ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριακών Συστημάτων

«Αυθεντικοποίηση και Εξουσιοδότηση – Παράδειγμα ελέγχου πρόσβασης με openldap»

Τμήμα Πληροφορικής

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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Περιεχόμενα

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

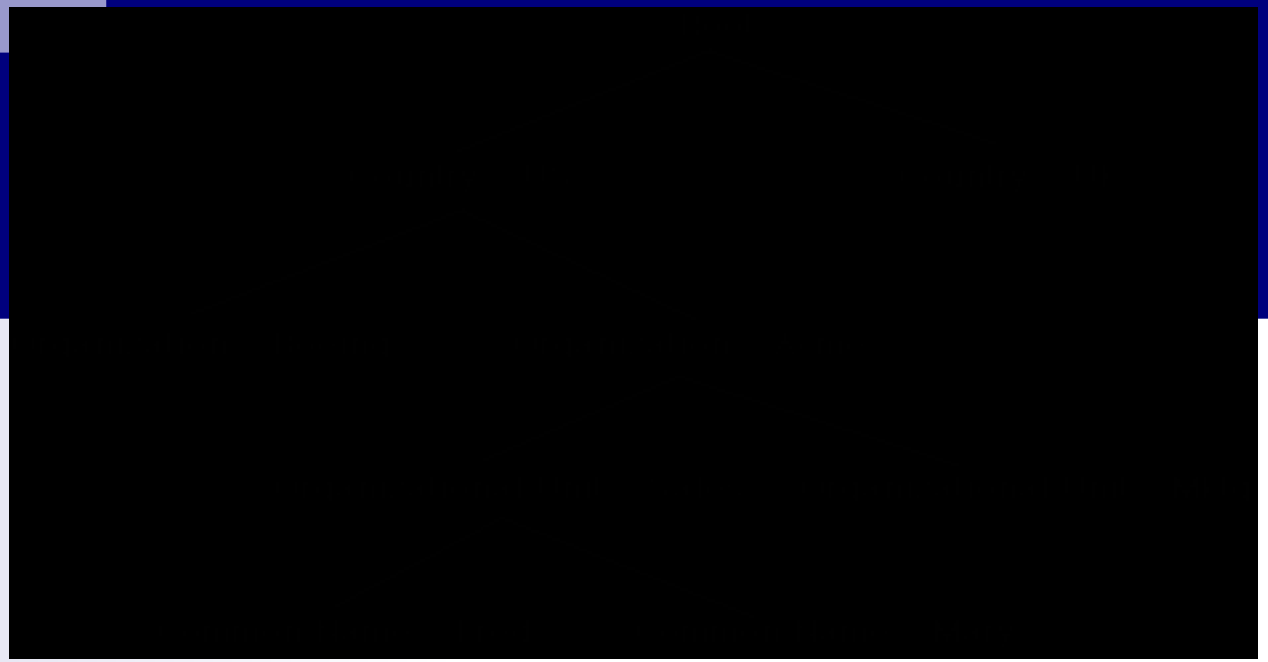
Εισαγωγή (2) - γενικά για το LDAP

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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

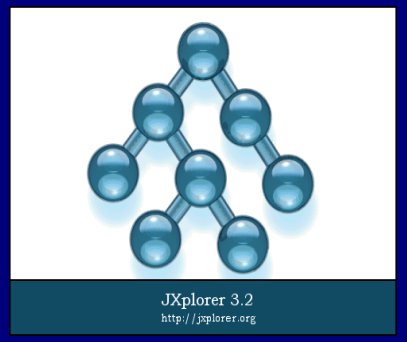
Εισαγωγή (6) - Η λειτουργία του LDAP

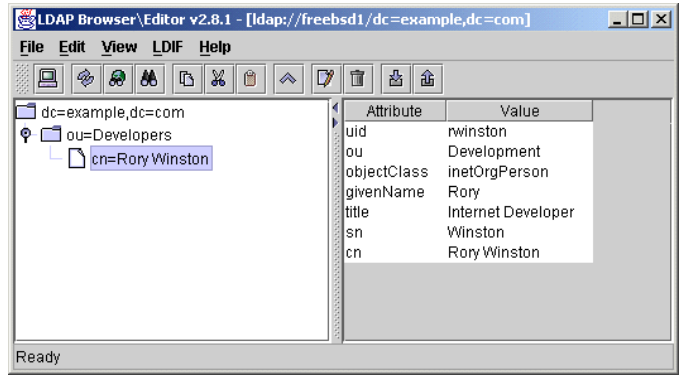
- Η υπηρεσία καταλόγου LDAP [OpenLDAP] είναι βασισμένη στο μοντέλο επικοινωνίας πελάτη-εξυπηρετητή.
- Ένας ή περισσότεροι κεντρικοί υπολογιστές LDAP περιέχουν τα δεδομένα που αποτελούν το δέντρο πληροφοριών καταλόγου
  (Directory Information Tree –DIT)
- Ο κεντρικός υπολογιστής αποκρίνεται με μια απάντηση 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





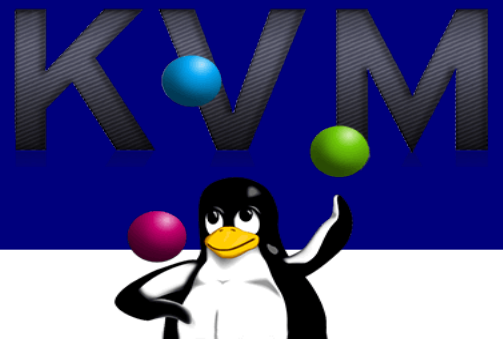
Δημιουργία εργαστηριακού περιβάλλοντος (1)

Επιλογή έκδοσης Linux server

Το λειτουργικό στο οποίο θα «τρέξει» ο LDAP server

Δημιουργία εργαστηριακού περιβάλλοντος (2)

Επιλογή λογισμικού για Virtualization

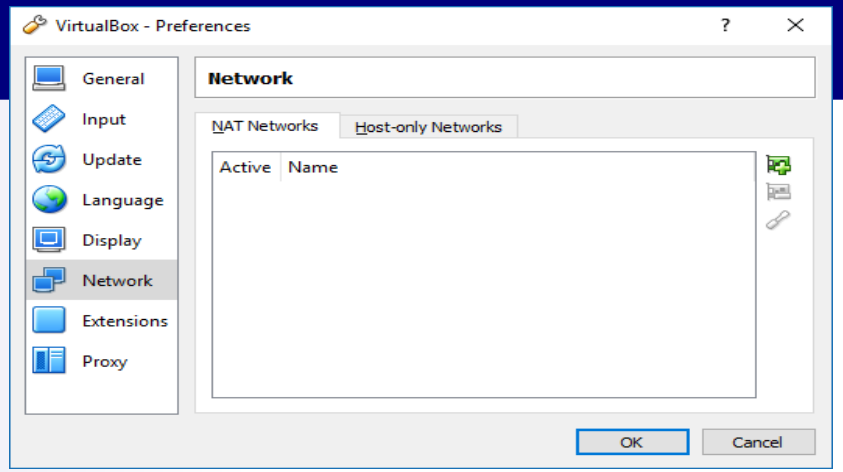


Για να μπορέσουμε να τρέξουμε παράλληλα το λειτουργικό του server

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 απο το μενού του virtualbox File>Preferences την καρτέλα Network

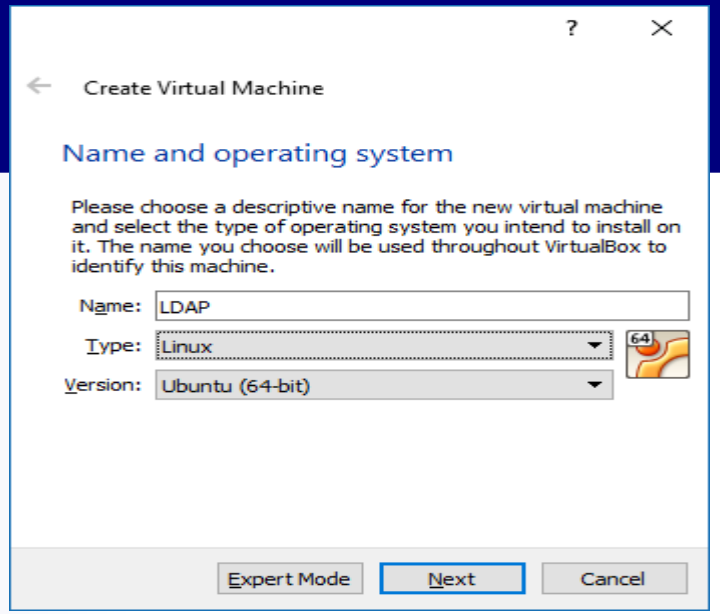


Δημιουργία εργαστηριακού περιβάλλοντος (4)

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

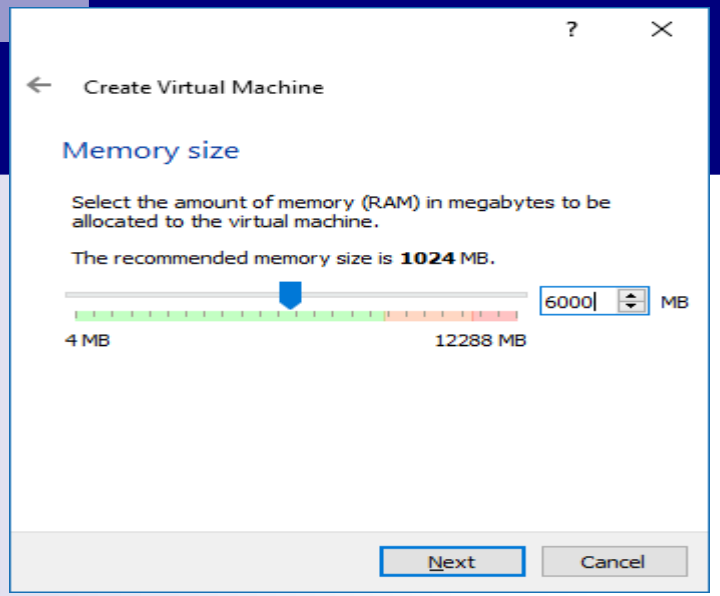


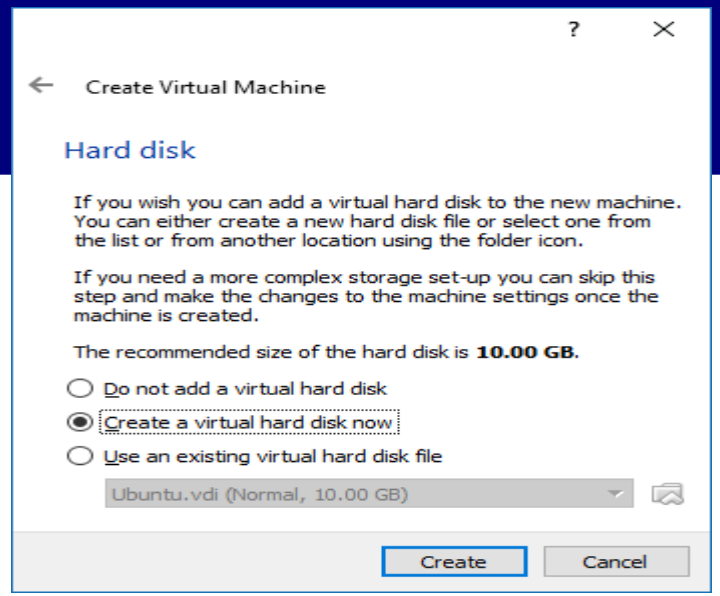
Δημιουργία εργαστηριακού περιβάλλοντος (5)

Εγκατάσταση Ubuntu server σε Virtualbox

7. Επιλέγουμε την ram που θα διαθέσουμε

8. Επιλέγουμε την χωρητικότητα του δίσκου που θα διαθέσουμε



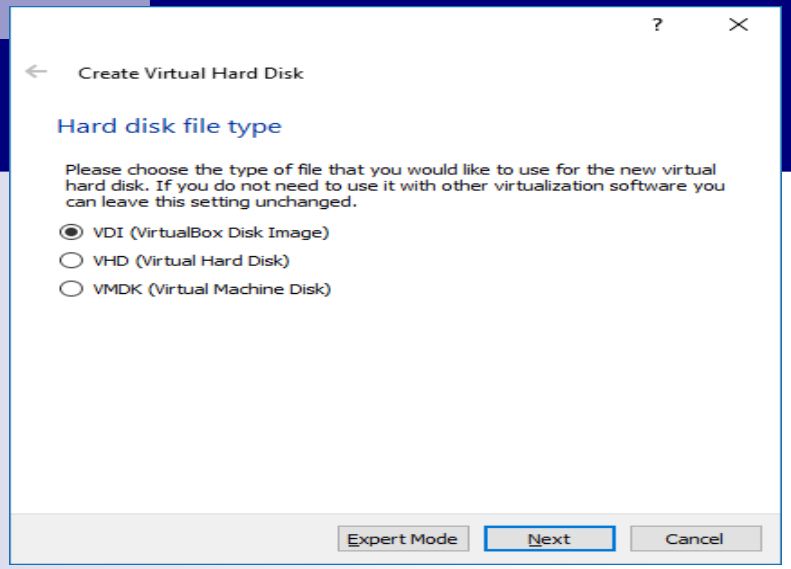


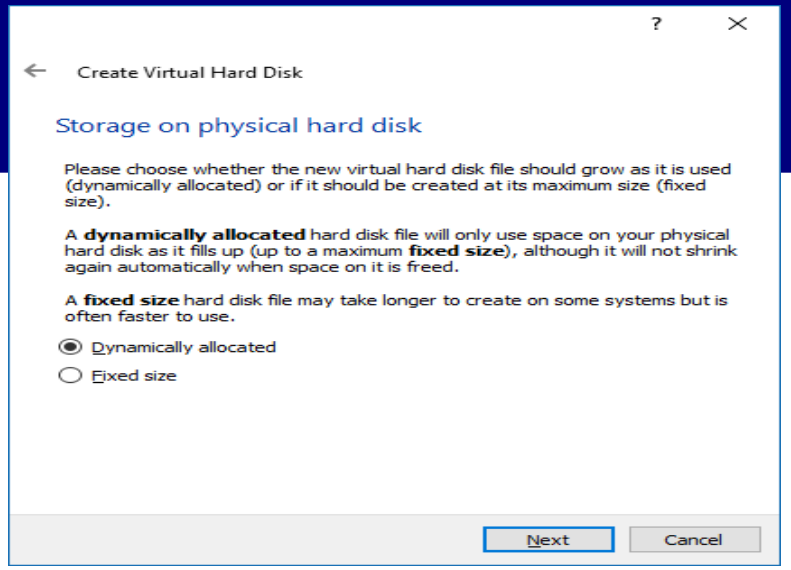
Δημιουργία εργαστηριακού περιβάλλοντος (6)

Εγκατάσταση Ubuntu server σε Virtualbox

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

10. Επιλέγουμε τον τρόπο αποθήκευσης του δίσκου

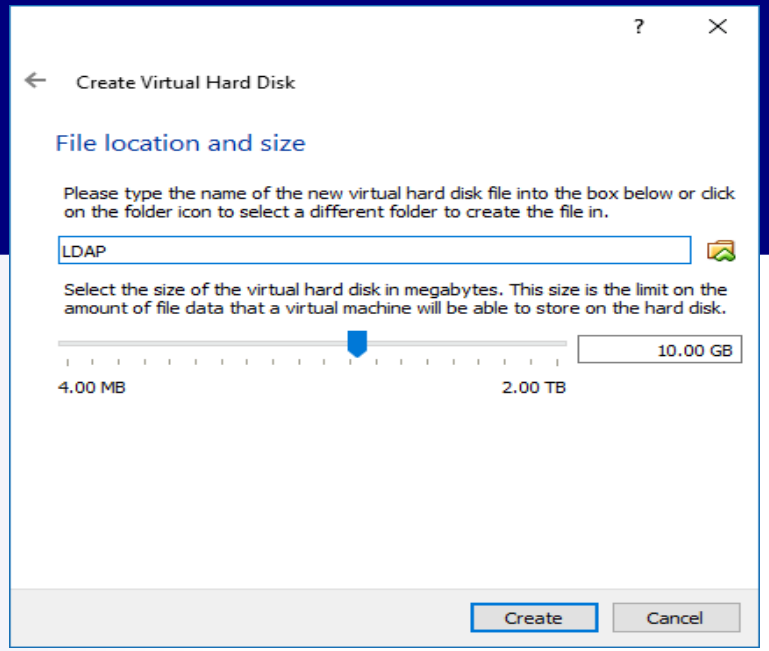




Δημιουργία εργαστηριακού περιβάλλοντος (7)

Εγκατάσταση Ubuntu server σε Virtualbox

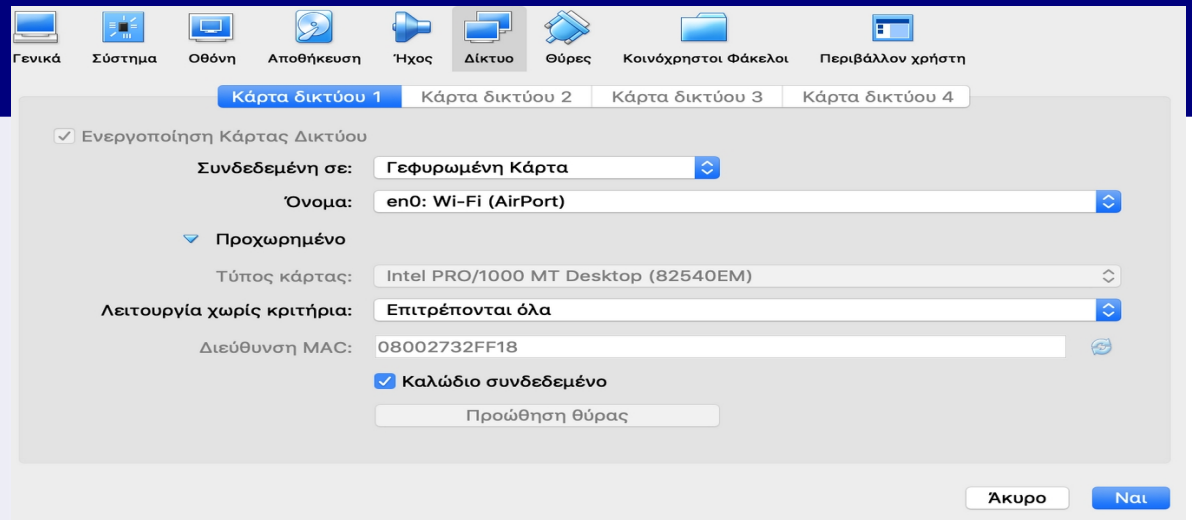
11. Επιλέγουμε τον χώρο αποθήκευσης για τον δίσκο και το μέγεθος του (προσοχή απαιτούνται τουλάχιστον 10gb)



Δημιουργία εργαστηριακού περιβάλλοντος (9)

Εγκατάσταση Ubuntu server σε Virtualbox

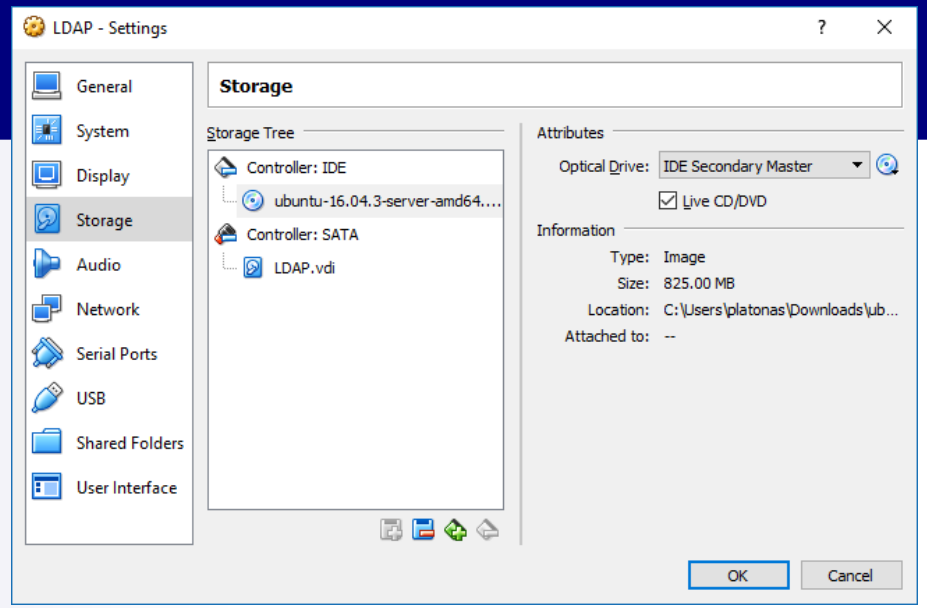
12. Επιλέγουμε από το μενού **Machine>Settings** και ενεργοποιούμε τους network adapters της στην καρτέλα network. Επιλέγουμε **Γεφυρωμένη Κάρτα (bridged adapter)**



Δημιουργία εργαστηριακού περιβάλλοντος (10)

Εγκατάσταση Ubuntu server σε Virtualbox

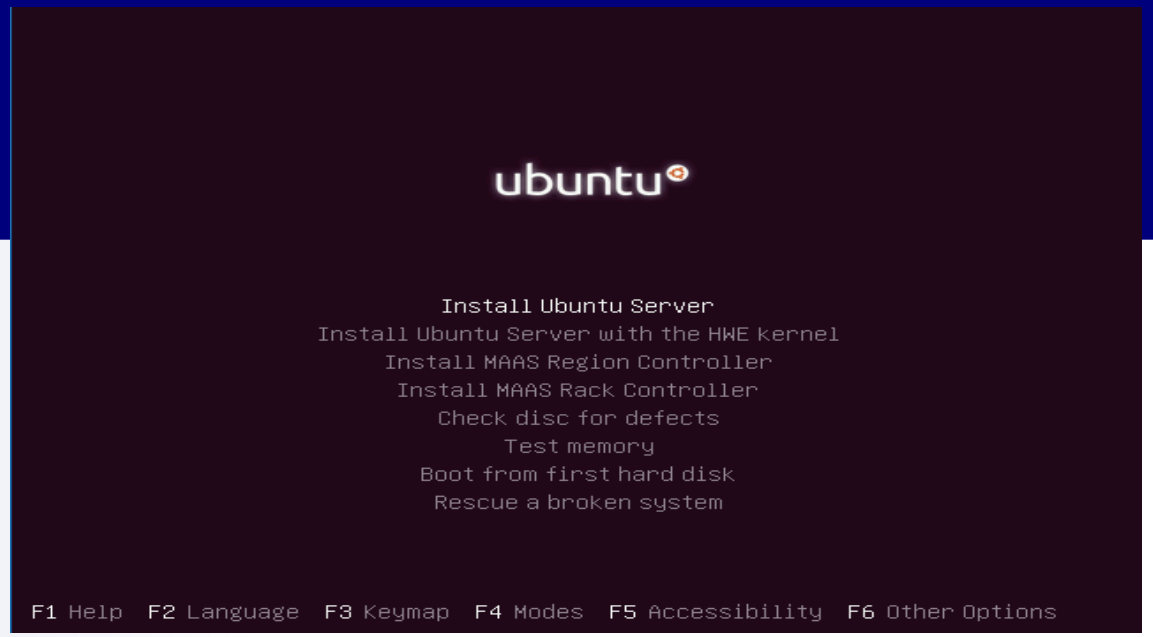
13. Επιλέγουμε από την καρτέλα storage το ubuntu-16.04.3-server-amd64.iso αρχείο (ή ubuntu-16.04.5-desktop-amd64 αν θέλουμε την Desktop έκδοση) και το «φορτώνουμε» στο σύστημά μας ενεργοποιώντας και την επιλογή Live CD/DVD



Δημιουργία εργαστηριακού περιβάλλοντος (11)

Εγκατάσταση Ubuntu server σε Virtualbox

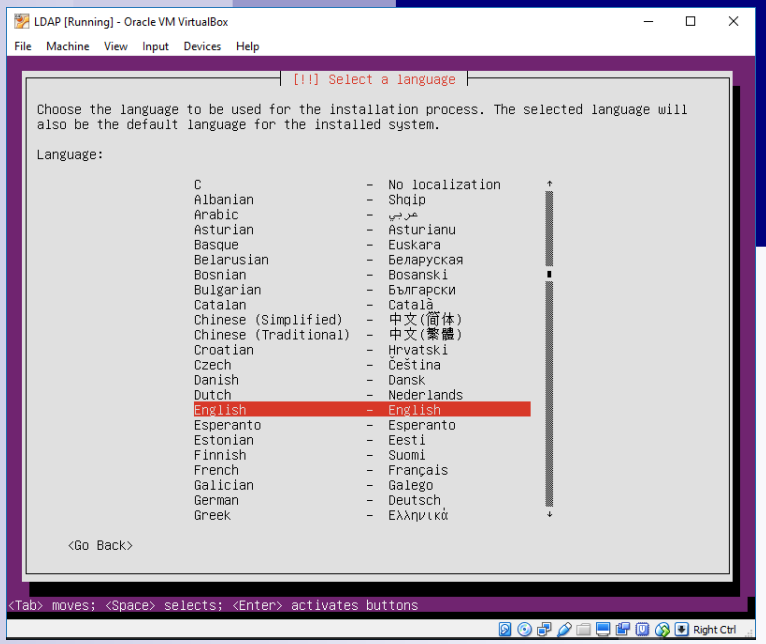
14. Επιλέγουμε από το μενού **Machine > Start** και κάνουμε εγκατάσταση τον Ubuntu server

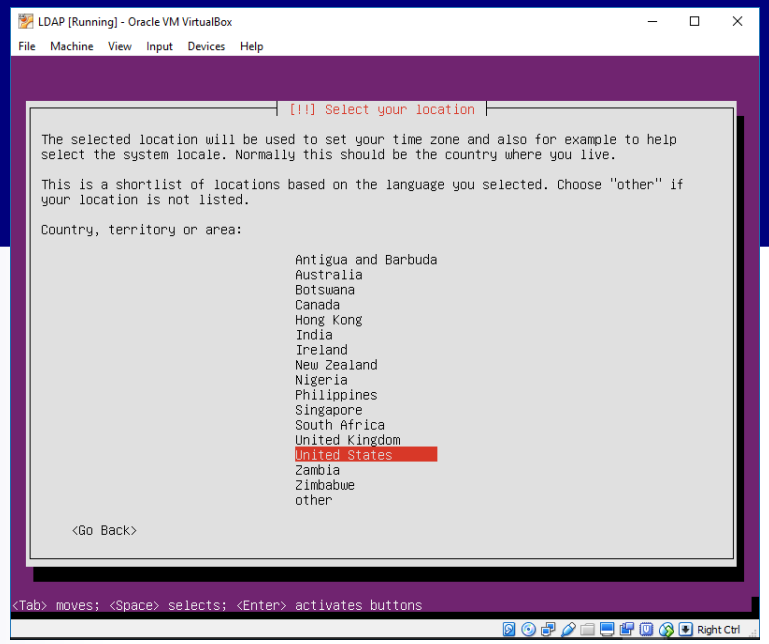


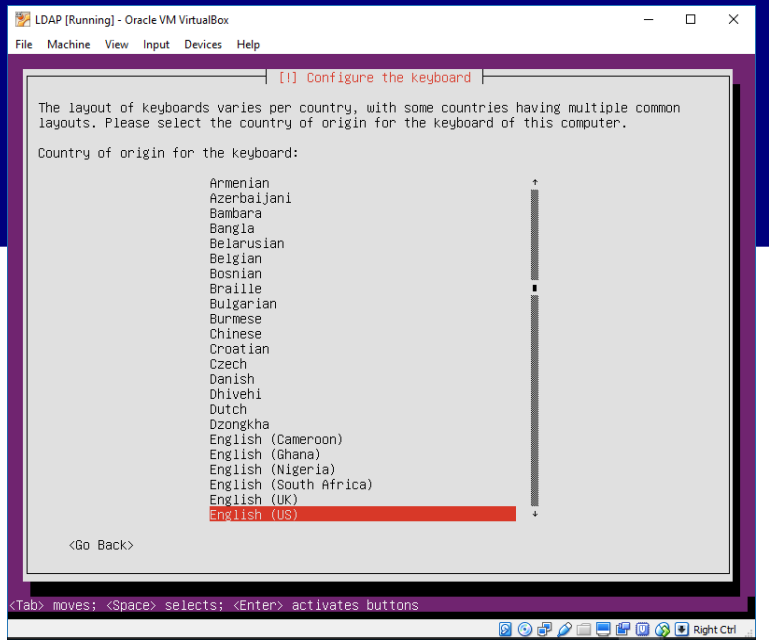
Δημιουργία εργαστηριακού περιβάλλοντος (11)

Εγκατάσταση Ubuntu server σε Virtualbox

15. Επιλέγουμε γλώσσα, τοποθεσία και πληκτρολόγιο



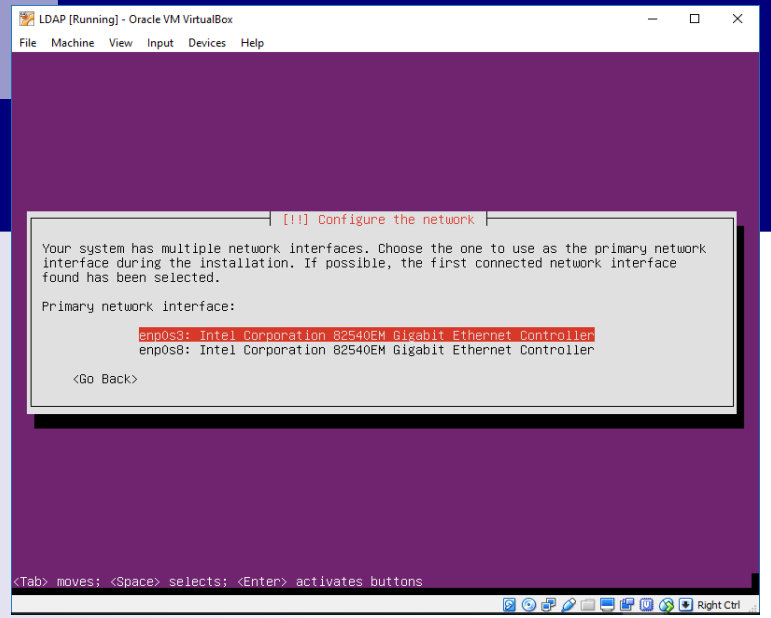


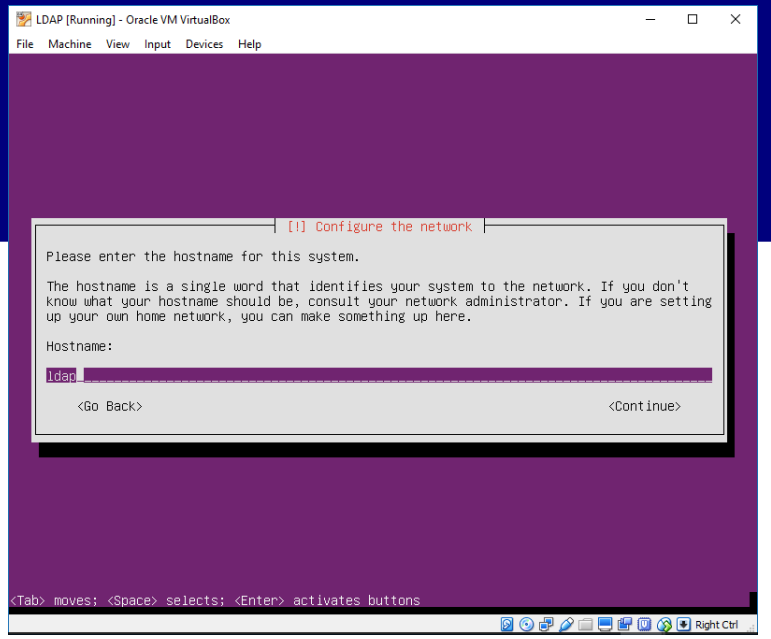


Δημιουργία εργαστηριακού περιβάλλοντος (12)

Εγκατάσταση Ubuntu server σε Virtualbox

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

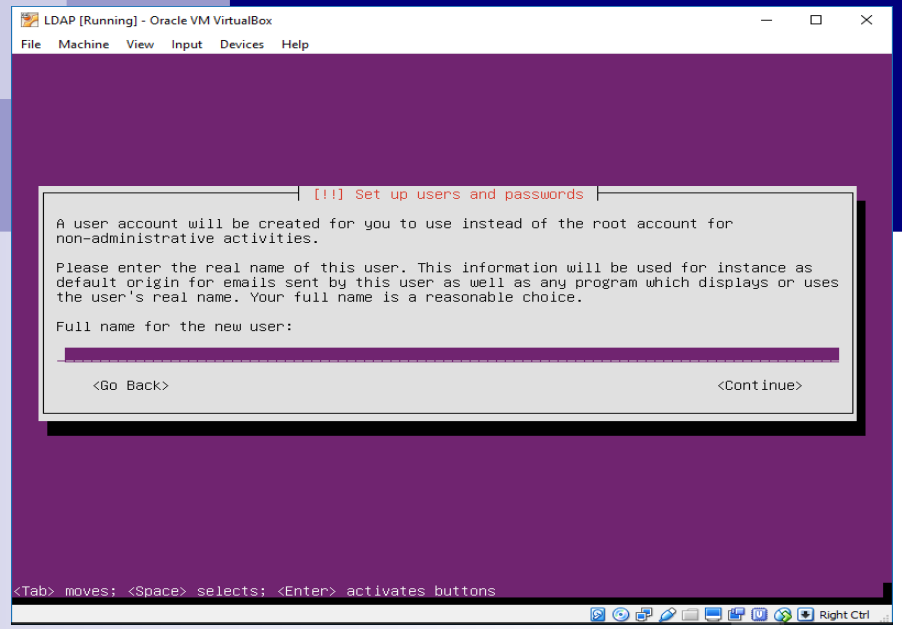


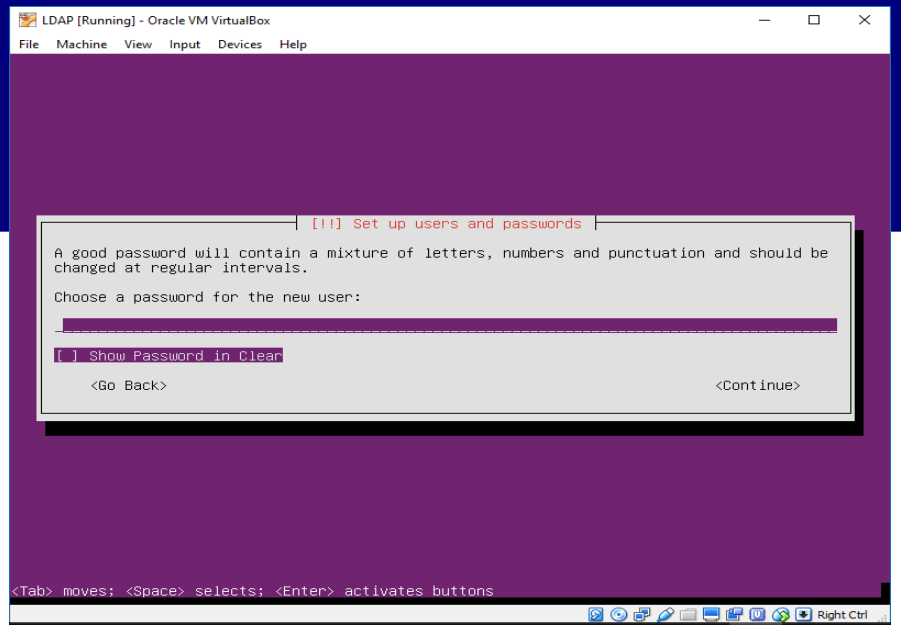


Δημιουργία εργαστηριακού περιβάλλοντος (13)

Εγκατάσταση Ubuntu server σε Virtualbox

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

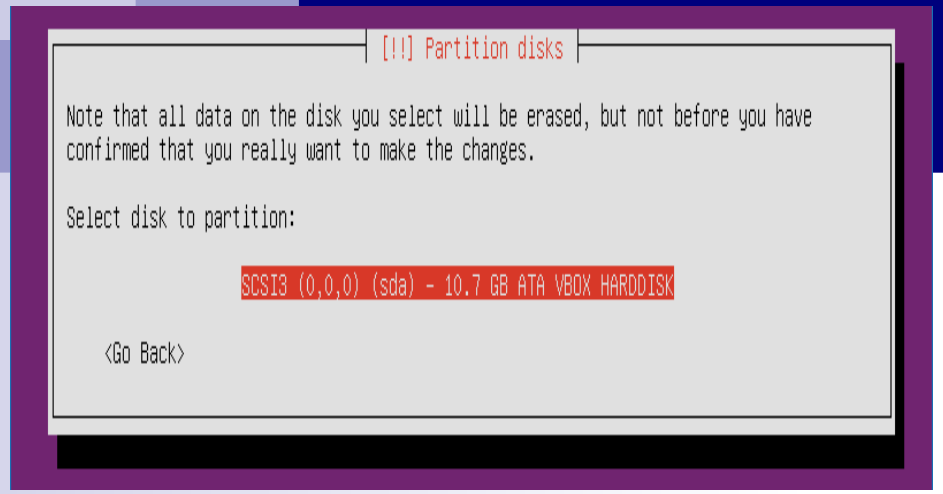


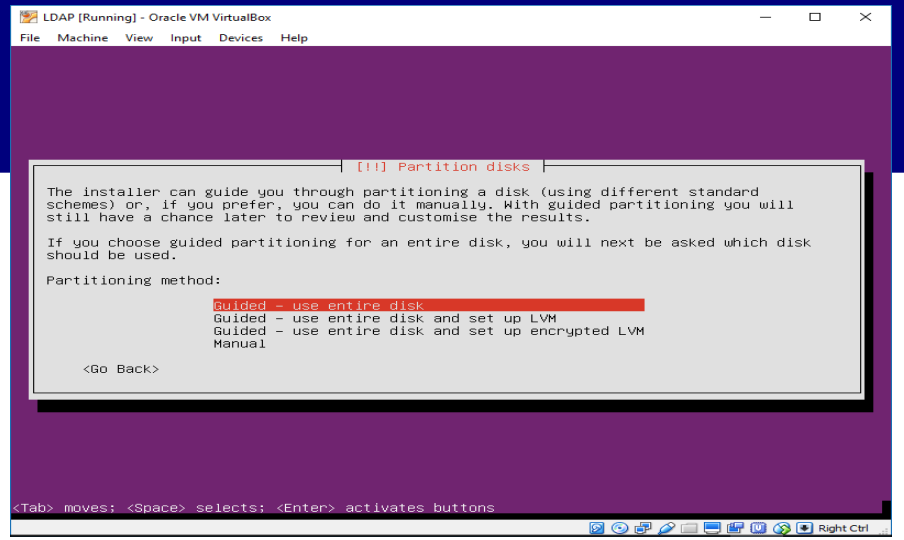


Δημιουργία εργαστηριακού περιβάλλοντος (14)

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

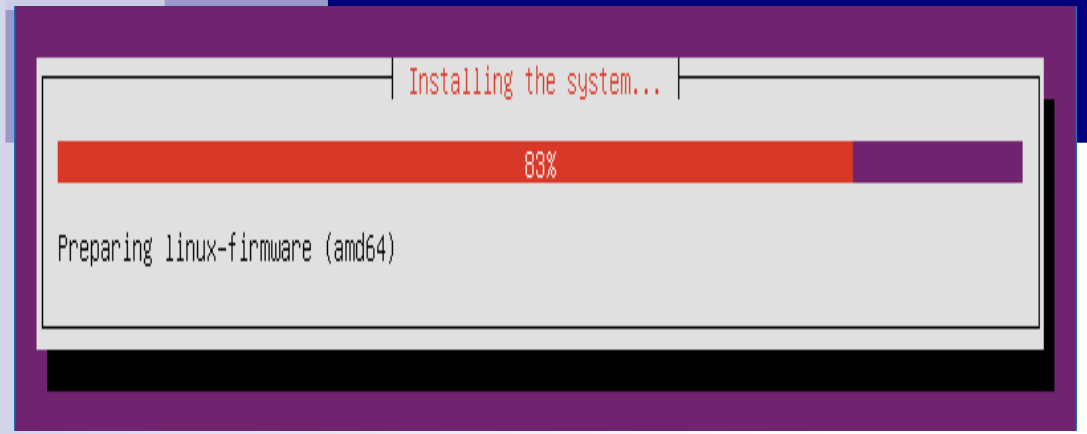


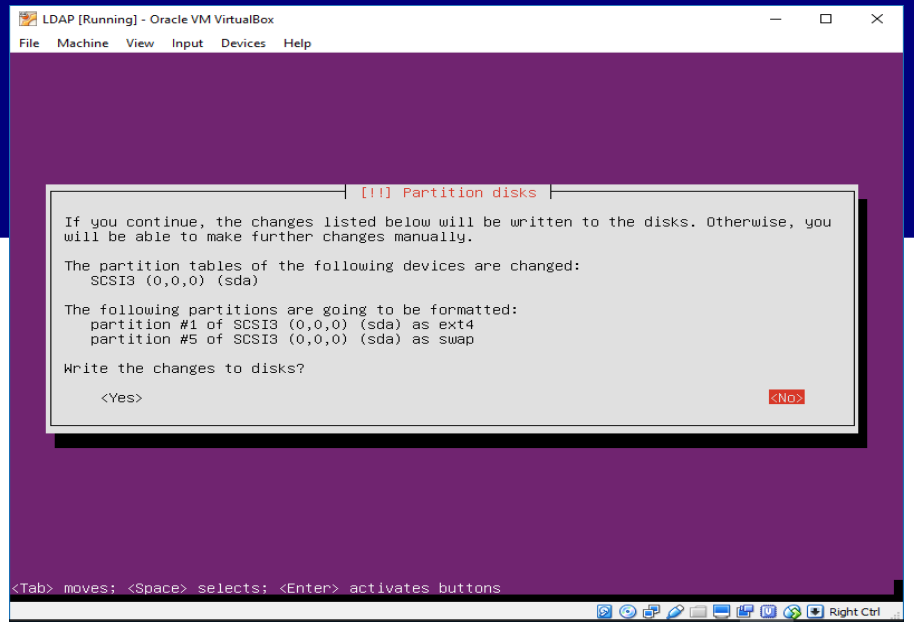


Δημιουργία εργαστηριακού περιβάλλοντος (15)

Εγκατάσταση Ubuntu server σε Virtualbox

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



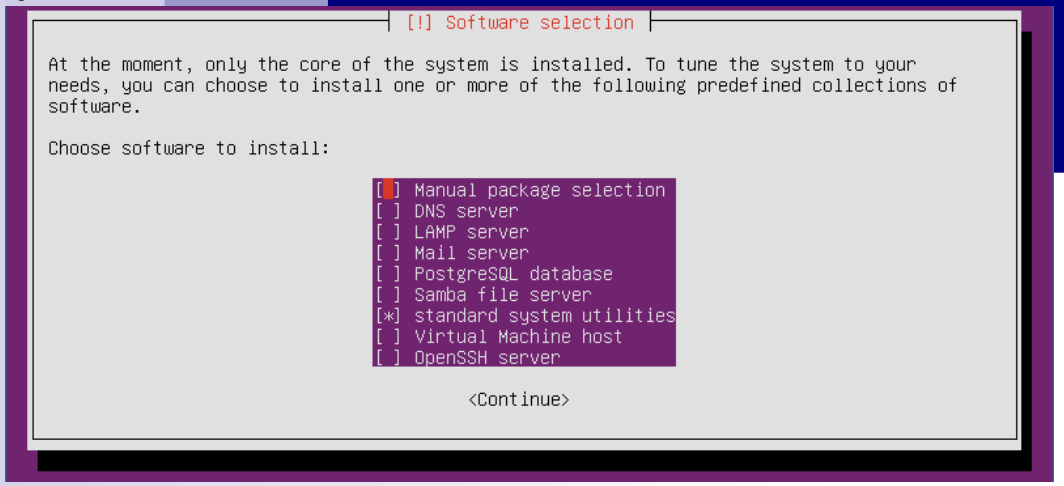


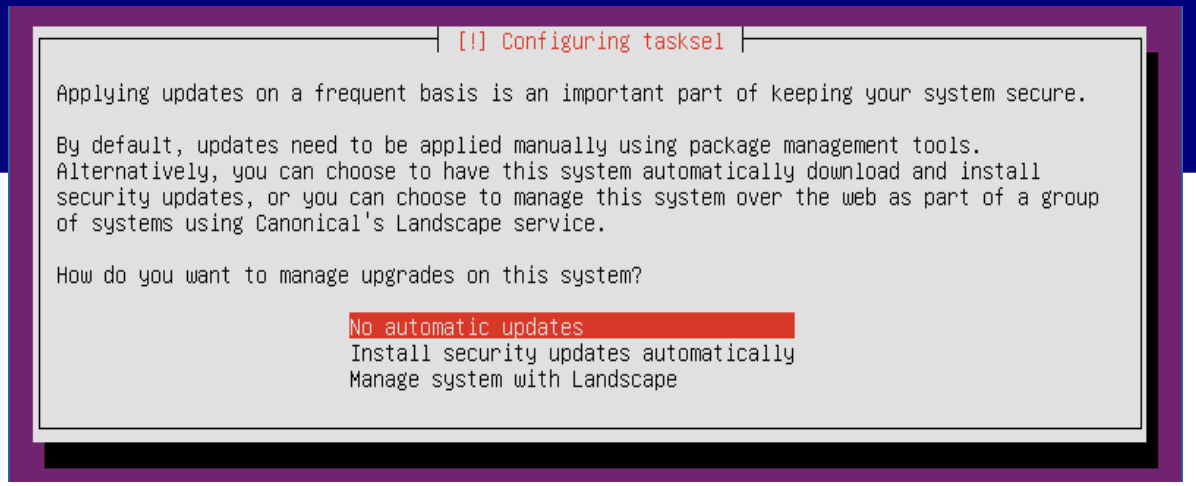
Δημιουργία εργαστηριακού περιβάλλοντος (16)

Εγκατάσταση Ubuntu server σε Virtualbox

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

.



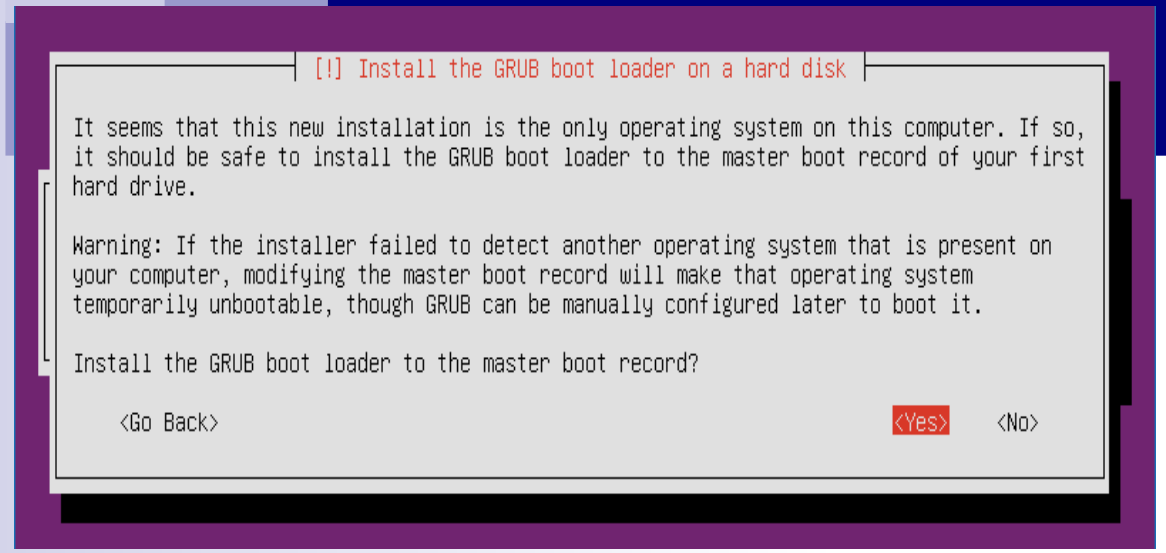


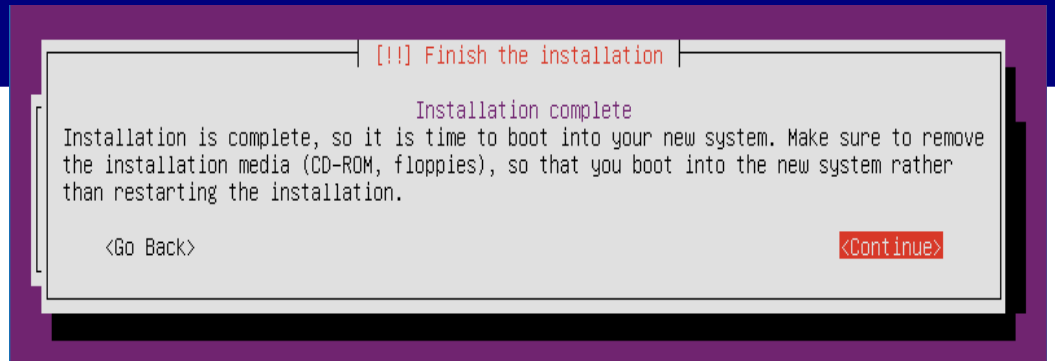
Δημιουργία εργαστηριακού περιβάλλοντος (17)

Εγκατάσταση Ubuntu server σε Virtualbox

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

.

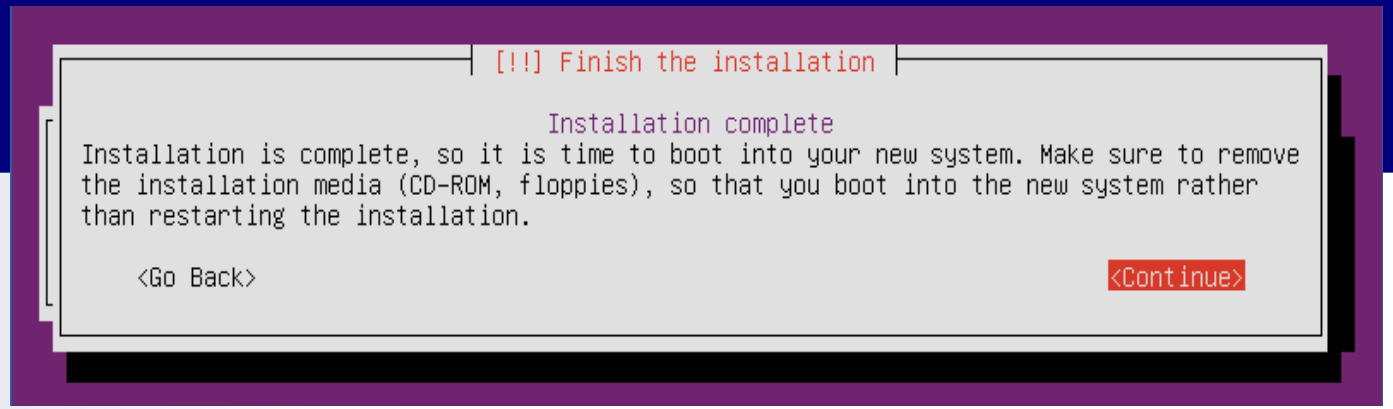




Δημιουργία εργαστηριακού περιβάλλοντος (18)

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



Εγκατάσταση του LDAP

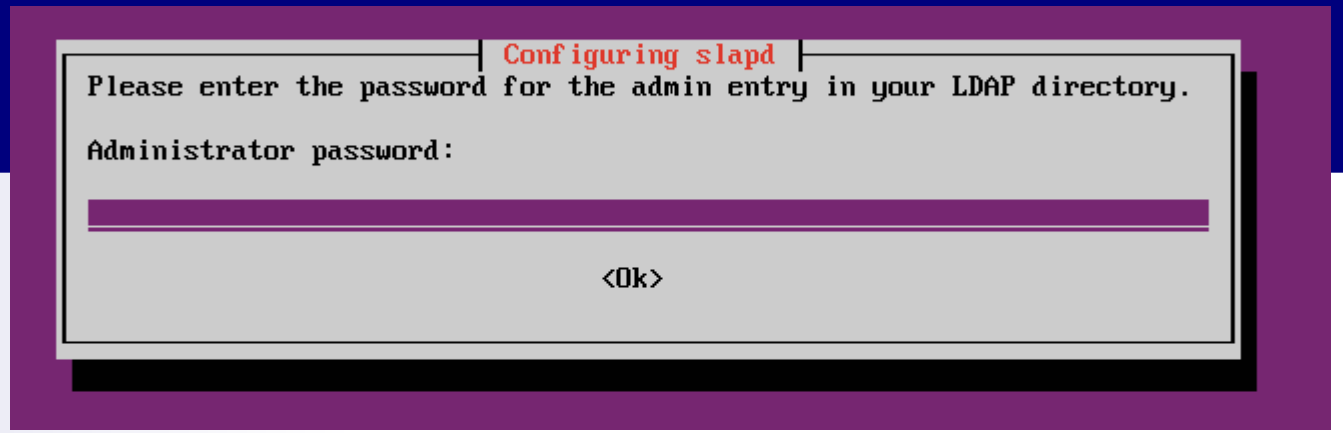
Εγκατάσταση του LDAP σε Ubuntu server

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
```

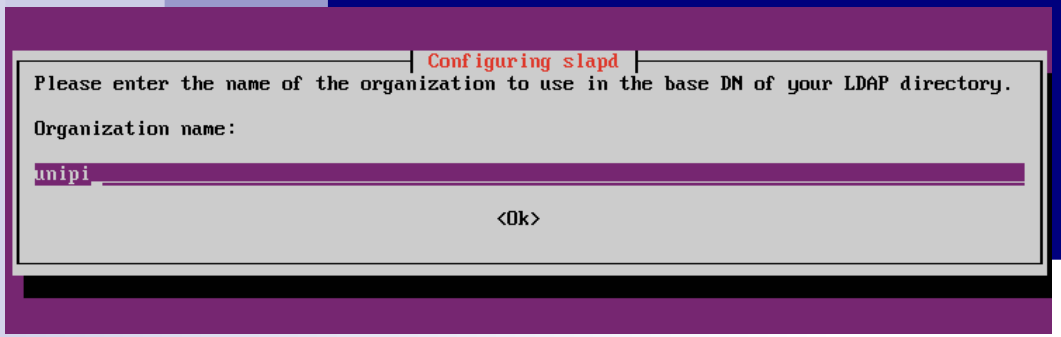
Ρύθμιση του LDAP (1)

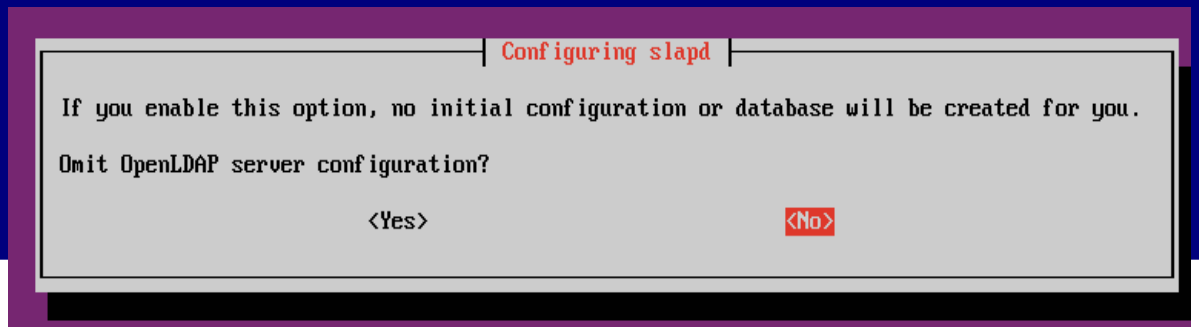
- Εισαγωγή κωδικού για την υπηρεσία slapd
- Ρύθμιση της υπηρεσίας εκ νέου με την εντολή sudo dpkg-reconfigure slapd

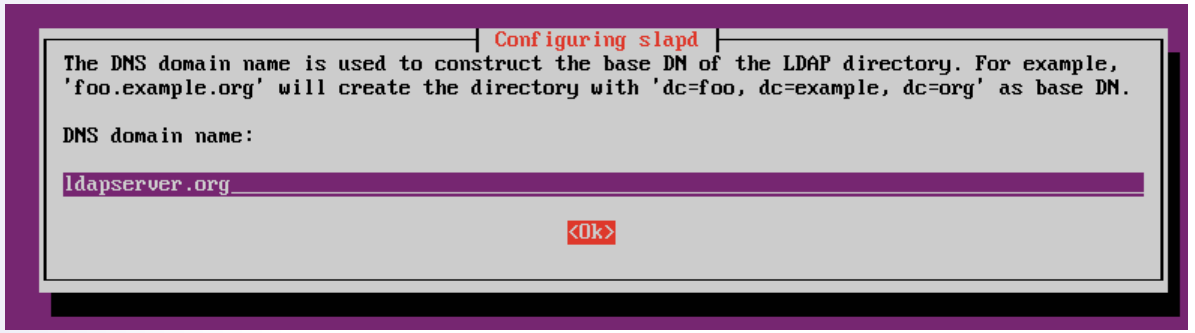


Ρύθμιση του LDAP (2)

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

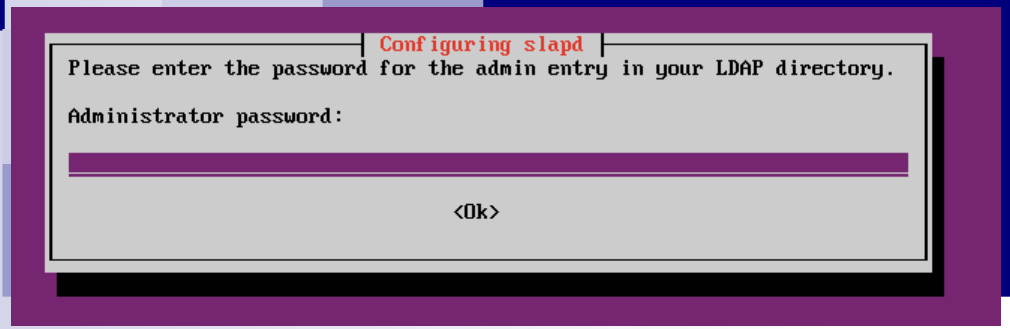


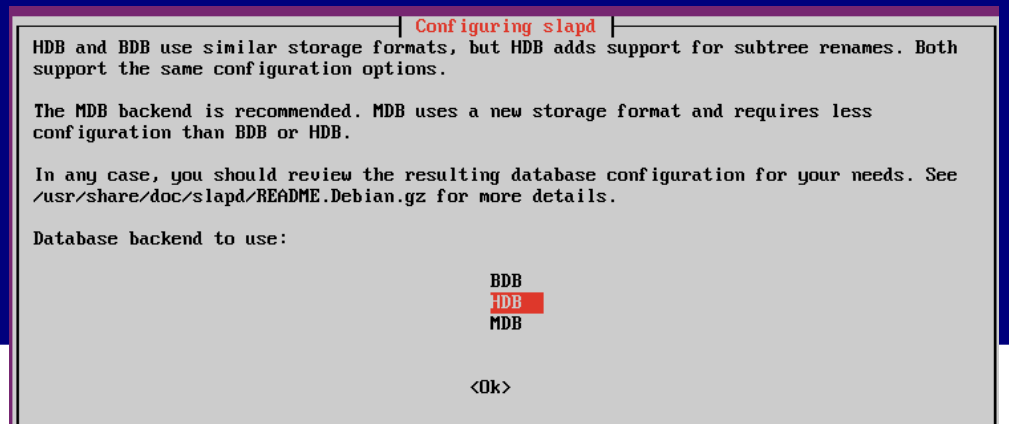




Ρύθμιση του LDAP (3)

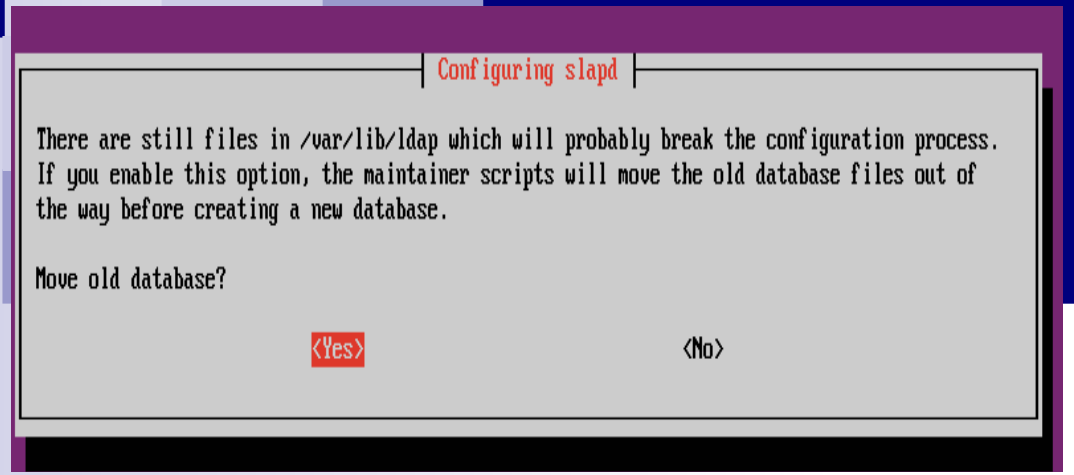
- Εισάγουμε συνθηματικό διαχειριστή, επιλέγουμε τύπο βάσης δεδομένων και μη κατάργηση της ΒΔ με τον τερματισμό της υπηρεσίας slapd

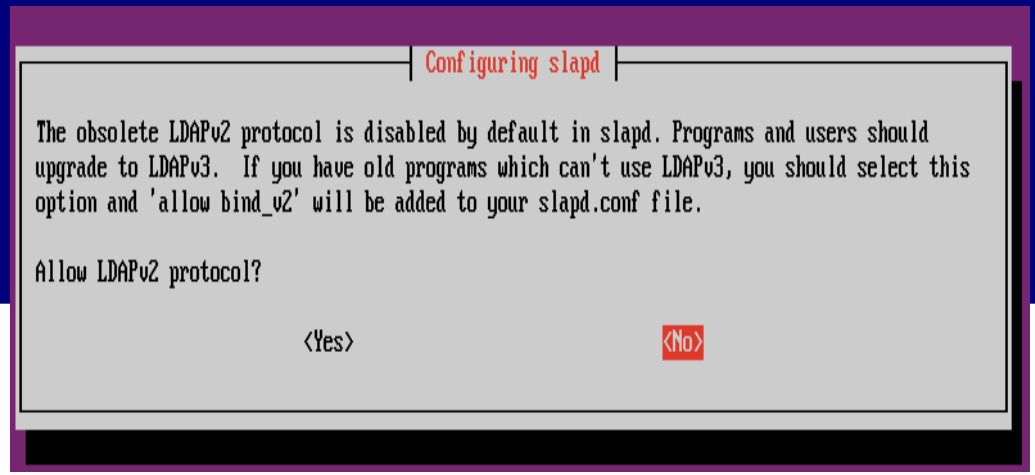




Ρύθμιση του LDAP (4)

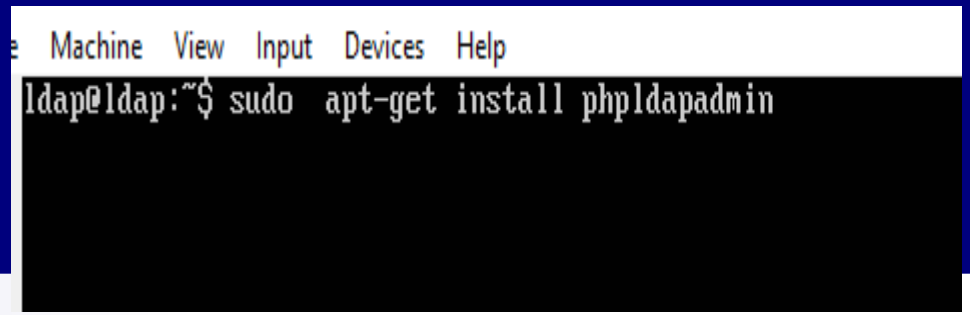
- Μετακίνηση της παλιάς βάσης σε άλλο σημείο, άρνηση συμβατότητας με την παλιά έκδοση 2 του ldap





Εγκατάσταση του PHPldapadmin

- Εγκαθιστούμε τον phpldapadmin με την εντολή 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**

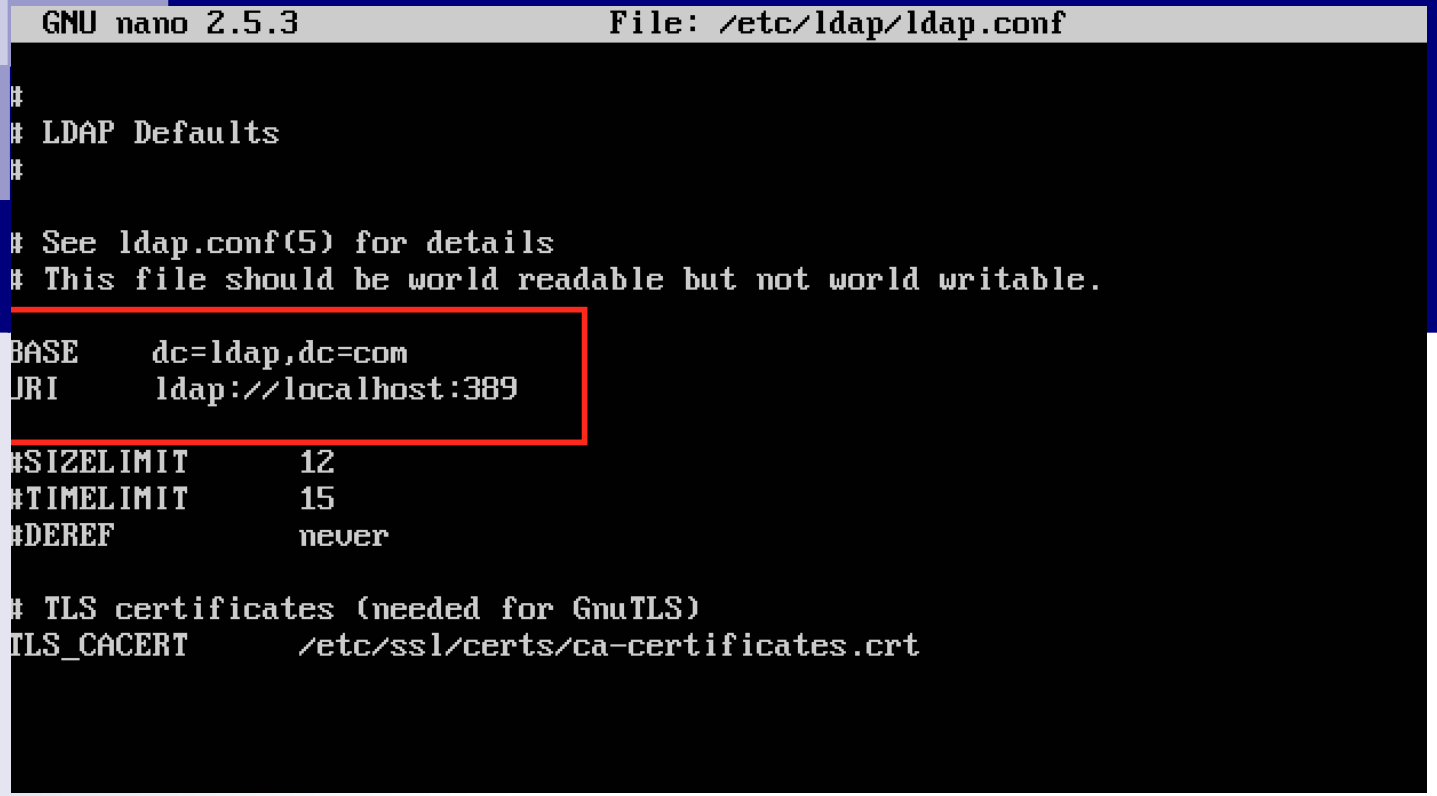
(ή με την εντολή **sudo gedit /etc/phpldapadmin/config.php** αν έχουμε εγκαταστήσει την Desktop έκδοση)

- 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:



Σύνδεση με τον PHPldapadmin (1)

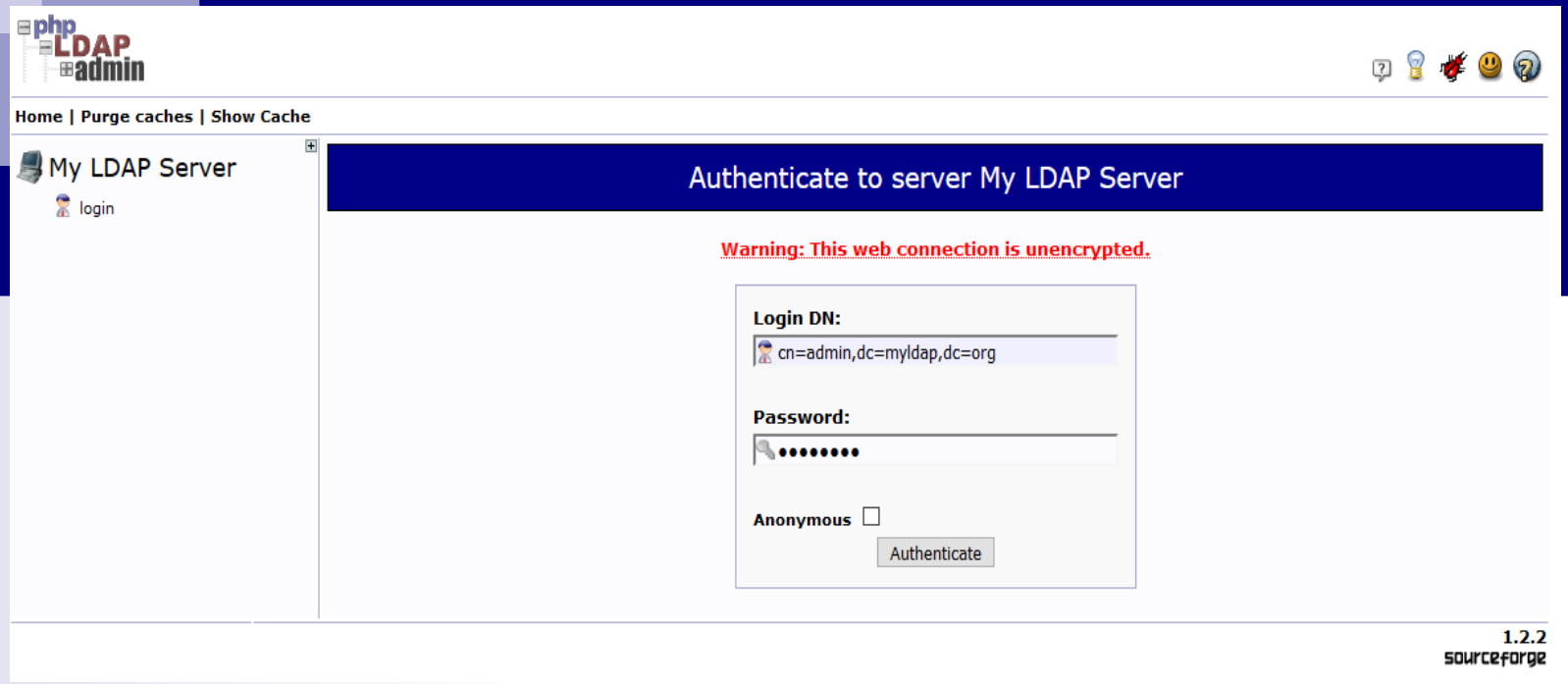
Πληκτρολογώντας την εντολή **ifconfig** μπορούμε να δούμε την ip που έχει ο server μας:

```
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)
```

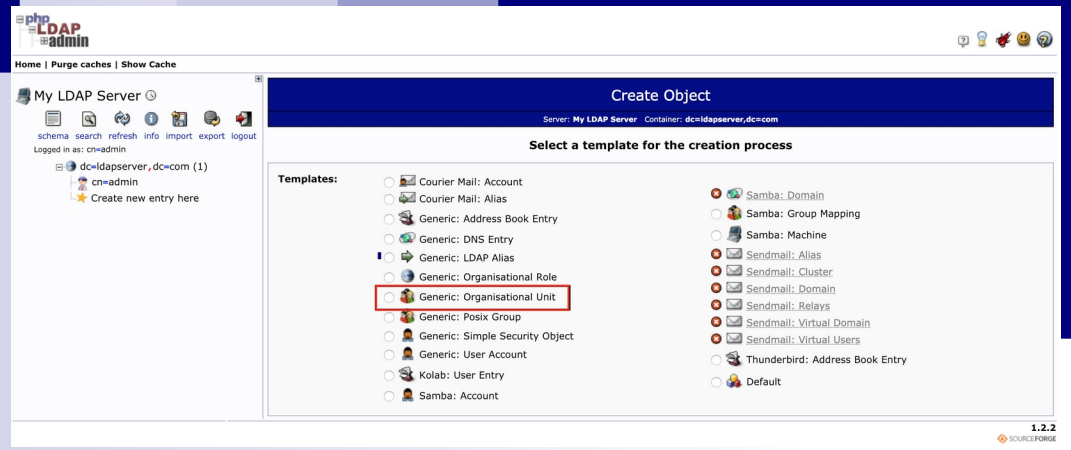
Σύνδεση με τον PHPldapadmin (2)

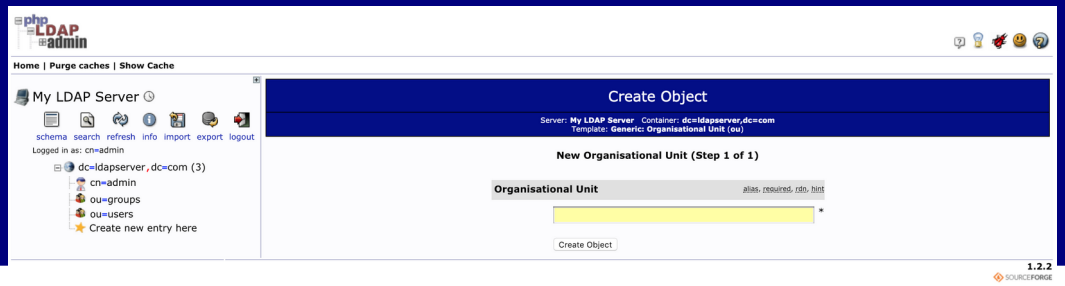
Μέσω του browser http://192.168.2.61/phpldapadmin/ συνδεόμαστε στον ldap server απο τον client:



Δημιουργία χρηστών με τον PHPldapadmin

Επιλέγουμε Organisational Unit για να φτιάξουμε τις διαφορετικές κατηγορίες χρηστών:

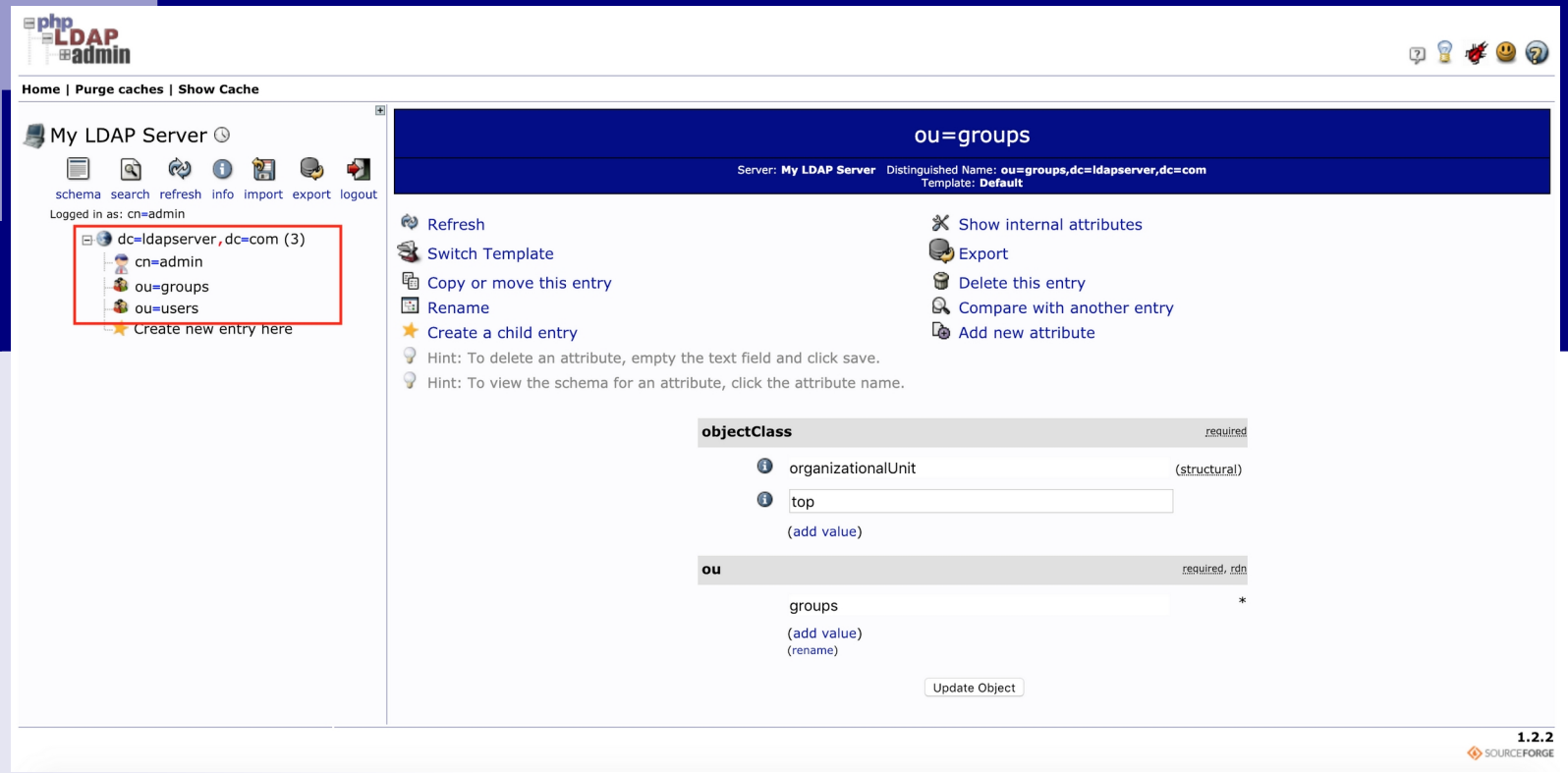




ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

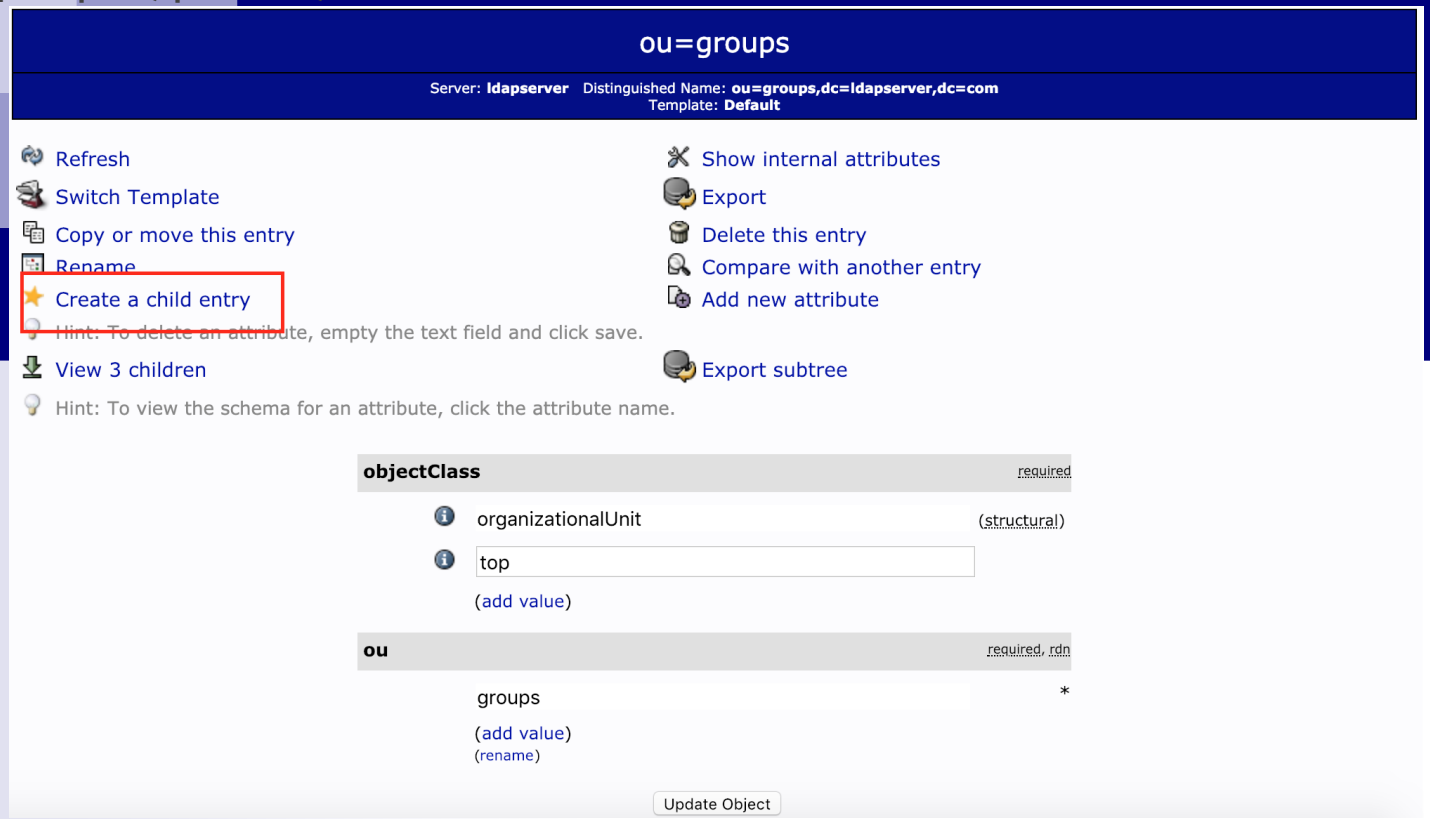
Δημιουργία χρηστών με τον PHPldapadmin

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



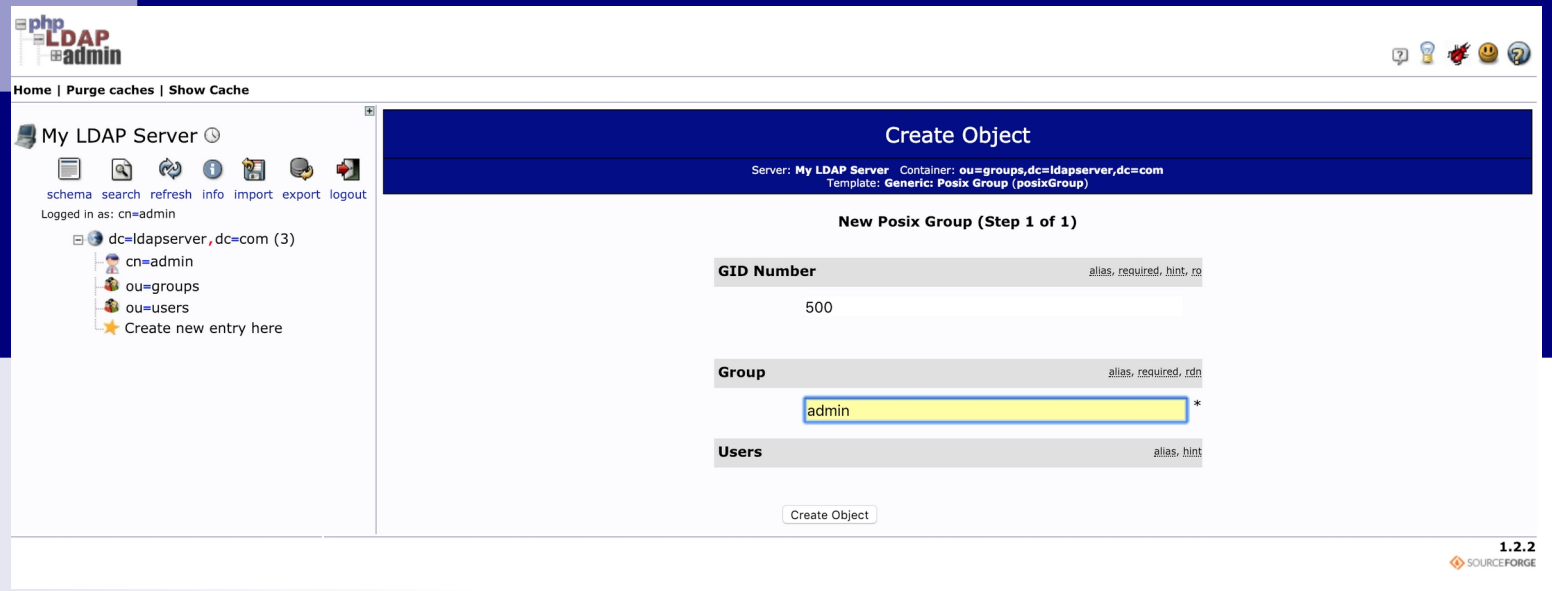
Δημιουργία χρηστών με τον PHPldapadmin

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



Δημιουργία χρηστών με τον PHPldapadmin

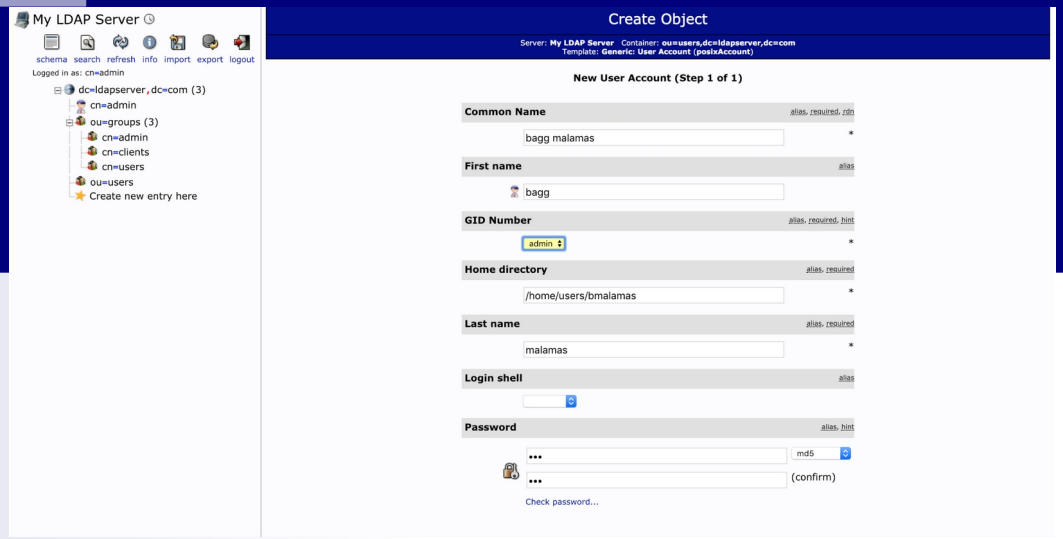
Με αυτό τον τρόπο θα δημιουργήσουμε τους διαφορετικούς ρόλους χρηστών:



Δημιουργία χρηστών με τον PHPldapadmin

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

Συμπληρώνουμε τα στοιχεία:

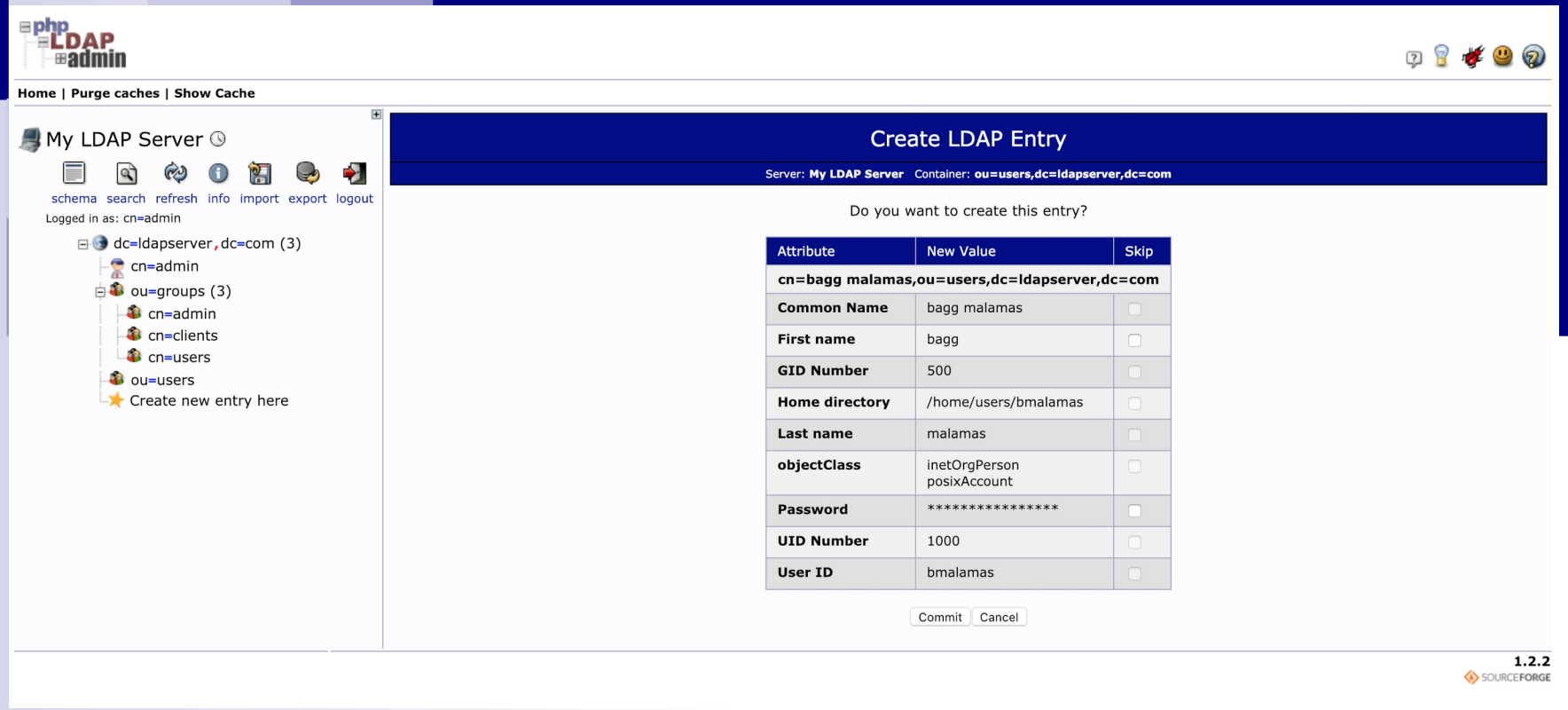


(προσοχή: καλό θα ήταν να μην αφήνουμε κενά)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

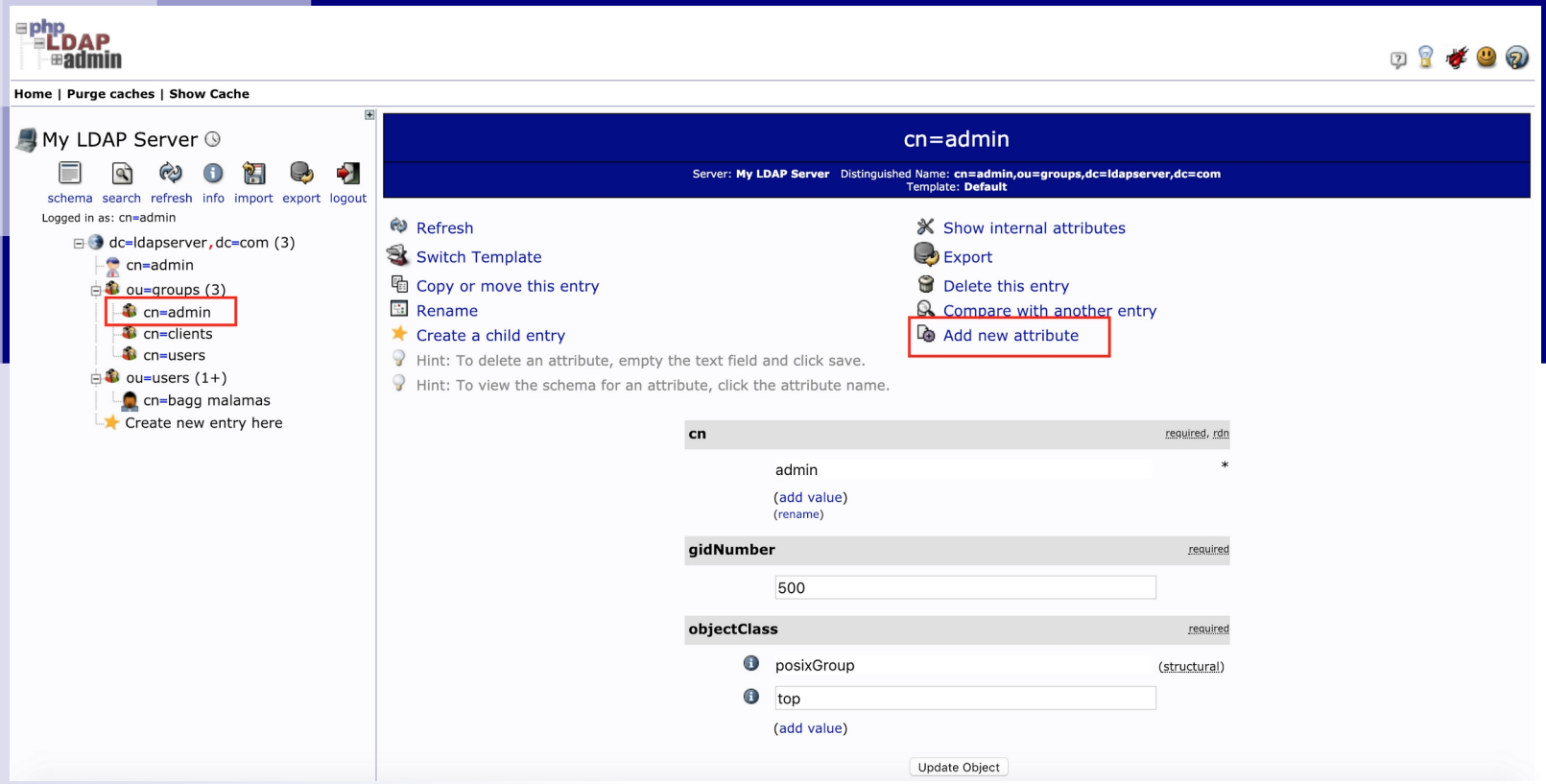
Δημιουργία χρηστών με τον PHPldapadmin

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



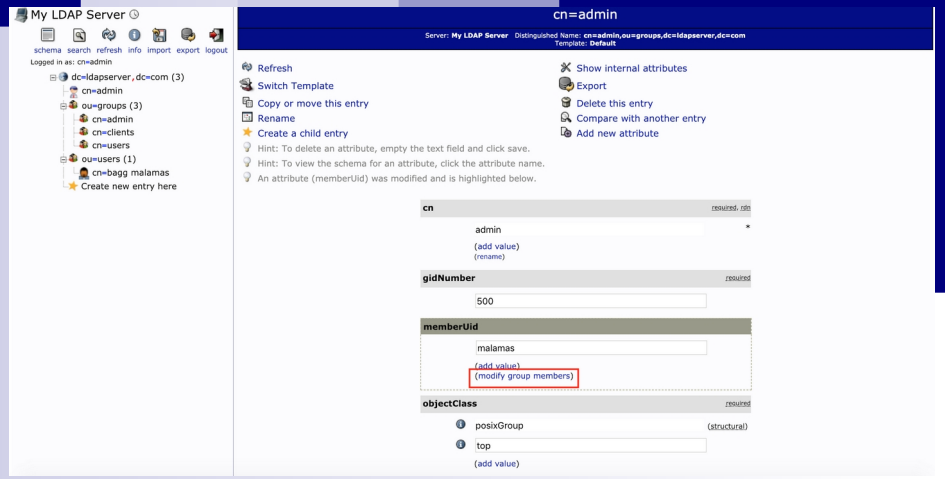
Δημιουργία χρηστών με τον PHPldapadmin

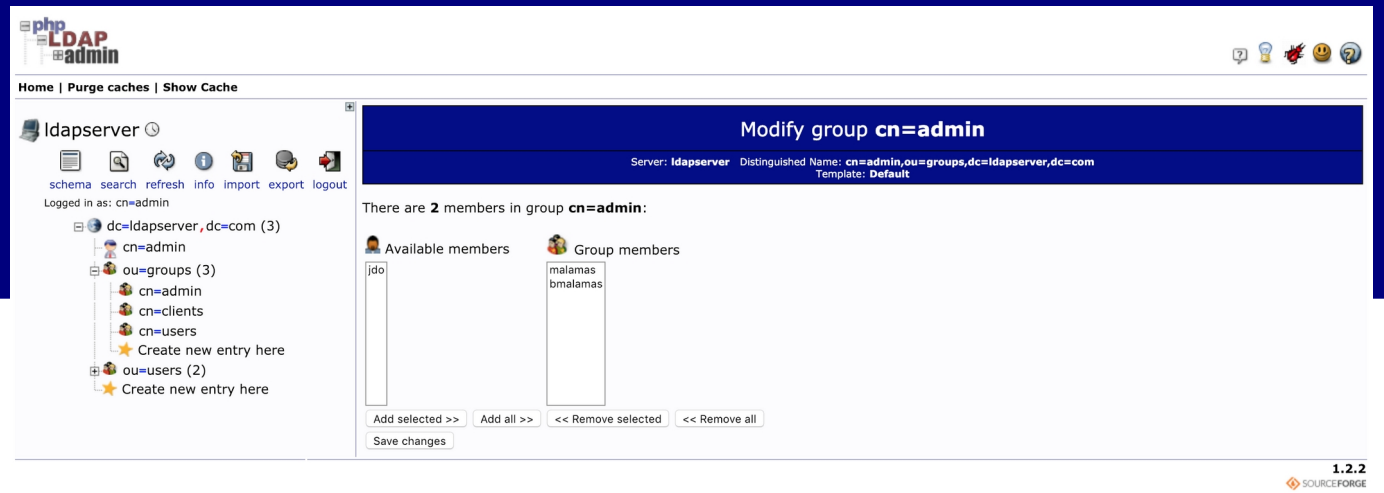
Στη συνέχεια εντάσσουμε τον χρήστη που φτιάξαμε στο γκρούπ των admin επιλέγοντας **add new attribute**:



Δημιουργία χρηστών με τον PHPldapadmin

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





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=TUDelft,c=NL’

Αναζήτηση εγγραφής

ldapsearch -b 'o=TUDelft,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 ένος 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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

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/realm-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