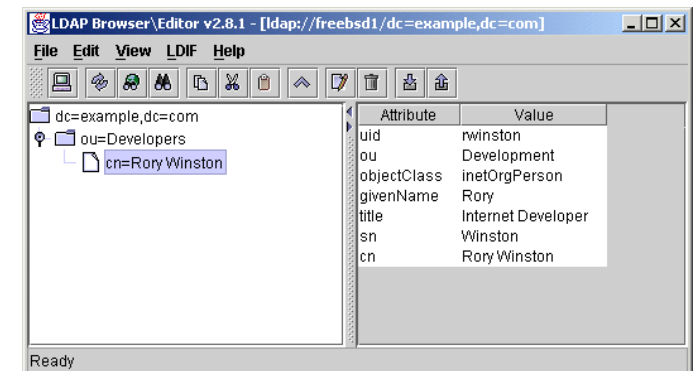
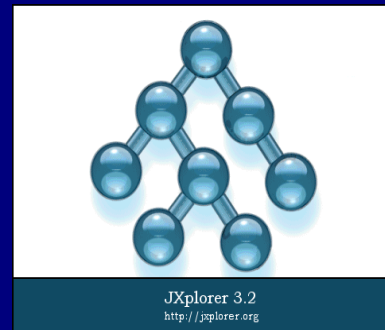
Εισαγωγή (6) - Η λειτουργία του LDAP

- Η υπηρεσία καταλόγου LDAP [OpenLDAP] είναι βασισμένη στο μοντέλο επικοινωνίας πελάτη-εξυπηρετητή.
- Ένας ή περισσότεροι κεντρικοί υπολογιστές LDAP περιέχουν τα δεδομένα που αποτελούν το δέντρο πληροφοριών καταλόγου (*Directory Information Tree -DIT*)
- Ο κεντρικός υπολογιστής αποκρίνεται με μια απάντηση ή/και με έναν δείκτη όπου ο πελάτης μπορεί να πάρει τις πρόσθετες πληροφορίες

Εισαγωγή (7) - Browsers για τον LDAP

Οι φυλλομετρητές LDAP έχουν την δυνατότητα να συνδεθούν με οποιοδήποτε LDAP εξυπηρετητή και να ανακτήσουν στοιχεία από αυτόν.

- LDAP Browser
- phpldapadmin
- Softerra
- LDAP Admin
- JXplorer



Δημιουργία εργαστηριακού περιβάλλοντος (1)

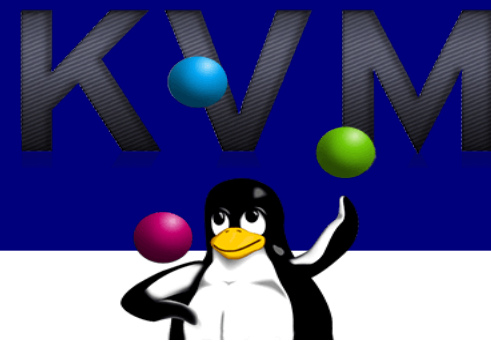
Επιλογή έκδοσης Linux server



Το λειτουργικό στο οποίο θα «τρέξει» ο LDAP server

Δημιουργία εργαστηριακού περιβάλλοντος (2)

Επιλογή λογισμικού για Virtualization

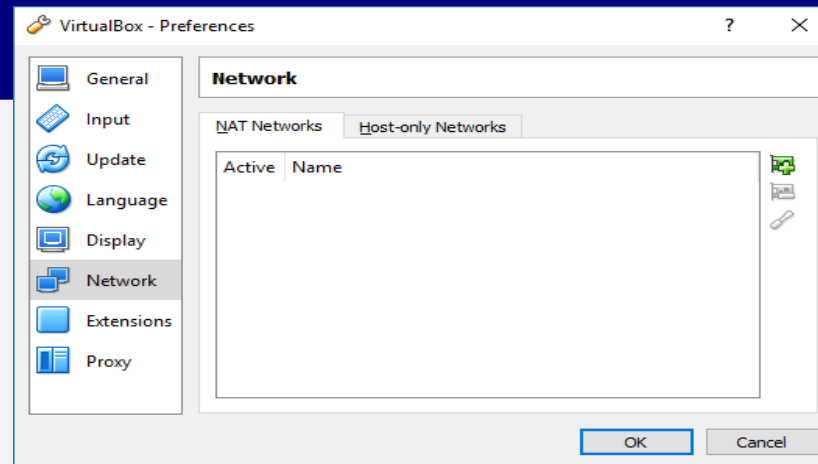


Για να μπορέσουμε να τρέξουμε παράλληλα το λειτουργικό του server

Δημιουργία εργαστηριακού περιβάλλοντος (3)

Εγκατάσταση Ubuntu server σε Virtualbox

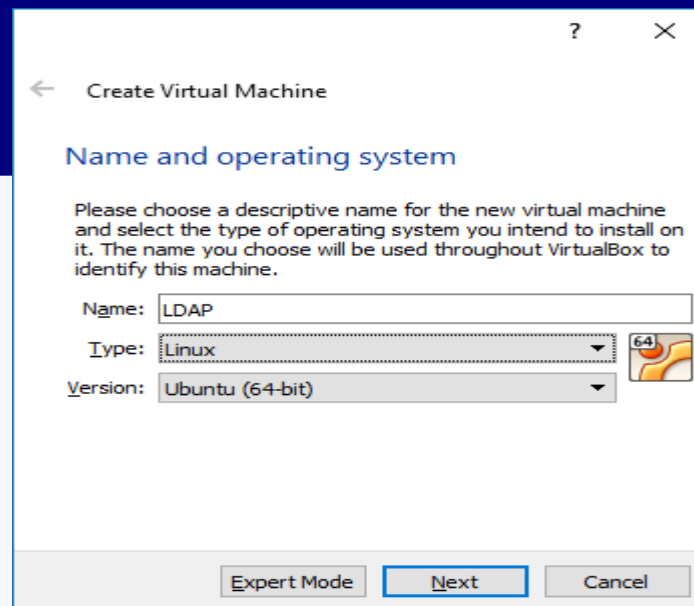
1. Κατεβάζουμε από τον ιστότοπο ubuntu.com την έκδοση `server16.04.3.iso` για 64bit
2. Ανοίγουμε το `virtualbox` αφού προηγουμένως το έχουμε κάνει εγκατάσταση στο λειτουργικό μας σύστημα
3. Επιλέγουμε από το μενού του `virtualbox` `File>Preferences` την καρτέλα `Network`



Δημιουργία εργαστηριακού περιβάλλοντος (4)

Εγκατάσταση Ubuntu server σε Virtualbox

5. Δημιουργούμε μια νέα virtual μηχανή με τον οδηγό από το μενού Machine >New
6. Επιλέγουμε το όνομα, τον τύπο του λειτουργικού που θα εγκαταστήσουμε και την έκδοση




← Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type: 

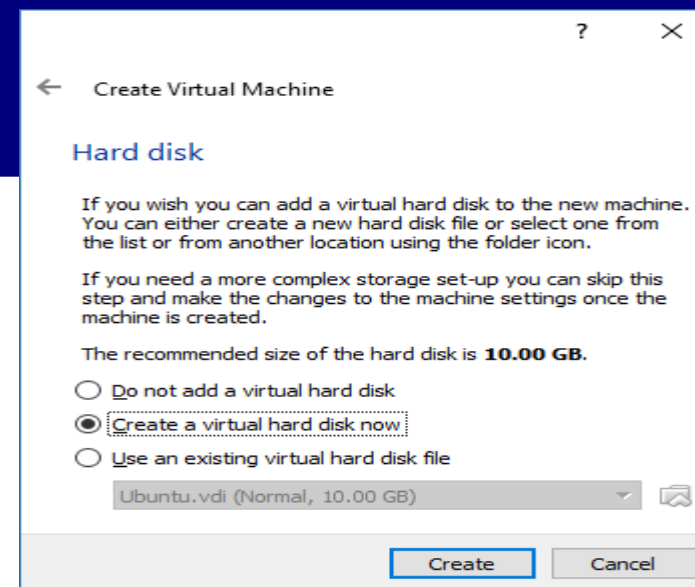
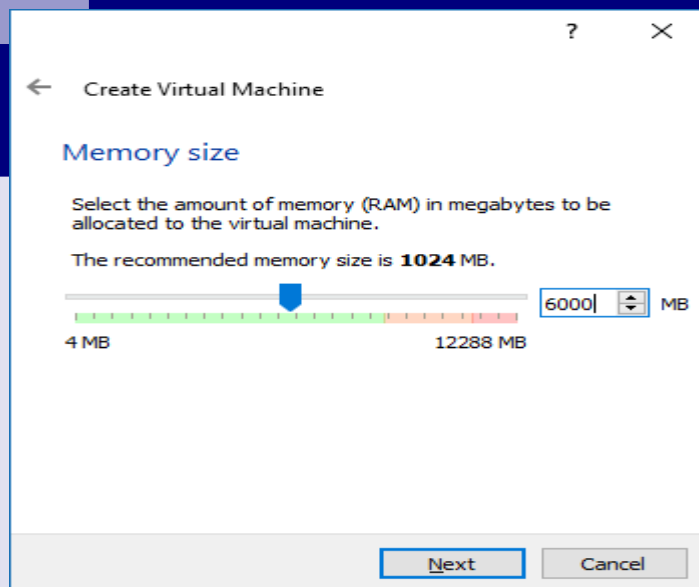
Version:

Δημιουργία εργαστηριακού περιβάλλοντος (5)

Εγκατάσταση Ubuntu server σε Virtualbox

7. Επιλέγουμε την ram που θα διαθέσουμε

8. Επιλέγουμε την χωρητικότητα του δίσκου που θα διαθέσουμε

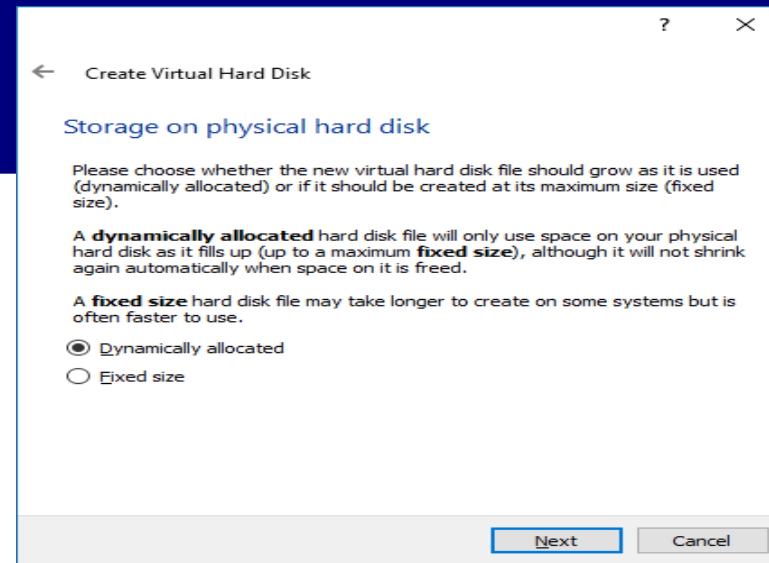
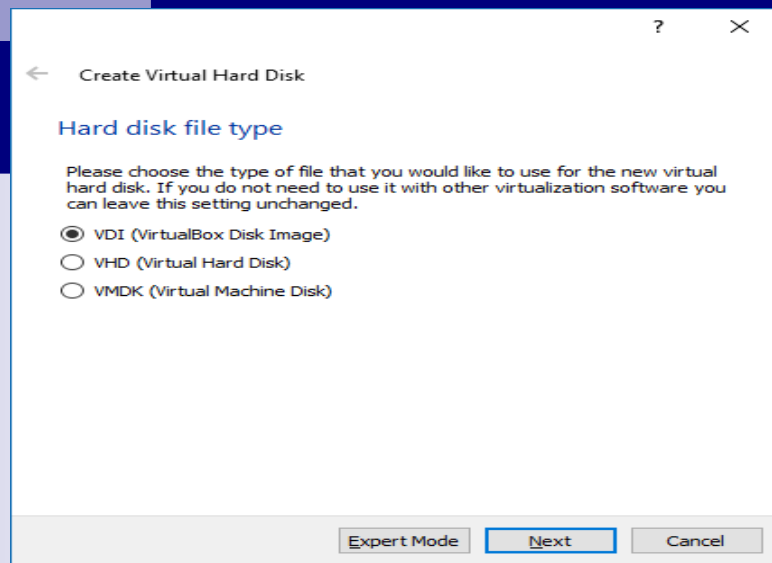


Δημιουργία εργαστηριακού περιβάλλοντος (6)

Εγκατάσταση Ubuntu server σε Virtualbox

9. Επιλέγουμε το format για τον εικονικό δίσκο που θα δημιουργήσουμε

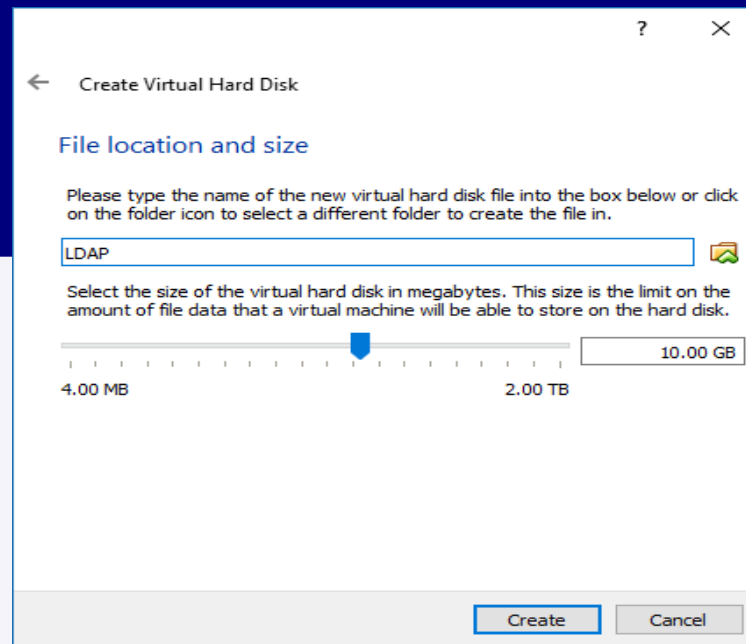
10. Επιλέγουμε τον τρόπο αποθήκευσης του δίσκου



Δημιουργία εργαστηριακού περιβάλλοντος (7)

Εγκατάσταση Ubuntu server σε Virtualbox

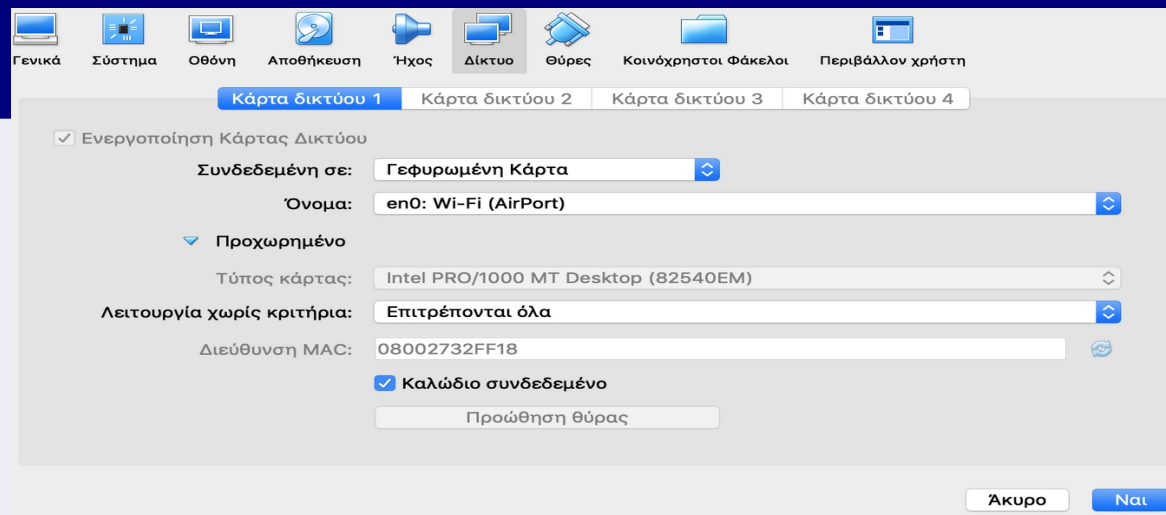
11. Επιλέγουμε τον χώρο αποθήκευσης για τον δίσκο και το μέγεθος του (προσοχή απαιτούνται τουλάχιστον 10gb)



Δημιουργία εργαστηριακού περιβάλλοντος (9)

Εγκατάσταση Ubuntu server σε Virtualbox

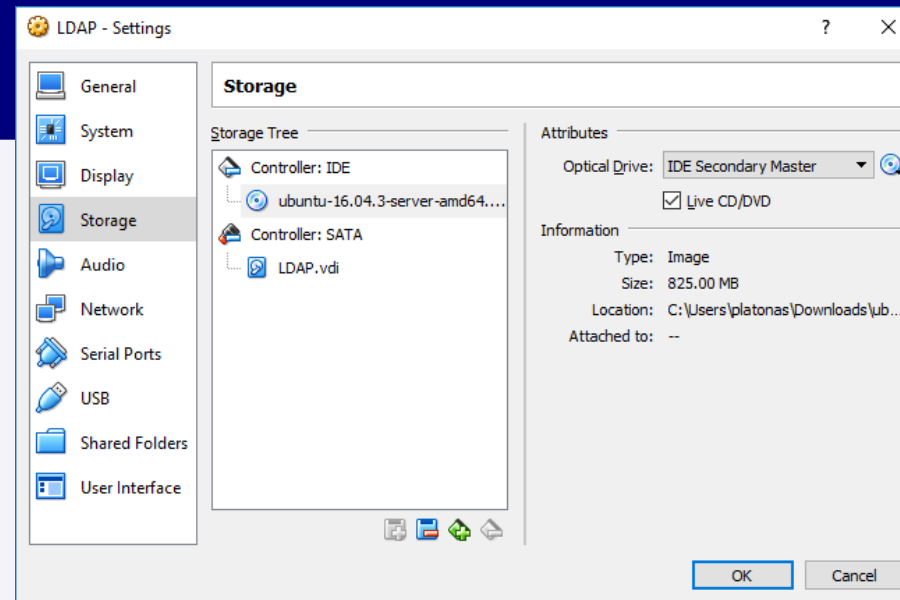
12. Επιλέγουμε από το μενού **Machine>Settings** και ενεργοποιούμε τους network adapters της στην καρτέλα network. Επιλέγουμε **Γεφυρωμένη Κάρτα (bridged adapter)**



Δημιουργία εργαστηριακού περιβάλλοντος (10)

Εγκατάσταση Ubuntu server σε Virtualbox

13. Επιλέγουμε από την καρτέλα storage το `ubuntu-16.04.3-server-amd64.iso` αρχείο (ή `ubuntu-16.04.5-desktop-amd64` αν θέλουμε την Desktop έκδοση) και το «φορτώνουμε» στο σύστημά μας ενεργοποιώντας και την επιλογή `Live CD/DVD`



Δημιουργία εργαστηριακού περιβάλλοντος (11)

Εγκατάσταση Ubuntu server σε Virtualbox

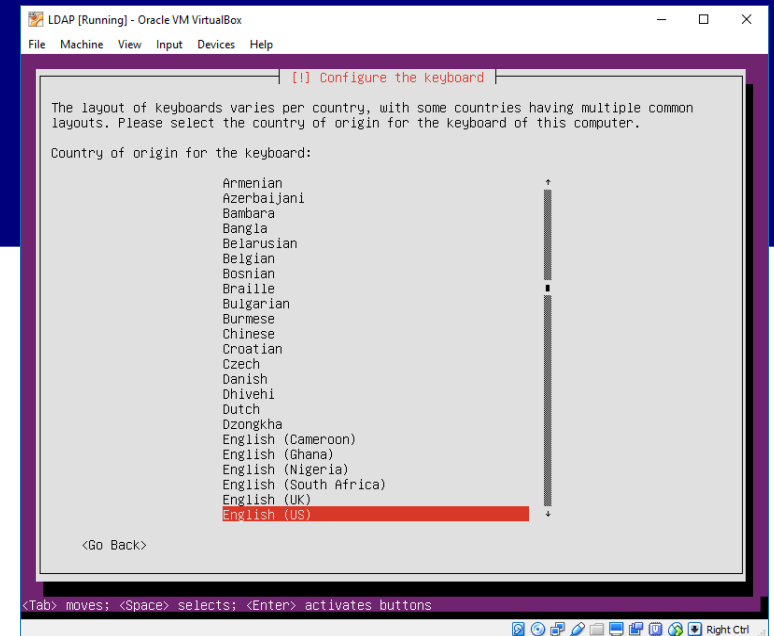
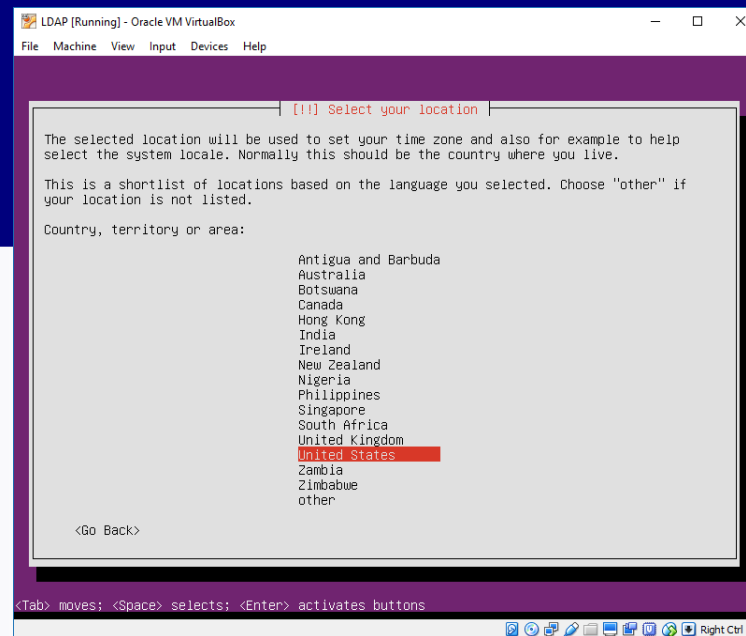
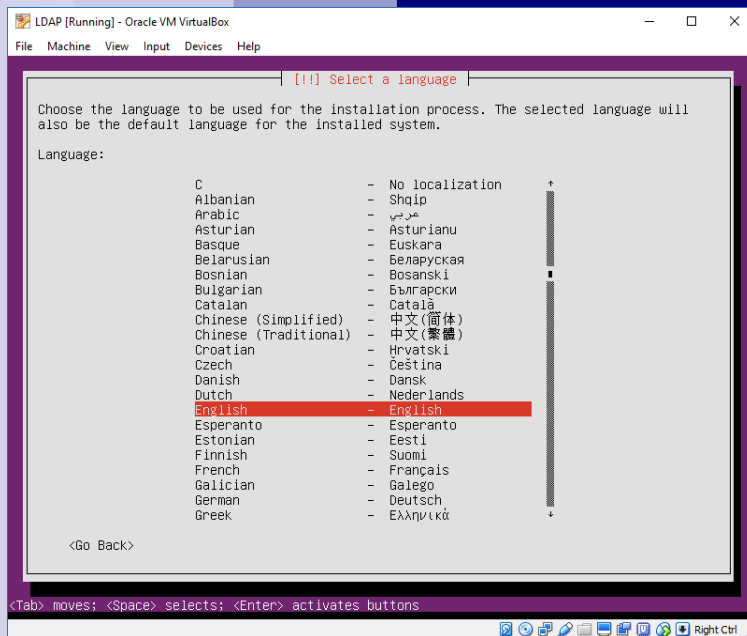
14. Επιλέγουμε από το μενού **Machine > Start** και κάνουμε εγκατάσταση τον Ubuntu server



Δημιουργία εργαστηριακού περιβάλλοντος (11)

Εγκατάσταση Ubuntu server σε Virtualbox

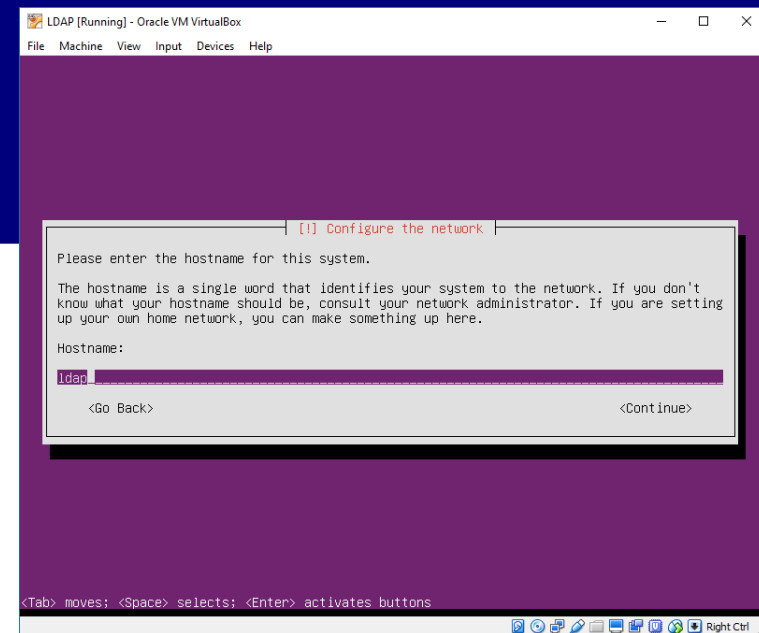
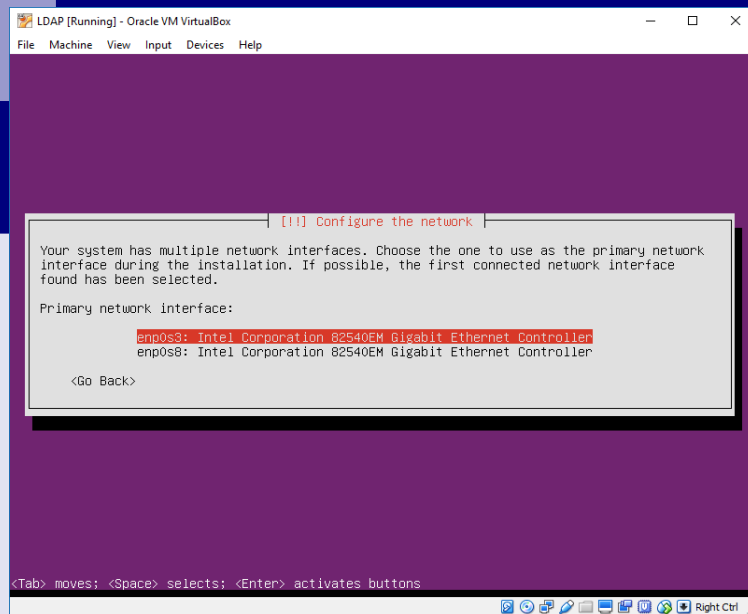
15. Επιλέγουμε γλώσσα, τοποθεσία και πληκτρολόγιο



Δημιουργία εργαστηριακού περιβάλλοντος (12)

Εγκατάσταση Ubuntu server σε Virtualbox

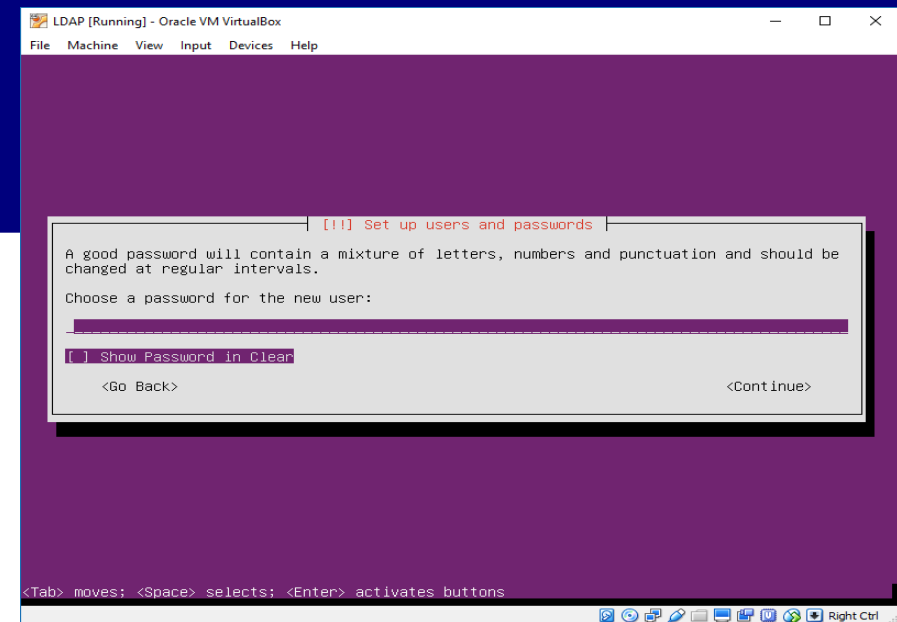
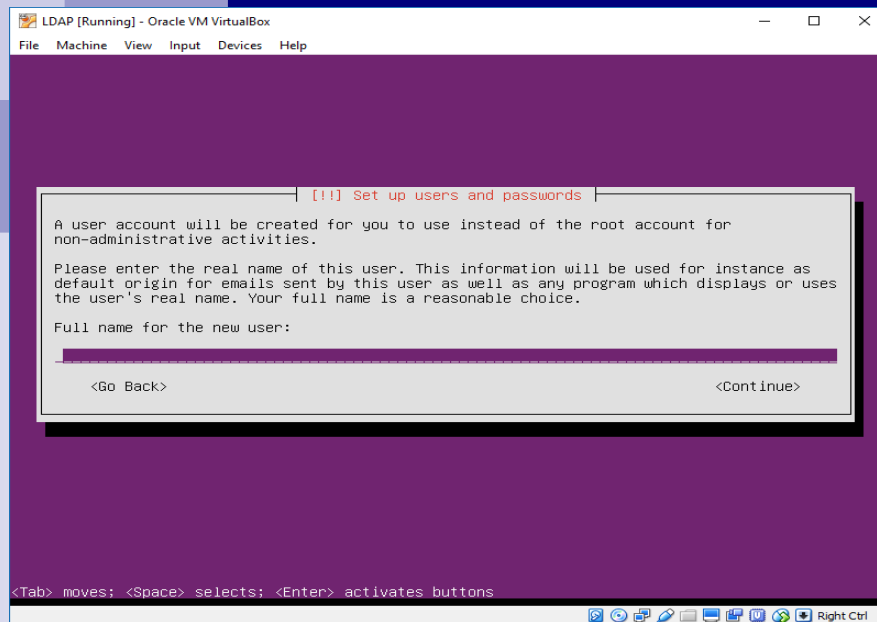
16. Επιλέγουμε την πρώτη κάρτα δικτύου με τον μεταφραστή διευθύνσεων δικτύου NAT και όνομα



Δημιουργία εργαστηριακού περιβάλλοντος (13)

Εγκατάσταση Ubuntu server σε Virtualbox

17. Επιλέγουμε το όνομα για τον χρήστη μας και επιλέγουμε συνθηματικό



Δημιουργία εργαστηριακού περιβάλλοντος (14)

Εγκατάσταση Ubuntu server σε Virtualbox

18. Στη συνέχεια κρυπτογραφούμε εφόσον θέλουμε τον home φάκελο μας, επιλέγουμε την time zone για το σύστημά μας και επιλέγουμε όλο τον δίσκο προς εγκατάσταση

```
[!!] Partition disks

Note that all data on the disk you select will be erased, but not before you have
confirmed that you really want to make the changes.

Select disk to partition:

SCSI3 (0,0,0) (sda) - 10.7 GB ATA VBOX HARDISK

<Go Back>
```

```
LDAP [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

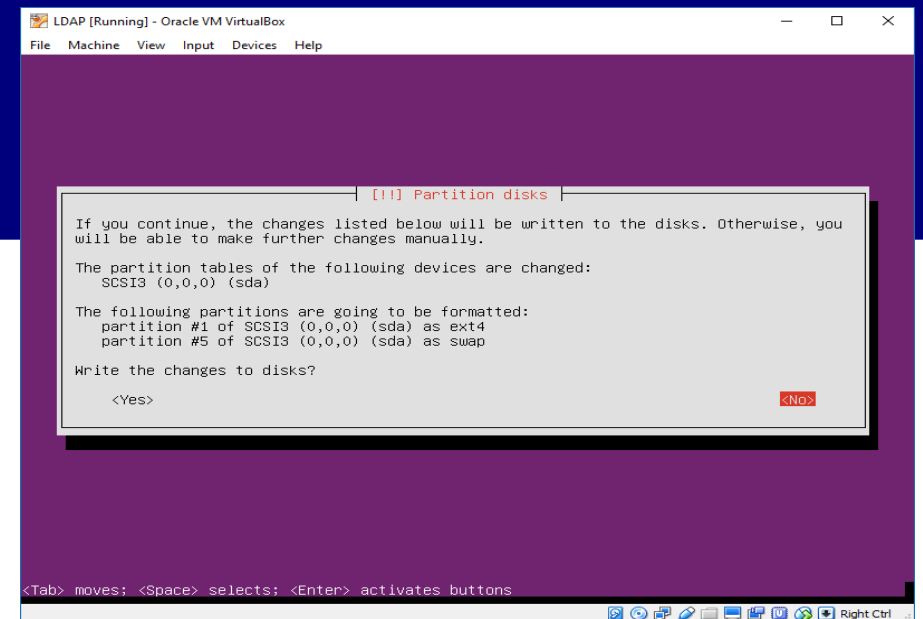
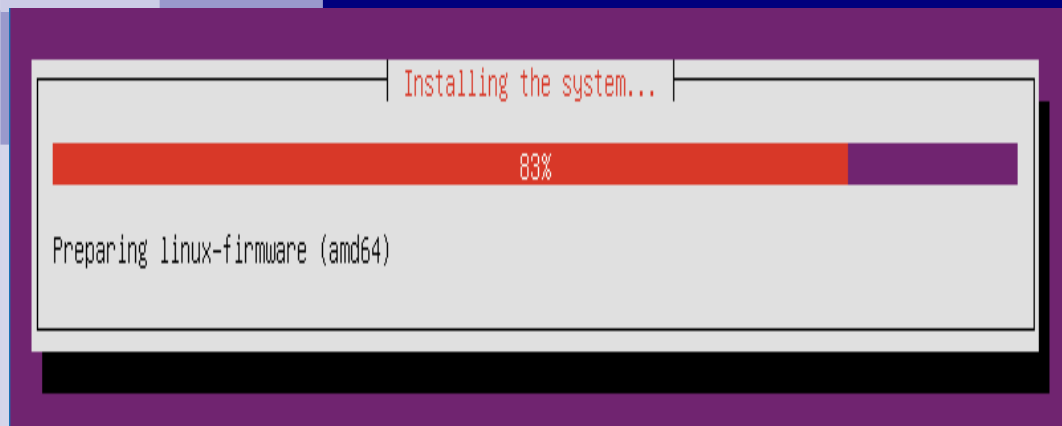
<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```


Δημιουργία εργαστηριακού περιβάλλοντος (15)

Εγκατάσταση Ubuntu server σε Virtualbox

19. Στη συνέχεια αποθηκεύουμε τις ρυθμίσεις του format στον δίσκο και κάνουμε εγκατάσταση στον δίσκο.



Δημιουργία εργαστηριακού περιβάλλοντος (16)

Εγκατάσταση Ubuntu server σε Virtualbox

20. Επιλέγουμε να κάνουμε εγκατάσταση αυτόματα το σύστημα με τις τελευταίες ενημερώσεις ασφαλείας
21. Δεν επιλέγουμε επιπρόσθετο software

```
[!] Software selection

At the moment, only the core of the system is installed. To tune the system to your
needs, you can choose to install one or more of the following predefined collections of
software.

Choose software to install:

[ ] Manual package selection
[ ] DNS server
[ ] LAMP server
[ ] Mail server
[ ] PostgreSQL database
[ ] Samba file server
[*] standard system utilities
[ ] Virtual Machine host
[ ] OpenSSH server

<Continue>
```

```
[!] Configuring tasksel

Applying updates on a frequent basis is an important part of keeping your system secure.

By default, updates need to be applied manually using package management tools.
Alternatively, you can choose to have this system automatically download and install
security updates, or you can choose to manage this system over the web as part of a group
of systems using Canonical's Landscape service.

How do you want to manage upgrades on this system?

No automatic updates
Install security updates automatically
Manage system with Landscape
```

Δημιουργία εργαστηριακού περιβάλλοντος (17)

Εγκατάσταση Ubuntu server σε Virtualbox

22. Εγκαθιστούμε τον bootloader Grub στον δίσκο μας έτσι ώστε να ξεκινάει το σύστημα μας αυτόματα

[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

<Go Back>

<Yes>

<No>

[!] Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

<Go Back>

<Continue>

Δημιουργία εργαστηριακού περιβάλλοντος (18)

Εγκατάσταση Ubuntu server σε Virtualbox

23. Κλείνουμε το virtual machine μας από το μενού και αφαιρούμε το iso αρχείο από τα settings της μηχανής μας στην καρτέλα storage

```
[!!] Finish the installation

Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove
the installation media (CD-ROM, floppies), so that you boot into the new system rather
than restarting the installation.

<Go Back>                                <Continue>
```

Εγκατάσταση του LDAP

Εγκατάσταση του LDAP σε Ubuntu server

1. Ενεργοποίηση των update για να έχουμε την τελευταία έκδοση του λογισμικού με την εντολή
`sudo apt-get update`
2. Εγκατάσταση του service του ldap μαζί με τα επιπρόσθετα utilities
`sudo apt-get install slapd ldap-utils`

```
ldap@ldap:~$ sudo apt-get update
Hit:1 http://security.ubuntu.com/ubuntu xenial-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Fetched 102 kB in 1s (81.3 kB/s)
Reading package lists... Done
ldap@ldap:~$ sudo apt-get install slapd ldap-utils
```



Ρύθμιση του LDAP (1)

- Εισαγωγή κωδικού για την υπηρεσία slapd
- Ρύθμιση της υπηρεσίας εκ νέου με την εντολή `sudo dpkg-reconfigure slapd`

```
Configuring slapd
Please enter the password for the admin entry in your LDAP directory.
Administrator password:
_____
<Ok>
```



Ρύθμιση του LDAP (2)

- Επιλέγουμε την δημιουργία ΒΔ
- Ορίζουμε DNS domain name και του οργανισμού

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

unipi

<Ok>

Configuring slapd

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

<Yes> <No>

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

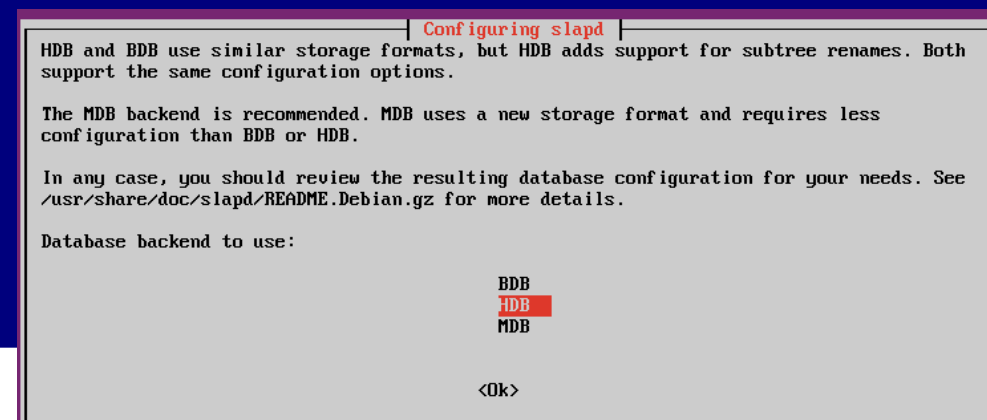
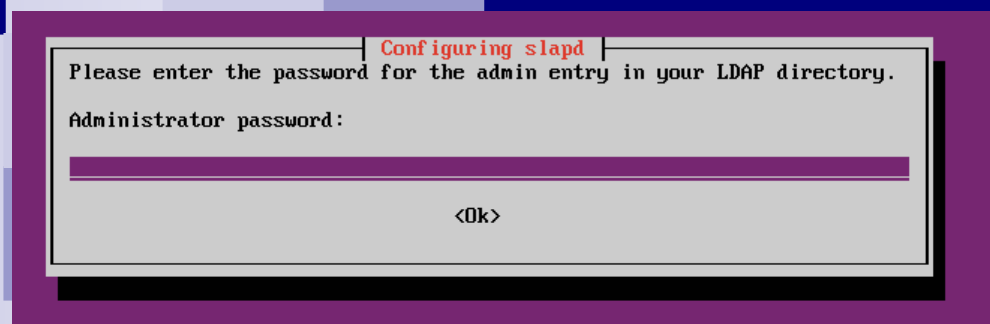
ldapsrvr.org

<Ok>



Ρύθμιση του LDAP (3)

- Εισάγουμε συνηματικό διαχειριστή, επιλέγουμε τύπο βάσης δεδομένων και μη κατάργηση της ΒΔ με τον τερματισμό της υπηρεσίας slapd





Ρύθμιση του LDAP (4)

- Μετακίνηση της παλιάς βάσης σε άλλο σημείο, άρνηση συμβατότητας με την παλιά έκδοση 2 του Idap

Configuring slapd

There are still files in `/var/lib/ldap` which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

<Yes> <No>

Configuring slapd

The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should upgrade to LDAPv3. If you have old programs which can't use LDAPv3, you should select this option and 'allow bind_v2' will be added to your slapd.conf file.

Allow LDAPv2 protocol?

<Yes> <No>

Εγκατάσταση του Phpldapadmin

- Εγκαθιστούμε τον phpldapadmin με την εντολή `sudo apt-get install phpldapadmin`

```
Machine View Input Devices Help  
ldap@ldap:~$ sudo apt-get install phpldapadmin
```



Ρύθμιση του PHPLdapadmin(1)

- Οι ρυθμίσεις του phpldapadmin θα γίνουν με την επεξεργασία του αρχείου config.php με την εντολή `sudo nano /etc/phpldapadmin/config.php` (ή με την εντολή `sudo gedit /etc/phpldapadmin/config.php` αν έχουμε εγκαταστήσει την Desktop έκδοση)
- Παραμετροποιούμε το αρχείο τοποθετώντας την τιμή για τον δικό μας DNS:

```
$ servers->setValue('server','base',array('dc=ldapserver,dc=org'));  
$servers->setValue('login','bind_id','cn=admin,dc=ldapserver,dc=org');  
$config->custom->appearance['hide_template_warning'] = true;
```



Ρύθμιση του PHPldapadmin(2)

Πληκτρολογώντας την εντολή `sudo nano /etc/ldap/ldap.conf` παραμετροποιούμε σωστά το αρχείο με βάση τις ρυθμίσεις μας:

```
GNU nano 2.5.3          File: /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE      dc=ldap,dc=com
URI       ldap://localhost:389
#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
```

Σύνδεση με τον RHPldapadmin (1)

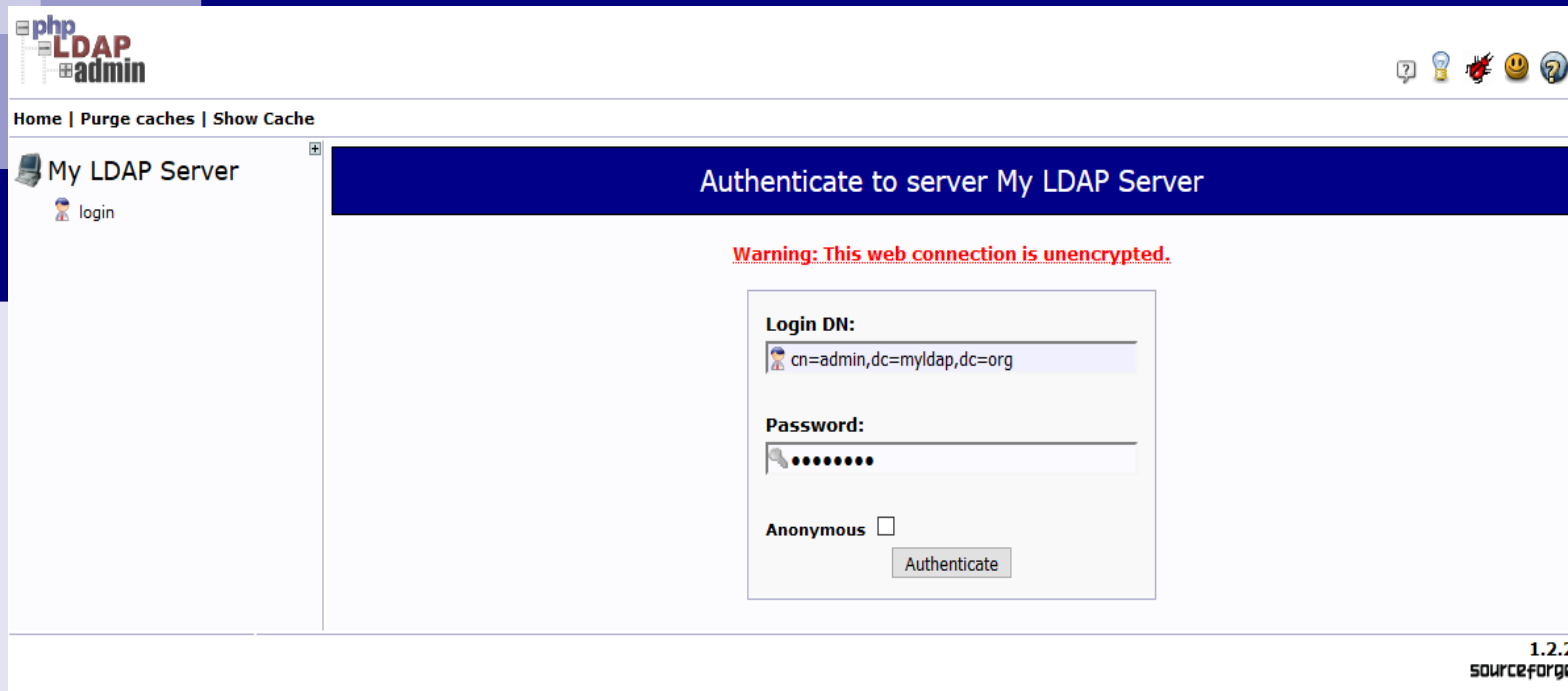
Πληκτρολογώντας την εντολή `ifconfig` μπορούμε να δούμε την ip που έχει ο server μας:

```
ldap@ldap-server:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:32:ff:18
        inet addr:192.168.2.61  Bcast:192.168.2.255  Mask:255.255.255.0
        inet6 addr: 2a02:85f:1f20:2d00:ed90:cb78:c160:7967/64  Scope:Global
        inet6 addr: fe80::daec:2dd4:ab99:69c9/64  Scope:Link
        inet6 addr: 2a02:85f:1f20:2d00:edd6:7710:e1b6:8037/64  Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:339 errors:0 dropped:0 overruns:0 frame:0
        TX packets:364 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:50645 (50.6 KB)  TX bytes:40708 (40.7 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:1776 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1776 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:136121 (136.1 KB)  TX bytes:136121 (136.1 KB)
```

Σύνδεση με τον PHPLdapadmin (2)

Μέσω του browser <http://192.168.2.61/phpldapadmin/> συνδεόμαστε στον ldap server απο τον client:



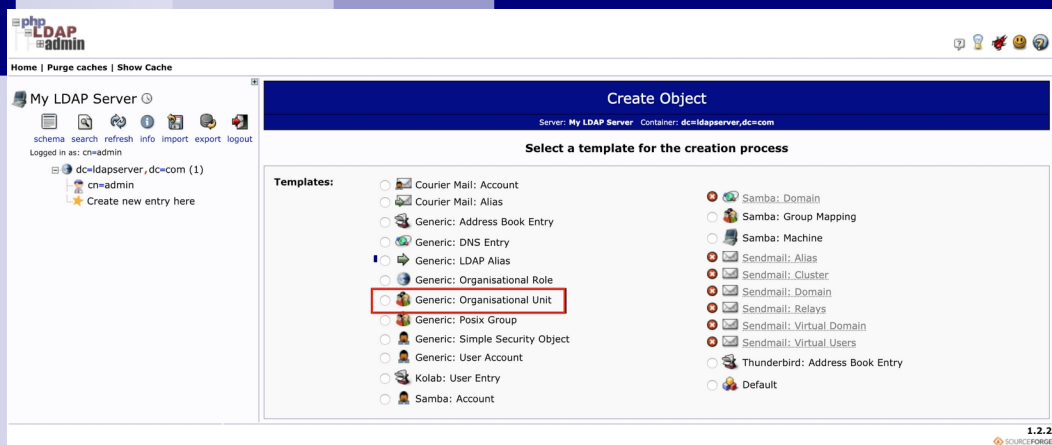
The screenshot displays the PHPLdapadmin web interface. The top navigation bar includes links for 'Home', 'Purge caches', and 'Show Cache'. The main content area is titled 'Authenticate to server My LDAP Server' and features a warning message: 'Warning: This web connection is unencrypted.' Below the warning is a form with the following fields:

- Login DN:** A text input field containing the value 'cn=admin,dc=myldap,dc=org'.
- Password:** A password input field with masked characters (dots).
- Anonymous:** A checkbox that is currently unchecked.
- Authenticate:** A button to submit the login information.

The bottom right corner of the interface shows the version '1.2.2' and the 'sourceforge' logo.

Δημιουργία χρηστών με τον PHPldapadmin

Επιλέγουμε Organisational Unit για να φτιάξουμε τις διαφορετικές κατηγορίες χρηστών:



The screenshot shows the 'Create Object' interface in PHPLDAPadmin. The server is 'My LDAP Server' and the container is 'dc=ldapserver,dc=com'. The user is logged in as 'cn=admin'. The 'Select a template for the creation process' section displays a list of templates. The 'Generic: Organisational Unit' template is highlighted with a red box.

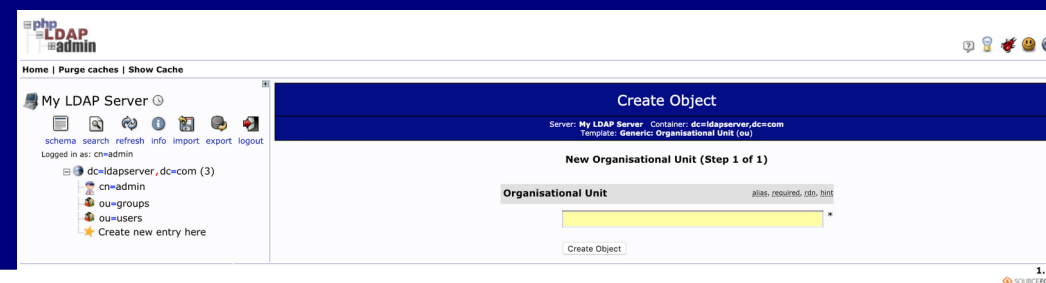
Server: My LDAP Server Container: dc=ldapserver,dc=com

Select a template for the creation process

Templates:

- Courier Mail: Account
- Courier Mail: Alias
- Generic: Address Book Entry
- Generic: DNS Entry
- Generic: LDAP Alias
- Generic: Organisational Role
- Generic: Organisational Unit
- Generic: Posix Group
- Generic: Simple Security Object
- Generic: User Account
- Kolab: User Entry
- Samba: Account
- Samba: Domain
- Samba: Group Mapping
- Samba: Machine
- Sendmail: Alias
- Sendmail: Cluster
- Sendmail: Domain
- Sendmail: Relays
- Sendmail: Virtual Domain
- Sendmail: Virtual Users
- Thunderbird: Address Book Entry
- Default

1.2.2 SOURCEFORGE



The screenshot shows the 'Create Object' interface in PHPLDAPadmin, specifically the 'New Organisational Unit (Step 1 of 1)' form. The server is 'My LDAP Server' and the container is 'dc=ldapserver,dc=com'. The user is logged in as 'cn=admin'. The form shows the 'Organisational Unit' field with a dropdown menu and a 'Create Object' button.

Server: My LDAP Server Container: dc=ldapserver,dc=com
Template: Generic: Organisational Unit (ou)

New Organisational Unit (Step 1 of 1)

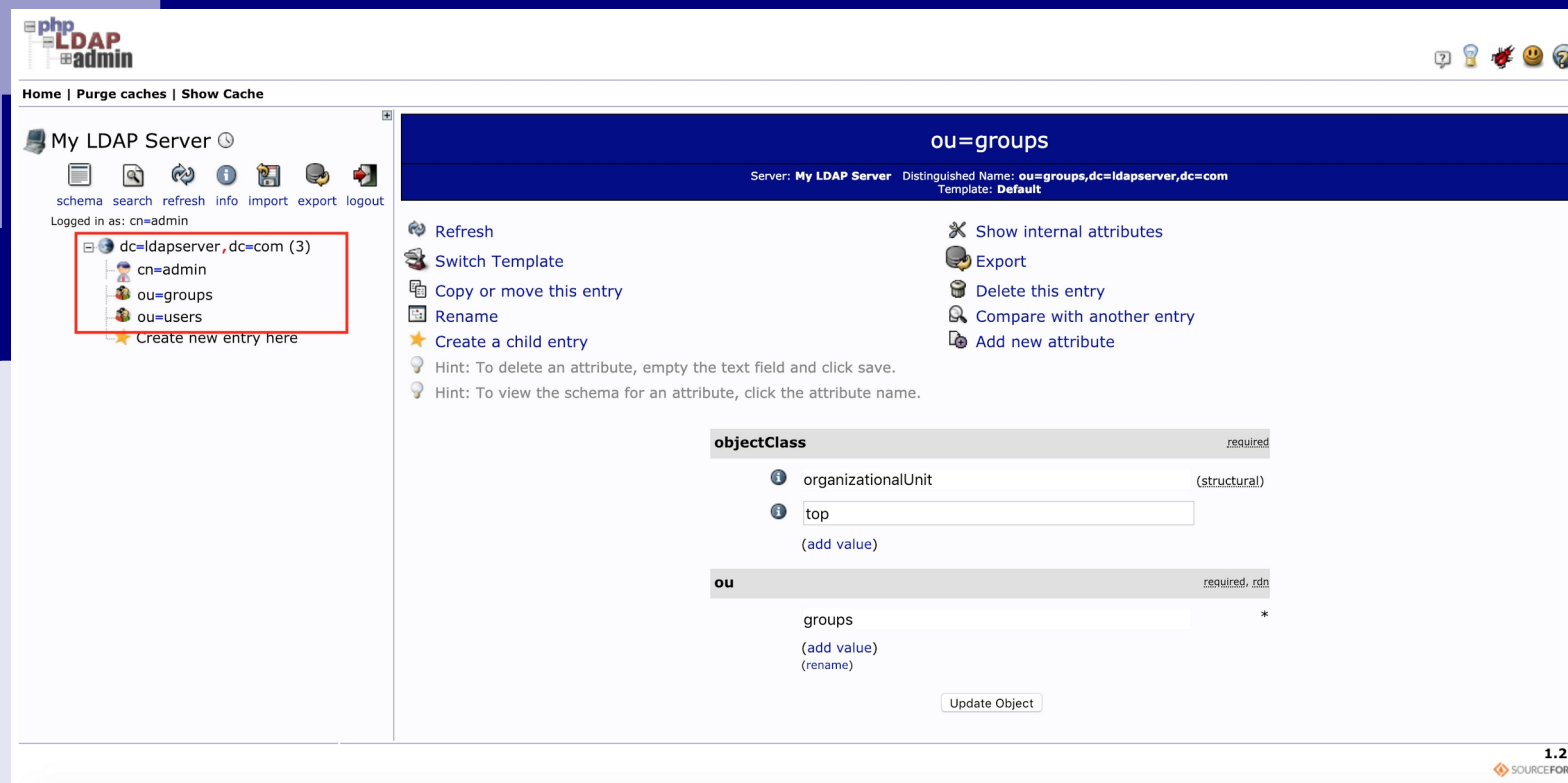
Organisational Unit

Create Object

1.2.2 SOURCEFORGE

Δημιουργία χρηστών με τον PHPldapadmin

Στη συνέχεια δημιουργούμε δύο ομάδες: το **groups** (στο οποίο θα φτιάξουμε τους διαφορετικούς ρόλους) και **users**.

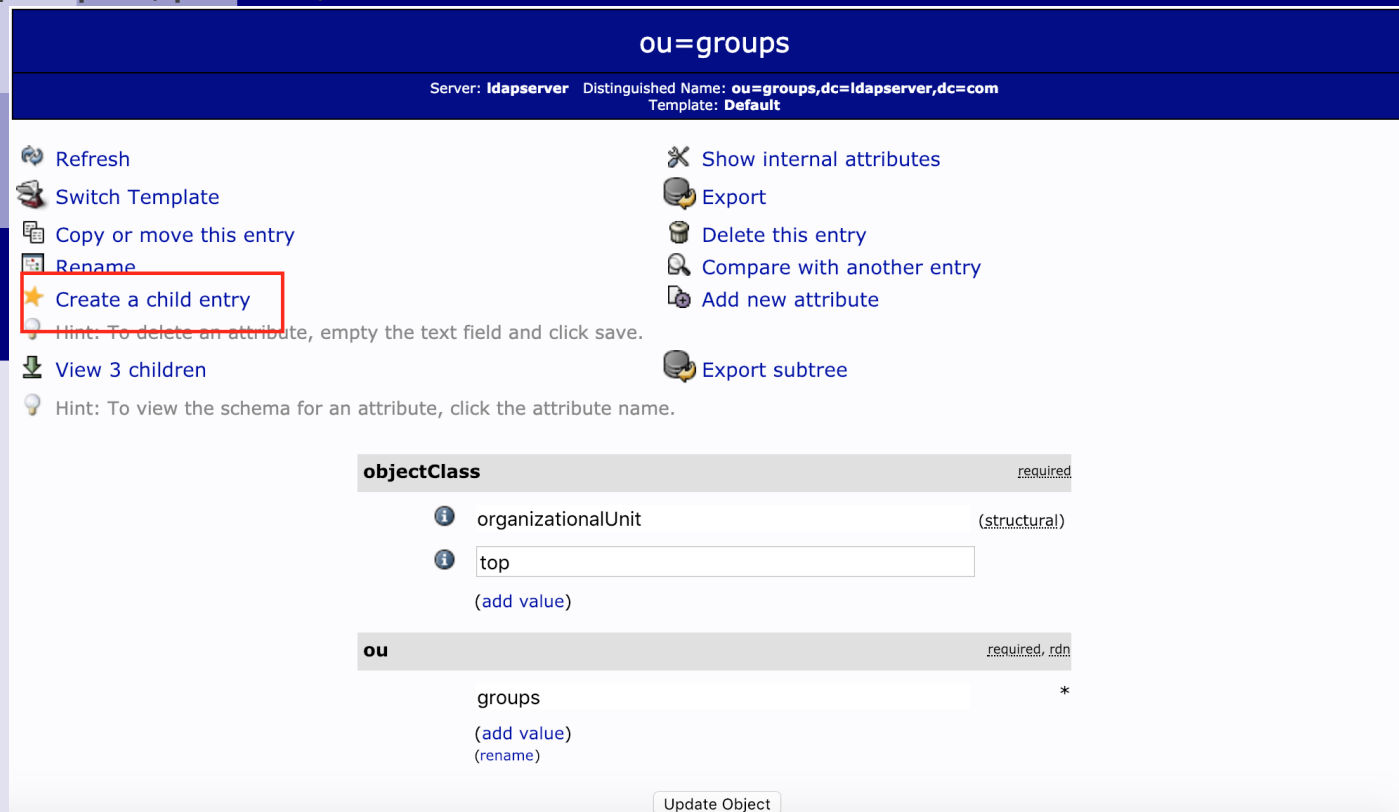


The screenshot shows the PHPLDAPadmin interface. On the left, a tree view of the LDAP directory is visible, with the entry `ou=groups` highlighted in a red box. The main area displays the configuration for the selected entry, `ou=groups`. The server is identified as `My LDAP Server` with a distinguished name of `ou=groups,dc=ldapservers,dc=com` and a default template. The interface includes a list of actions such as Refresh, Switch Template, Copy or move this entry, Rename, Create a child entry, Show internal attributes, Export, Delete this entry, Compare with another entry, and Add new attribute. The `objectClass` field is set to `organizationalUnit` (structural) and `top`. The `ou` field is set to `groups`. An `Update Object` button is located at the bottom right of the configuration area.

1.2.2
SOURCEFORGE

Δημιουργία χρηστών με τον PHPldapadmin

Μέσα στην ομάδα **groups** που δημιουργήσαμε προηγουμένως θα επιλέξουμε το **create a child entry** και θα φτιάξουμε τρεις ρόλους:



The screenshot shows the configuration page for the LDAP entry 'ou=groups'. The page title is 'ou=groups' and it includes server information: 'Server: ldapservers Distinguished Name: ou=groups,dc=ldapservers,dc=com' and 'Template: Default'. A list of actions is available on the left, with 'Create a child entry' highlighted by a red box. Below the actions, there are two sections for attribute configuration: 'objectClass' (required) and 'ou' (required, rdn). The 'objectClass' section has a dropdown menu with 'organizationalUnit' selected and 'top' entered in a text field. The 'ou' section has a dropdown menu with 'groups' selected. An 'Update Object' button is at the bottom.

ou=groups

Server: ldapservers Distinguished Name: ou=groups,dc=ldapservers,dc=com
Template: Default

- Refresh
- Switch Template
- Copy or move this entry
- Rename
- Create a child entry**
- Hint: To delete an attribute, empty the text field and click save.
- View 3 children
- Hint: To view the schema for an attribute, click the attribute name.
- Show internal attributes
- Export
- Delete this entry
- Compare with another entry
- Add new attribute
- Export subtree

objectClass required

- organizationalUnit (structural)
- top (add value)

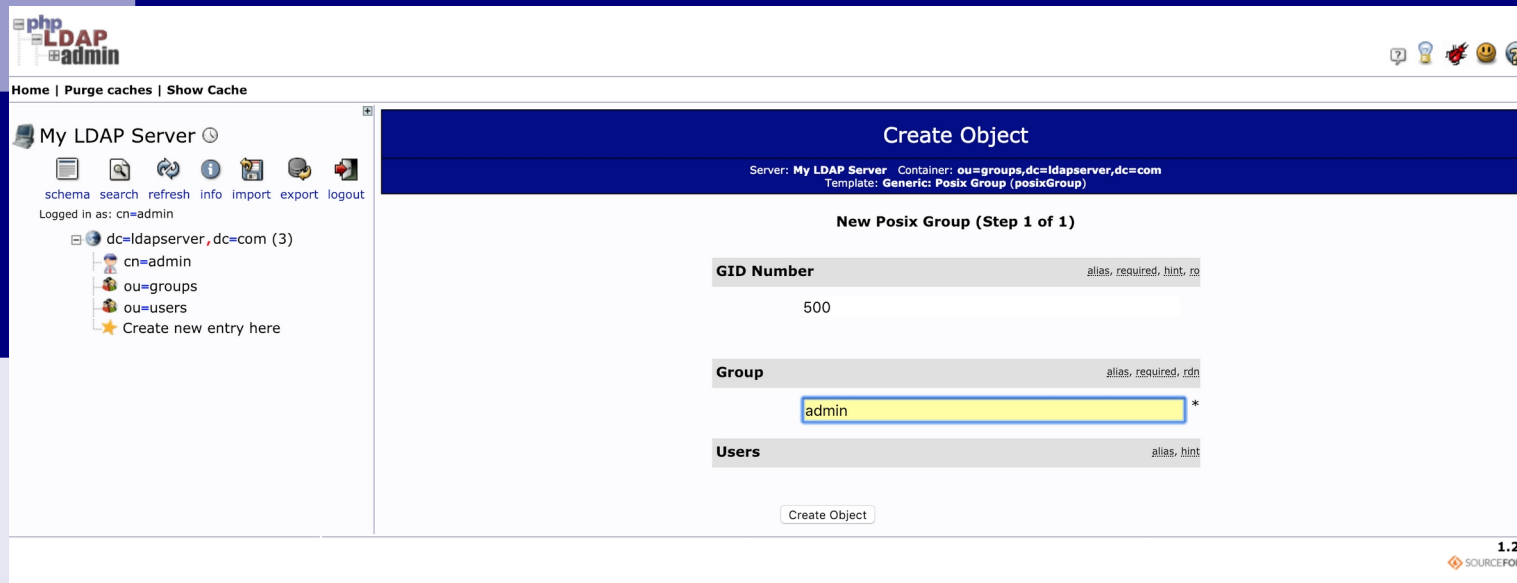
ou required, rdn

- groups *
- (add value)
- (rename)

Update Object

Δημιουργία χρηστών με τον PHPldapadmin

Με αυτό τον τρόπο θα δημιουργήσουμε τους διαφορετικούς ρόλους χρηστών:



The screenshot displays the PHPLDAPadmin web interface. The main content area is titled "Create Object" and shows the configuration for a "New Posix Group (Step 1 of 1)". The server is identified as "My LDAP Server" with the container "ou=groups,dc=ldapservers,dc=com". The template used is "Generic: Posix Group (posixGroup)".

The form fields are as follows:

- GID Number:** 500 (with hints: alias, required, hint, ro)
- Group:** admin (with hints: alias, required, rdn)
- Users:** (with hints: alias, hint)

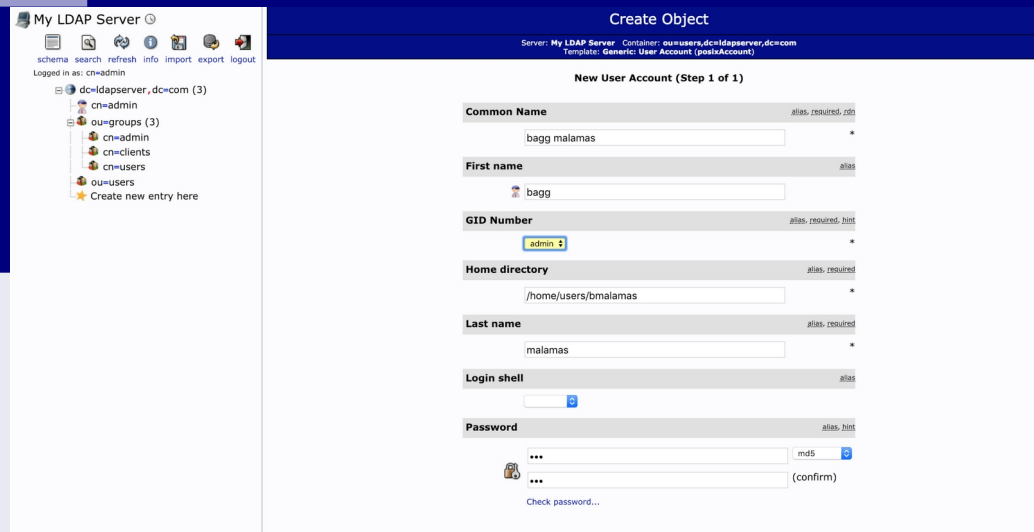
A "Create Object" button is located at the bottom of the form. The left sidebar shows a tree view of the LDAP directory structure, including "dc=ldapservers,dc=com (3)", "cn=admin", "ou=groups", and "ou=users".

1.2.2
SOURCEFORGE

Δημιουργία χρηστών με τον PHPIdpadmin

Αφού φτιάξουμε τους διαφορετικούς ρόλους - προχωράμε στην δημιουργία χρηστών και τους αποδίδουμε κάποιο ρόλο επιλέγοντας στο `ou = users` to **create a child entry** και στη συνέχεια **user account**.

Συμπληρώνουμε τα στοιχεία:

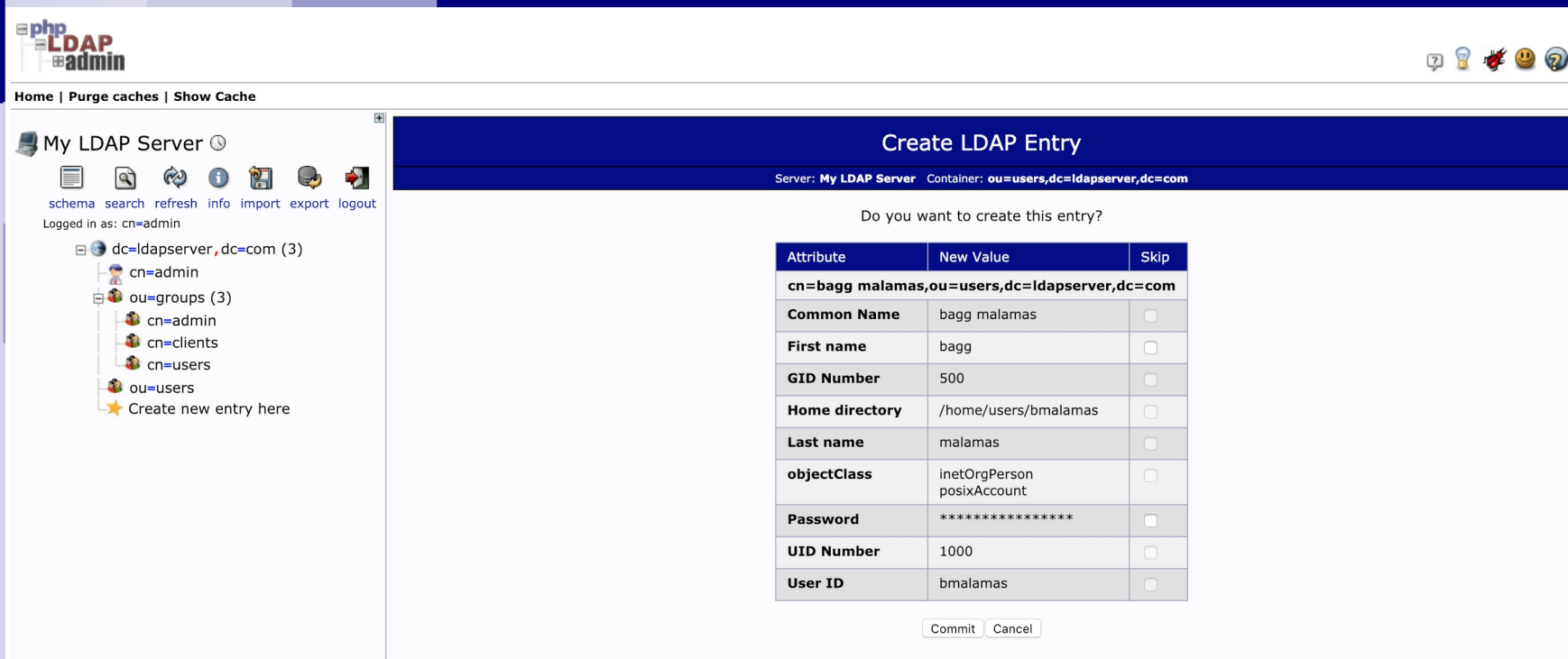


The screenshot displays the PHPIdpadmin web interface. On the left, the 'My LDAP Server' tree shows the hierarchy: `dc=ldapservers,dc=com` (3) containing `cn=admin`, `ou=groups` (3) containing `cn=admin`, `cn=clients`, and `cn=users`, and `ou=users`. A 'Create new entry here' link is visible under `ou=users`. The main area is titled 'Create Object' and shows the 'New User Account (Step 1 of 1)' form. The form fields are: Common Name (bagg malamas), First name (bagg), GID Number (admin), Home directory (/home/users/bmalamas), Last name (malamas), Login shell (empty), and Password (with md5 and confirm options).

(προσοχή: καλό θα ήταν να μην αφήνουμε κενά)

Δημιουργία χρηστών με τον PHPldapadmin

Επιλέγοντας **commit** ένας νέος χρήστης θα δημιουργηθεί:



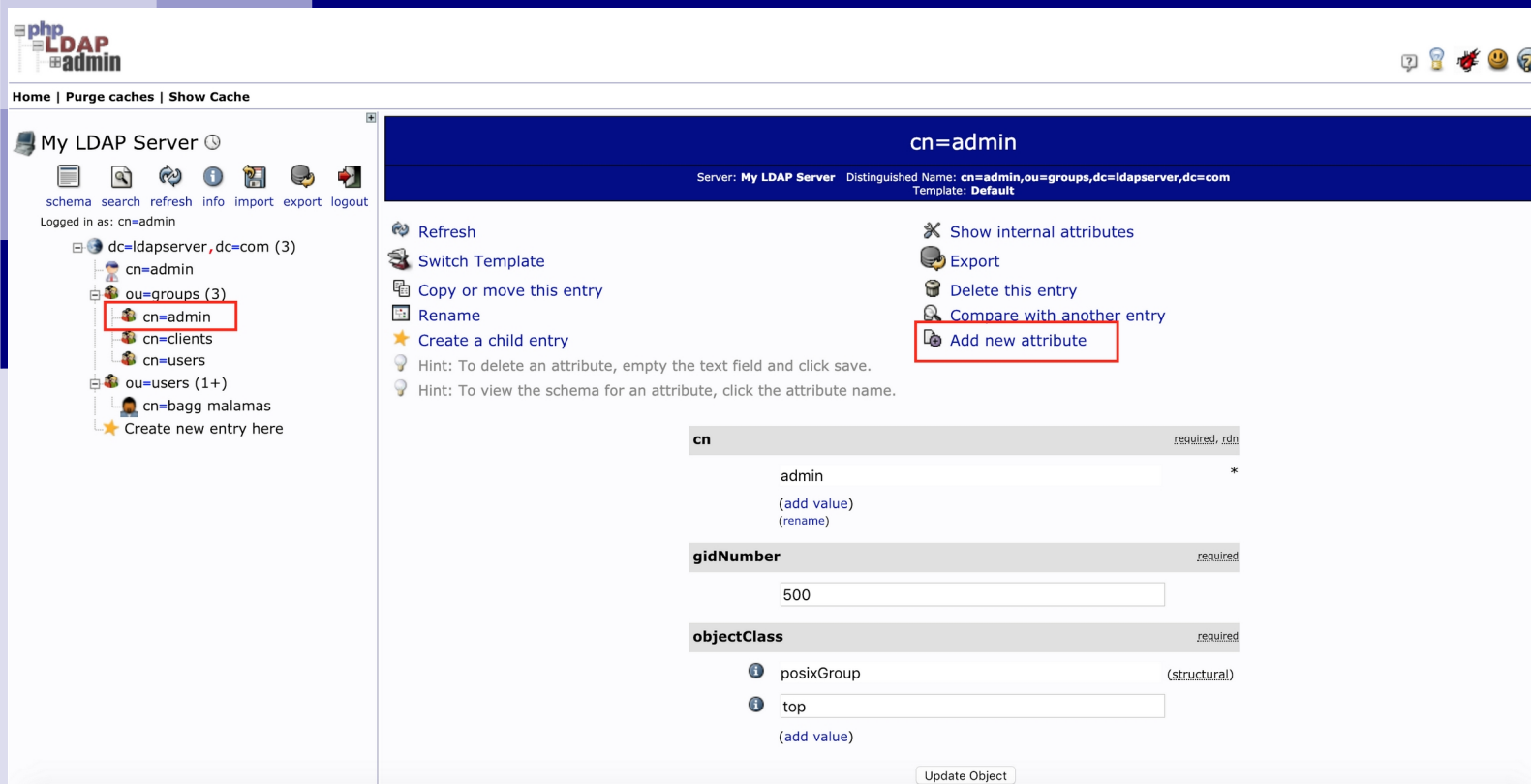
The screenshot shows the PHPLDAPadmin web interface. The main heading is "Create LDAP Entry". Below the heading, it displays "Server: My LDAP Server" and "Container: ou=users,dc=ldapserver,dc=com". A confirmation message asks "Do you want to create this entry?". A table lists the attributes and their values for the new entry:

Attribute	New Value	Skip
cn=bagg malamas,ou=users,dc=ldapserver,dc=com		
Common Name	bagg malamas	<input type="checkbox"/>
First name	bagg	<input type="checkbox"/>
GID Number	500	<input type="checkbox"/>
Home directory	/home/users/bmalamas	<input type="checkbox"/>
Last name	malamas	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1000	<input type="checkbox"/>
User ID	bmalamas	<input type="checkbox"/>

At the bottom of the form, there are "Commit" and "Cancel" buttons.

Δημιουργία χρηστών με τον PHPLDAPadmin

Στη συνέχεια εντάσσουμε τον χρήστη που φτιάξαμε στο γκρούπ των admin επιλέγοντας **add new attribute**:



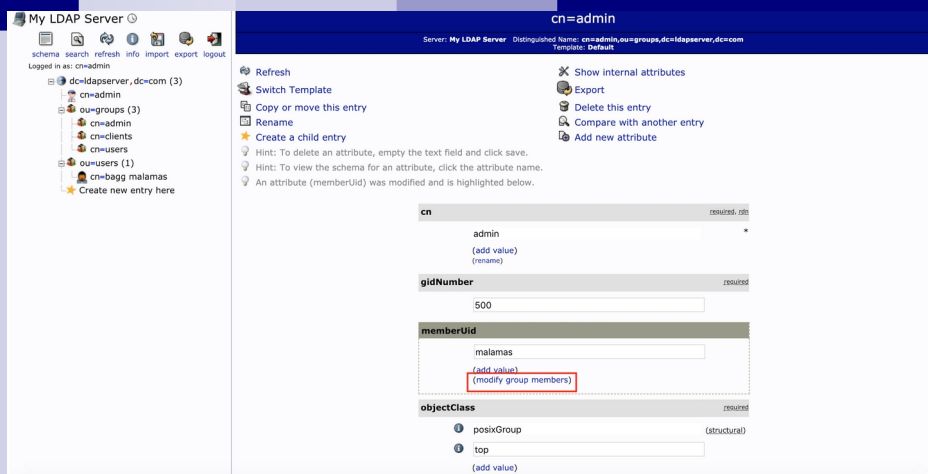
The screenshot shows the PHPLDAPadmin interface. On the left, a tree view shows the LDAP hierarchy: `dc=ldapserver,dc=com` (3) containing `cn=admin`, `ou=groups` (3) containing `cn=admin` (highlighted with a red box), `cn=clients`, and `cn=users`; `ou=users` (1+) containing `cn=bagg malamas`; and a "Create new entry here" option. The main area displays the configuration for the selected entry `cn=admin`. The distinguished name is `cn=admin,ou=groups,dc=ldapserver,dc=com`. A list of actions is shown, with "Add new attribute" highlighted by a red box. Below, the attribute configuration is shown:

- cn** (required, rdn): Value `admin`. Includes "(add value)" and "(rename)" links.
- gidNumber** (required): Value `500`.
- objectClass** (required): Includes `posixGroup` (structural) and `top`. Includes "(add value)" link.

An "Update Object" button is at the bottom.

Δημιουργία χρηστών με τον PHPldapadmin

Ο χρήστης εντάχθηκε στο group όπως μπορούμε εύκολα να διαπιστώσουμε επιλέγοντας **modify group members**:



My LDAP Server

Server: My LDAP Server Distinguished Name: cn=admin,ou=groups,dc=ldapserver,dc=com Template: Default

Logged in as: cn=admin

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

cn

admin

gidNumber

500

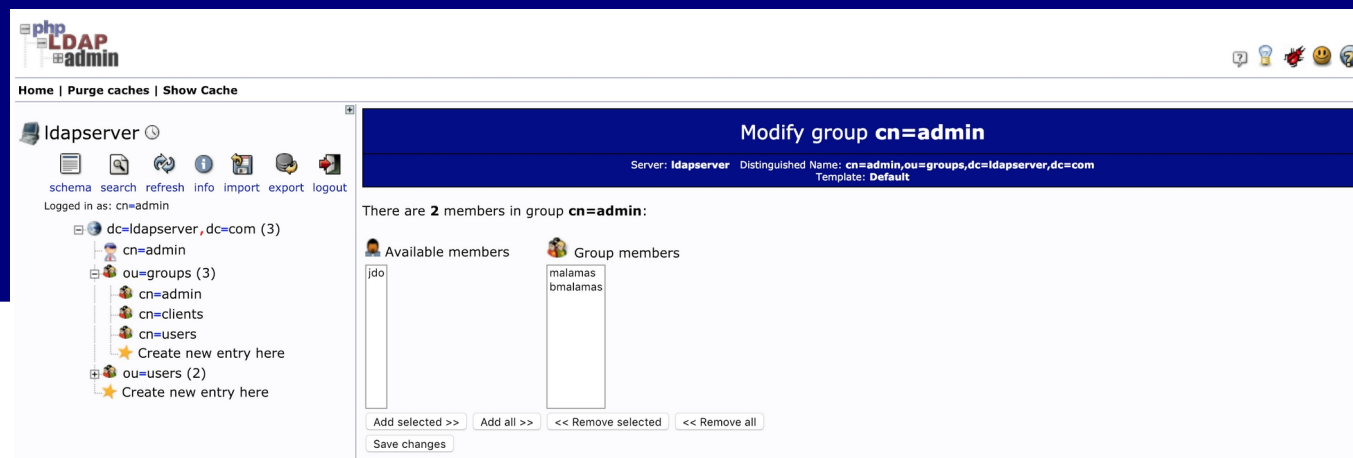
memberUid

malamas

objectClass

posixGroup

top



phpLDAPadmin

Home | Purge caches | Show Cache

ldapservers

Server: ldapserver Distinguished Name: cn=admin,ou=groups,dc=ldapserver,dc=com Template: Default

Logged in as: cn=admin

There are 2 members in group **cn=admin**:

Available members

Group members

malamas

bmalamas

Add selected >> Add all >> << Remove selected << Remove all

Save changes

Εντολές ενεργειών στον LDAP - αρχεία LDIF (Data Interchange Format)

Οι προηγούμενες ενέργειες μπορούν να πραγματοποιηθούν και με την χρήση εντολών:

Προσθήκη εγγραφής

```
ldapadd -f /tmp/entrymods (έστω ότι υπάρχει το αρχείο /tmp/entrymods)
```

Τροποποίηση εγγραφής

```
ldapmodify -b -r -f /tmp/entrymods
```

Διαγραφή εγγραφής

```
ldapdelete 'cn=Luiz Malere,o=TUDeft,c=NL'
```

Αναζήτηση εγγραφής

```
ldapsearch -b 'o=TUDeft,c=NL' 'cn=Rene van Leuken'
```



Παράδειγμα δομής ενός αρχείου LDIF

```
# occurrences of the default suffix "dc=yourco,dc=com" with the suffix  
# that your LDAP server is configured for
```

```
dn: dc=denver,dc=ldap,dc=com  
objectclass: domain  
objectclass: top
```

```
# Add lines according to this scheme that correspond to your suffix
```

```
dc: dc=denver,dc=ldap,dc=com  
dn: cn=users,dc=denver,dc=ldap,dc=com  
objectclass: container  
objectclass: top  
cn: users  
dn: cn=groups,dc=denver,dc=ldap,dc=com  
objectclass: top  
objectclass: container  
cn: groups
```


Δημιουργία ενός LDIF αρχείου και εισαγωγή στον LDAP

Δημιουργία ενός ldif αρχείο με ονομασία newgroups και προσθήκη στον LDAP server

```
ldapadd -x -D "cn=admin,dc=ldap,dc=com" -w password -H ldap:// -f newgroups.ldif
```

Τροποποίηση εγγραφών που υπάρχουν ήδη στον LDAP server

```
ldapmodify -a -x -D "cn=admin,dc=example,dc=com" -w password -H ldap:// -f newgroups.ldif
```

Μέσα σε ένα αρχείο ldif μπορούν να γίνονται πολλαπλές αλλαγές όπως προσθήκη χρηστών, γκρούπ ή χαρακτηριστικών,

μεταβολές σε υπάρχουσες εγγραφές κλπ:

```
Οι αλλαγές δηλώνονται μέσα στο αρχείο ακριβώς κάτω απο το dn  
dn: uid=jsmith1,ou=People,dc=example,dc=com  
changetype: modify  
delete: description
```

Προσοχή μεταξύ δύο διαφορετικών ενεργειών μέσα σε ένα ldif αρχείο μεσολαβεί μια κενή γραμμή

Παράδειγμα σύνδεσης PHP και LDAP

```
<?php $ldap_dn = "cn=admin,dc=ldapserver,dc=org"; $ldap_password = "*****";  
$ldaptree = "OU=Managers,DC=ldapserver,DC=org";  
$ldapconn = ldap_connect("192.168.2.53");  
ldap_set_option($ldapconn, LDAP_OPT_PROTOCOL_VERSION, 3);  
$result=ldap_bind($ldapconn, $ldap_dn, $ldap_password);  
if($result) { $search = ldap_search($ldapconn,$ldaptree, "(cn=*)") or die ("Error"); $data =  
ldap_get_entries($ldapconn, $search);  
print_r($data);  
} else {echo "Invalid user/pass or other errors!";} ?>
```

Παράδειγμα σύνδεσης Tomcat και LDAP

```
<Realm className="org.apache.catalina.realm.JNDIRealm"  
connectionURL="ldap://localhost:389"  
userPattern="uid={0},ou=people,dc=mycompany,dc=com"  
roleBase="ou=groups,dc=mycompany,dc=com"  
roleName="cn"  
roleSearch="(uniqueMember={0})"  
>
```

Περισσότερα στον σύνδεσμο:

<http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/index.html>

<http://tomcat.apache.org/tomcat-7.0-doc/realms-howto.html>

<https://www.javacodegeeks.com/2015/09/java-to-ldap-tutorial-including-how-to-install-an-ldap-server-client.html>



Χρήσιμες πηγές

Σχετικά με την εγκατάσταση

- YoLinux.com (<http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP.html>)
- <http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/index.html>
- <http://tomcat.apache.org/tomcat-7.0-doc/realm-howto.html>
- <https://www.javacodegeeks.com/2015/09/java-to-ldap-tutorial-including-how-to-install-an-ldap-server-client.html>