



VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF FUNDAMENTAL SCIENCES

DEPARTMENT OF INFORMATION SYSTEMS

## **OPENLDAP**

Information Technology Security Methods

Prepared by: Simona Riška

Checked by: lect. [REDACTED]

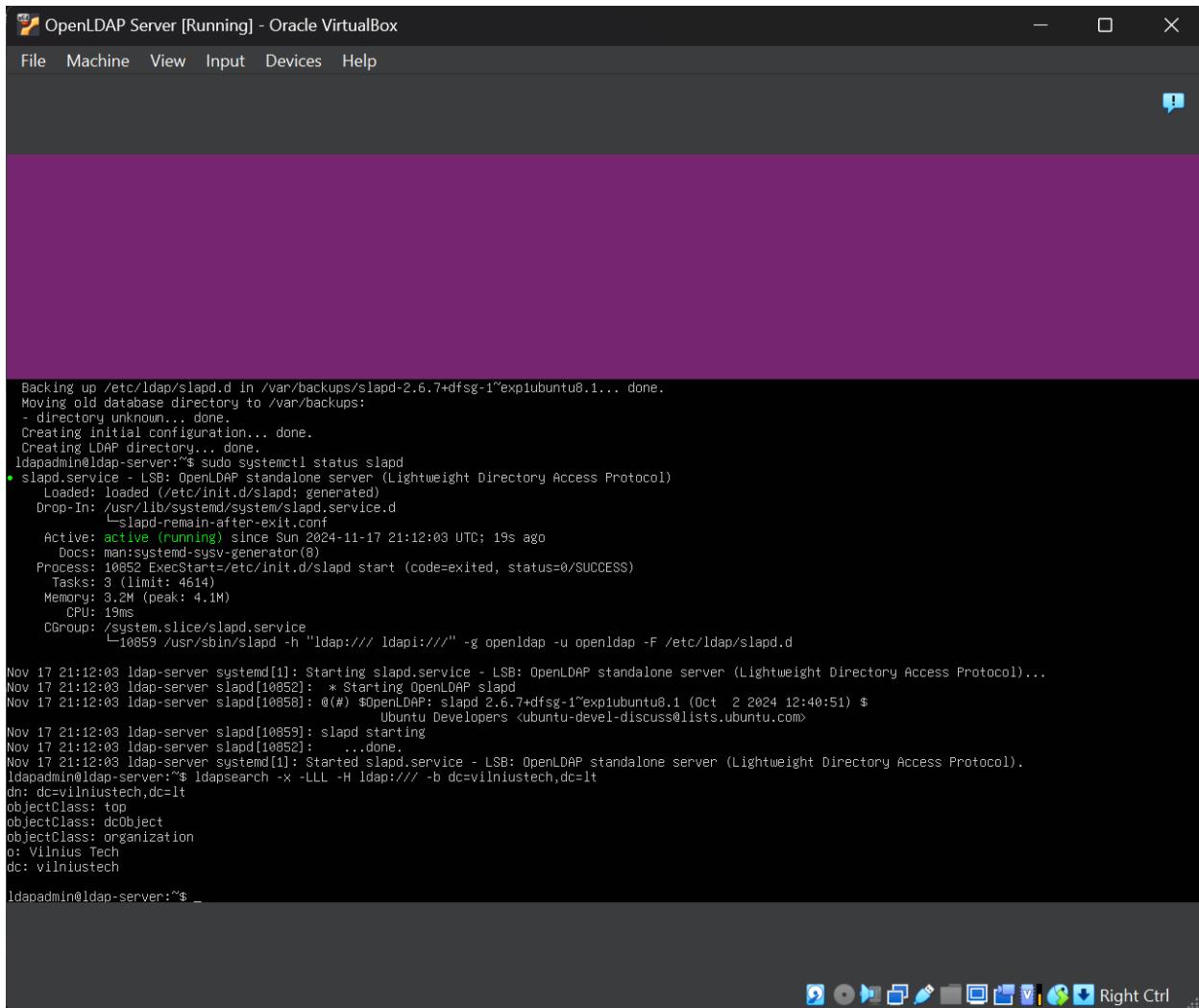
First, I installed the required packages with these commands

**sudo apt update** – updates the list of available packages and their versions to ensure the system retrieves the latest package data.

**sudo apt upgrade -y** – automatically upgrades all installed packages to the latest version. The **-y** flag confirms the upgrade without manual intervention.

**sudo apt install slapd ldap-utils -y** – **slapd** installs the OpenLDAP directory server daemon, **ldap-utils** provides command-line utilities for interacting with an LDAP directory.

Then, I configured OpenLDAP during installation by setting the admin password. To check if everything is running, I used **sudo systemctl status slapd** command:



```
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.6.7+dfsg-1~exp1ubuntu8.1... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
ldapadmin@ldap-server:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
  Loaded: loaded (/etc/init.d/slapd; generated)
  Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
  Active: active (running) since Sun 2024-11-17 21:12:03 UTC; 19s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 10852 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 4614)
   Memory: 3.2M (peak: 4.1M)
      CPU: 19ms
     CGroup: /system.slice/slapd.service
             └─10859 /usr/sbin/slapd -h "ldap:/// ldapi://" -g openldap -u openldap -F /etc/ldap/slapd.d

Nov 17 21:12:03 ldap-server systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)...
Nov 17 21:12:03 ldap-server slapd[10852]: * Starting OpenLDAP slapd
Nov 17 21:12:03 ldap-server slapd[10858]: @(#) $OpenLDAP: slapd 2.6.7+dfsg-1~exp1ubuntu8.1 (Oct 2 2024 12:40:51) $
                                                 Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Nov 17 21:12:03 ldap-server slapd[10859]: slapd starting
Nov 17 21:12:03 ldap-server slapd[10852]: ...done.
Nov 17 21:12:03 ldap-server systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
ldapadmin@ldap-server:~$ ldapsearch -x -LLL -H ldap:// -b dc=vilniustech,dc=lt
dn: dc=vilniustech,dc=lt
objectClass: top
objectClass: dcObject
objectClass: organization
o: Vilnius Tech
dc: vilniustech

ldapadmin@ldap-server:~$ _
```

To enhance the security of the LDAP server, I enabled SSL/TLS to encrypt communication between the client and server. First, with command **sudo mkdir -p /etc/ldap/ssl** I made a dedicated directory for SSL certificate and key:

```
ldapadmin@ldap-server:~$ sudo mkdir -p /etc/ldap/ssl
```

Then, I generated a self-signed certificate with **sudo openssl req -new -x509 -days 365 -nodes -out /etc/ldap/ssl/ldap\_cert.pem -keyout /etc/ldap/ssl/ldap\_key.pem**:

**-new** – creates a new certificate signing request (CSR).

**-x509** – specifies X.509 as the certificate standard for SSL/TLS.

**-days 365** - validates the certificate for 365 days.

**-nodes** - ensures the private key is not password protected.

**-out** and **-keyout** - specify the output paths for the certificate and private key.

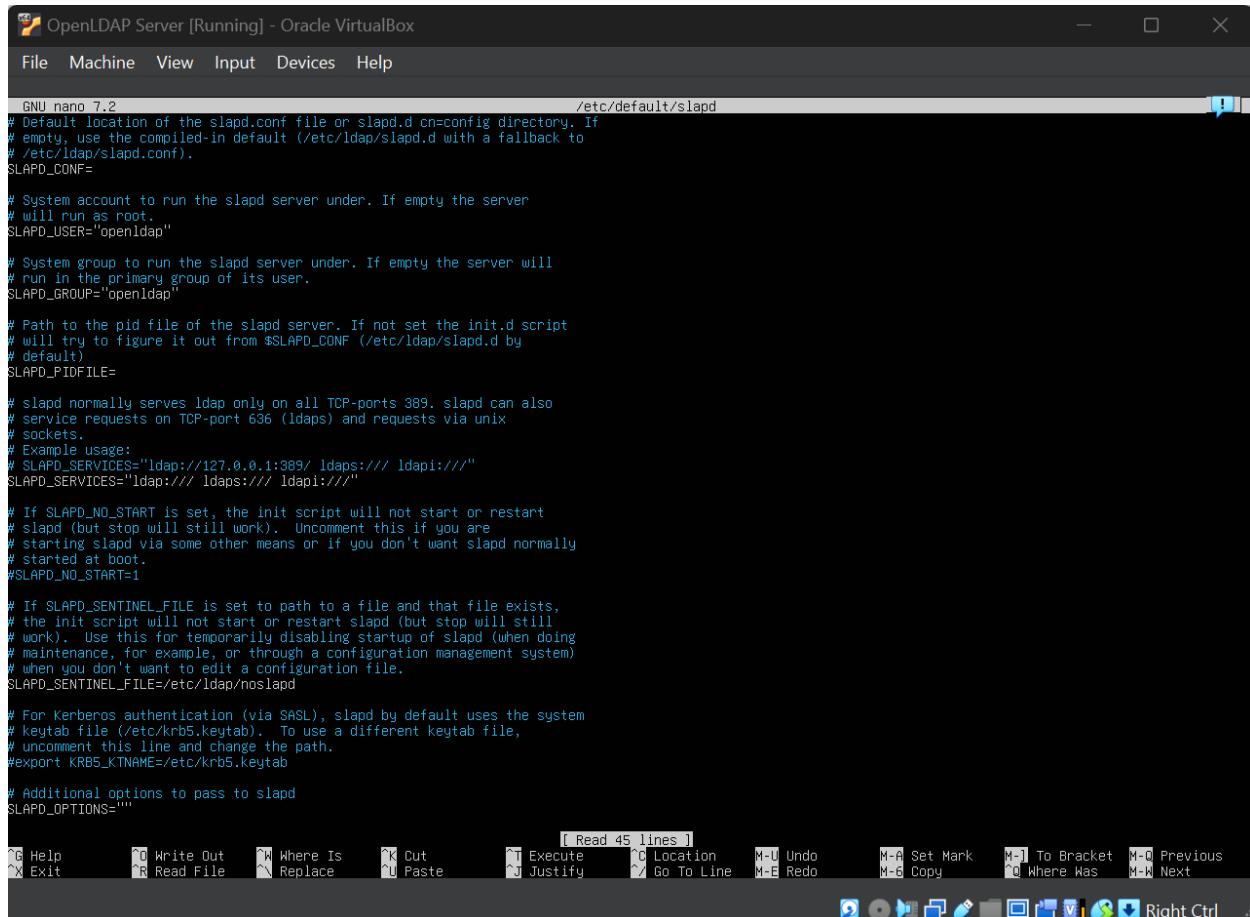
I provided the necessary information for the certificate, such as the organization name and domain.

```
ldapadmin@ldap-server:~$ sudo openssl req -new -x509 -days 365 -nodes -out /etc/ldap/ssl/ldap_cert.pem -keyout /etc/ldap/ssl/ldap_key.pem
...
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:LT
State or Province Name (full name) [Some-State]:Vilnius
Locality Name (eg, city) []:Vilnius
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Vilnius Tech
Organizational Unit Name (eg, section) []:FMF
Common Name (e.g. server FQDN or YOUR name) []:ldap-server
Email Address []:
ldapadmin@ldap-server:~$ sudo chmod openldap /etc/ldap/ssl/*
ldapadmin@ldap-server:~$ sudo chmod 644 /etc/ldap/ssl/ldap_cert.pem
ldapadmin@ldap-server:~$ sudo chmod 600 /etc/ldap/ssl/ldap_key.pem
ldapadmin@ldap-server:~$ sudo systemctl restart slapd
```

I also edited slapd configuration file with **sudo nano /etc/default/slapd** command to configure slapd to support SSL:

```
ldapadmin@ldap-server:~$ sudo nano /etc/default/slapd
```

There, I added to **SLAPD\_SERVICES** that it could be used with SSL with **ldaps://**:



```
GNU nano 7.2                               /etc/default/slapd
# Default location of the slapd.conf file or slapd.d cn=config directory. If
# empty, use the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.d by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldaps:/// ldaps:/// ldapi:///"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work). Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
# the init script will not start or restart slapd (but stop will still
# work). Use this for temporarily disabling startup of slapd (when doing
# maintenance, for example, or through a configuration management system)
# when you don't want to edit a configuration file.
SLAPD_SENTINEL_FILE=/etc/ldap/noslapd

# For Kerberos authentication (via SASL), slapd by default uses the system
# keytab file (/etc/krb5.keytab). To use a different keytab file,
# uncomment this line and change the path.
#export KRB5_KTNAME=/etc/krb5.keytab

# Additional options to pass to slapd
SLAPD_OPTIONS=""
```

Then, to apply the new configuration I restarted slapd service with **sudo systemctl restart slapd**:

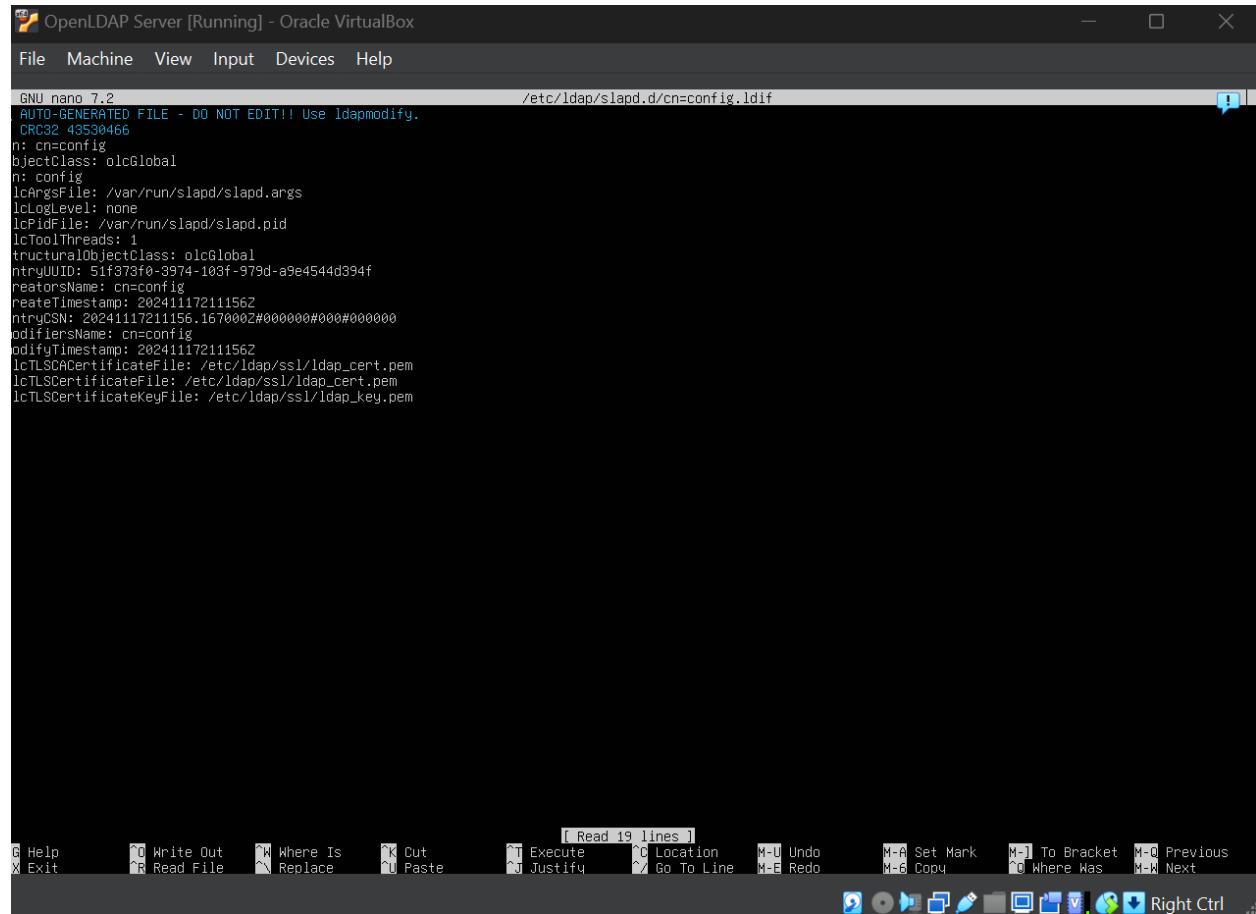
```
ldapadmin@ldap-server:~$ sudo systemctl restart slapd
```

I updated the LDAP configuration to include the generated SSL certificate and key by editing the file `sudo nano /etc/ldap/slapd.d/cn=config.ldif`:

```
ldapadmin@ldap-server:~$ sudo nano /etc/ldap/slapd.d/cn=config.ldif
```

The following lines were added to specify the certificate and key:

```
olcTLSCACertificateFile: /etc/ldap/ssl/ldap_cert.pem  
olcTLSCertificateFile: /etc/ldap/ssl/ldap_cert.pem  
olcTLSCertificateKeyFile: /etc/ldap/ssl/ldap_key.pem
```

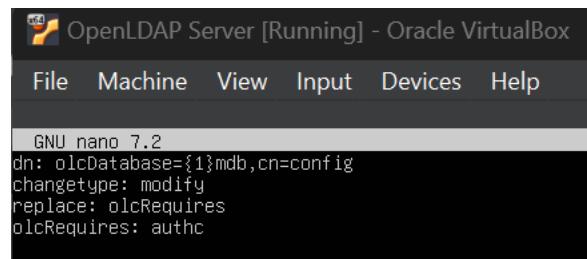


```
GNU nano 7.2                                     /etc/ldap/slapd.d/cn=config.ldif
AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
CRC32 43530466
n: cn=config
objectClass: olcGlobal
n: config
lclArgsFile: /var/run/slapd/slapd.args
lclLogLevel: none
lclPidFile: /var/run/slapd/slapd.pid
lclToolThreads: 1
structuralObjectClass: olcGlobal
ntryUUID: 51f373f0-3974-103f-979d-a9e4544d394f
reactorsName: cn=config
createTimestamp: 202411172111562
ntryCSN: 20241117211156.1670002#000000#000#00000
modifiersName: cn=config
modifyTimestamp: 202411172111562
lclTLSCACertificateFile: /etc/ldap/ssl/ldap_cert.pem
lclTLSCertificateFile: /etc/ldap/ssl/ldap_cert.pem
lclTLSCertificateKeyFile: /etc/ldap/ssl/ldap_key.pem
```

Then with `sudo nano disable-anon.ldif` I created a file to disable anonymous binds:

```
ldapadmin@ldap-server:~$ sudo nano disable-anon.ldif
```

Content of `disable-anon.ldif`:



```
GNU nano 7.2
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRequires
olcRequires: authc
```

Then, I applied the configuration with `sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f disable-anon.ldif`:

```
ldapadmin@ldap-server:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f disable-anon.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"
```

And tested it with **ldapsearch -H ldap://localhost -x -b dc=vilniustech,dc=lt** command. It can be seen here that the authentication is required and anonymous binds were disabled:

```
ldapadmin@ldap-server:~$ ldapsearch -H ldap://localhost -x -b dc=vilniustech,dc=lt
# extended LDIF
#
# LDAPv3
# base <dc=vilniustech,dc=lt> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 53 Server is unwilling to perform
text: authentication required
#
# numResponses: 1
```

Then, I tried to login with admin account with command **ldapsearch -H ldaps://localhost -x -D "cn=admin,dc=vilniustech,dc=lt" -w password123 -b dc=vilniustech,dc=lt** and it worked:

```
ldapadmin@ldap-server:~$ ldapsearch -H ldaps://localhost -x -D "cn=admin,dc=vilniustech,dc=lt" -w password123 -b dc=vilniustech,dc=lt
# extended LDIF
#
# LDAPv3
# base <dc=vilniustech,dc=lt> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# vilniustech.lt
dn: dc=vilniustech,dc=lt
objectClass: top
objectClass: dcObject
objectClass: organization
o: Vilnius Tech
dc: vilniustech

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
ldapadmin@ldap-server:~$
```

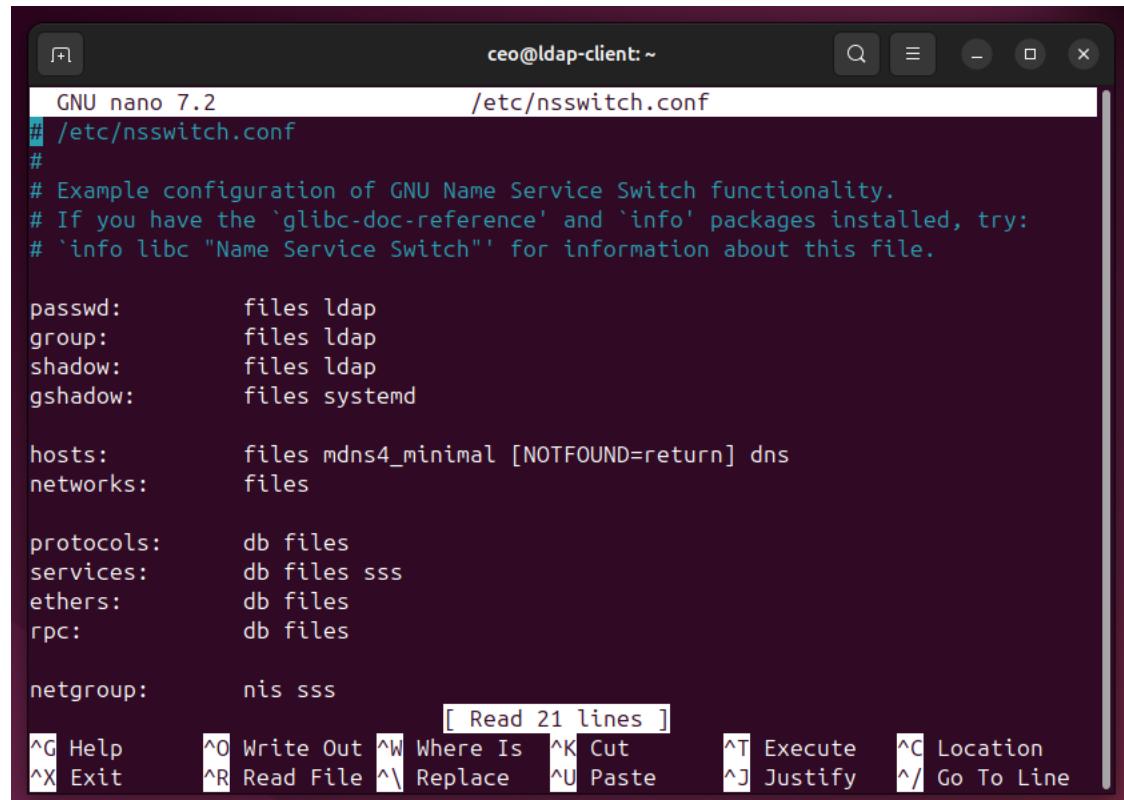
For client I updated system packages on the client machine to ensure it had the latest versions of the required dependencies with commands `sudo apt update` and `sudo apt upgrade -y`, then I installed the necessary LDAP utilities and PAM/NSS modules with command `sudo apt install ldap-utils libnss-ldapd libpam-ldapd nsldc`. `ldap-utils` – command-line utilities for interacting with the LDAP directory, `libnss-ldapd` – enables LDAP support for NSS (Name Service Switch), `libpam-ldapd` – allows PAM (Pluggable Authentication Module) to authenticate users using LDAP, `nsldc` – the daemon that handles LDAP name service lookups.

```
ldap-client@ldap-client:~$ sudo apt install ldap-utils libnss-ldap libpam-ldapd nsldc -y
```

Then, I configured NSS (Name Service Switch). I opened `sudo nano /etc/nsswitch.conf` for editing:

```
ldap-client@ldap-client:~$ sudo nano /etc/nsswitch.conf
```

I modified the following lines to include `ldap`. This allows the system to query the LDAP server for user, group, and shadow information.:



The screenshot shows a terminal window titled "ceo@ldap-client:~". The window contains the contents of the /etc/nsswitch.conf file. The file includes configuration for passwd, group, shadow, gshadow, hosts, networks, protocols, services, ethers, rpc, netgroup, and nis. The "passwd", "group", and "shadow" entries now include "files ldap" instead of just "files". The "hosts" entry includes "files mdns4\_minimal [NOTFOUND=return] dns". The "networks" entry includes "files". The "protocols", "services", "ethers", and "rpc" entries include "db files". The "netgroup" entry includes "nis". The "nis" entry includes "sss". At the bottom of the screen, there is a menu bar with options like Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, and Go To Line. A status bar at the bottom indicates "[ Read 21 lines ]".

```
GNU nano 7.2          /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files systemd

hosts:        files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files sss
ethers:      db files
rpc:         db files

netgroup:    nis sss
[ Read 21 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^P Replace  ^U Paste    ^J Justify  ^/ Go To Line
```

Then, with I opened `sudo nano /etc/pam.d/common-session` and added the following line to enable automatic home directory creation upon first login:

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

`pam_mkhomedir.so` - creates the user's home directory if it doesn't exist.

`skel=/etc/skel` - specifies the skeleton directory for creating the default home directory structure.

`umask=0022` - sets the default permissions for new directories and files.

```

GNU nano 7.2          /etc/pam.d/common-session
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
session required pam_mkhomedir.so skel=/etc/skel umask=0022
# here are the per-package modules (the "Primary" block)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite           pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
[ Read 33 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line

```

To simplify communication with the LDAP server, I added server ip address to `/etc/hosts` with command `sudo nano /etc/hosts`:

```
ldap-client@ldap-client:~$ sudo nano /etc/hosts
```

There I added ip address and named it `ldap-server`. This ensures the client can resolve ldap-server to the server's IP address:

```

GNU nano 7.2          /etc/hosts *
127.0.0.1 localhost
127.0.1.1 ldap-client
192.168.31.18 ldap-server

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
[ Read 10 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line
^M-U Undo   ^M-E Redo

```

To establish secure communication, I copied the SSL certificate from the server to the client using the `scp` command:

```
ldapadmin@ldap-server:~$ scp /etc/ldap/ssl/ldap_cert.pem ldap-client@192.168.31.196:~
ldap-client@192.168.31.196's password:
ldap_cert.pem
ldapadmin@ldap-server:~$
```

Then, on the client machine I created `/etc/ldap/ssl` folder to store certificates with `mkdir -p /etc/ldap/ssl`:

```
ldap-client@ldap-client:~$ sudo mkdir -p /etc/ldap/ssl
```

Then, I moved certificate to this directory:

```
ldap-client@ldap-client:~$ sudo chmod 755 /etc/ldap/ssl
```

```
ldap-client@ldap-client:~$ sudo mv ~/ldap_cert.pem /etc/ldap/ssl/
```

```
ldap-client@ldap-client:~$ sudo chmod 644 /etc/ldap/ssl/ldap_cert.pem
```

I configured `nsLCD` with opening `sudo nano /etc/nsLCD.conf` and updated the configuration with the following:

```
ldap-client@ldap-client:~$ sudo nano /etc/nsLCD.conf
ldap-client@ldap-client:~$
```

`uri` – specifies the LDAP server's URI using the ldaps protocol for secure communication.

`base` – the base DN for LDAP queries.

`binddn` and `bindpw` – the DN and password of the admin user for binding.

`tls_reqcert allow` – accepts self-signed certificates.

`tls_cacertfile` – points to the path of the server's SSL certificate.

```
GNU nano 7.2          /etc/nsLCD.conf
# /etc/nsLCD.conf
# nsLCD configuration file. See nsLCD.conf(5)
# for details.

# The user and group nsLCD should run as.
uid nsLCD
gid nsLCD

# The location at which the LDAP server(s) should be reachable.
uri ldaps://ldap-server/

# The search base that will be used for all queries.
base dc=vilniustech,dc=lt
binddn cn=admin,dc=vilniustech,dc=lt
bindpw password123
ssl on
tls_reqcert allow
tls_cacertfile /etc/ldap/ssl/ldap_cert.pem
# The LDAP protocol version to use.
#ldap_version 3
```

Then, to configure the LDAP client globally I opened `sudo nano /etc/ldap/ldap.conf`:

```
ldap-client@ldap-client:~$ sudo nano /etc/ldap/ldap.conf
```

I updated the file:

`BASE` – sets the base DN for all LDAP operations.

`URI` – specifies the secure LDAP server URI.

`TLS_CACERT` – points to the certificate file for secure communication.

ceo@ldap-client: ~

GNU nano 7.2 /etc/ldap/ldap.conf

```
# LDAP Defaults

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE    dc=example,dc=com
BASE    dc=vilniustech,dc=lt
#URI    ldap://ldap.example.com ldap://ldap-provider.example.com:666
URI    ldaps://ldap-server

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

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

[ Read 19 lines ]

**^G** Help      **^O** Write Out    **^W** Where Is    **^K** Cut    **^T** Execute    **^C** Location  
**^X** Exit      **^R** Read File    **^\\** Replace    **^U** Paste    **^J** Justify    **^/** Go To Line

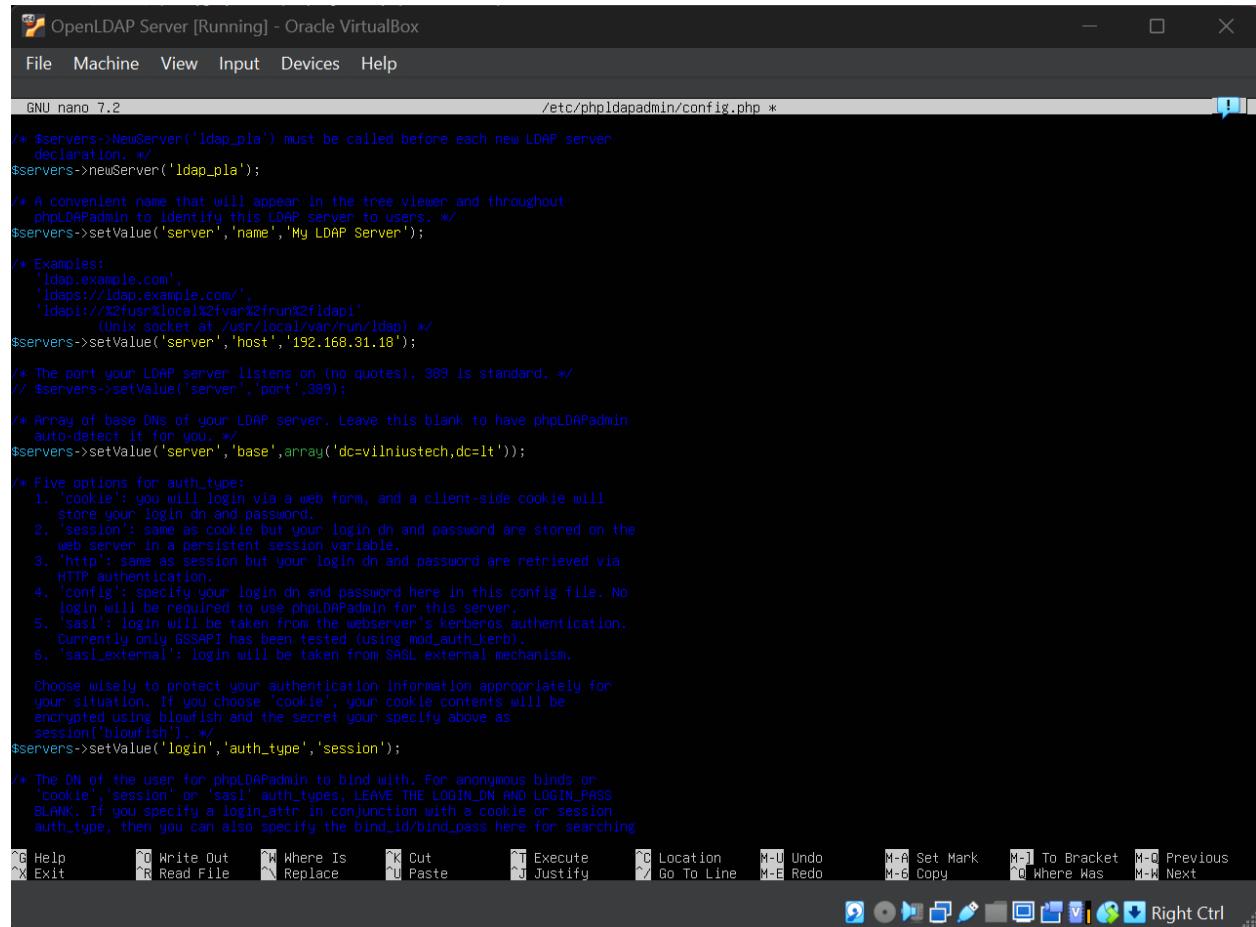
To simplify user management in the OpenLDAP directory, I installed and configured phpLDAPAdmin on the LDAP server with `sudo apt install phpldapadmin -y`:

```
ldapadmin@ldap-server:~$ sudo apt install phpldapadmin -y
```

I edited config file `sudo nano /etc/phpldapadmin/config.php`:

```
ldapadmin@ldap-server:~$ sudo nano /etc/phpldapadmin/config.php
```

There, I set host to server ip address and base to `dc=vilniustech,dc=lt`:



The screenshot shows a terminal window titled "OpenLDAP Server [Running] - Oracle VirtualBox". The window contains the configuration file for phpLDAPAdmin, specifically `/etc/phpldapadmin/config.php`. The file is a PHP script with various configuration parameters. Key settings include setting the host to '192.168.31.18' and the base DN to 'dc=vilniustech,dc=lt'. The configuration file also includes comments explaining the purpose of each parameter and how to protect authentication information.

```
/* $servers->NewServer('ldap_pla') must be called before each new LDAP server declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout phpLDAPAdmin to identify this LDAP server to users. */
$servers->setValue('server','name','My LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com',
   'ldapi://%fusr@local%2fvar%2frun%2fldapi'
   (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.31.18');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPAdmin auto-detect it for you. */
$servers->setValue('server','base',array('dc=vilniustech,dc=lt'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via HTTP authentication.
   4. 'config': specify your login dn and password here in this config file. No login will be required to use phpLDAPAdmin for this server.
   5. 'sasl': login will be taken from the webserver's kerberos authentication.
   Currently only GSSAPI has been tested (using mod_auth_kerb).
   6. 'sasl_external': login will be taken from SASL external mechanism.

choose wisely to protect your authentication information appropriately for your situation. If you choose 'cookie', your cookie contents will be encrypted using blowfish and the secret you specify above as session[ blowfish ]. */
$servers->setValue('login','auth_type','session');

/* The DN of the user for phpLDAPAdmin to bind with. For anonymous binds or 'cookie' 'session' or 'sasl' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS BLANK. If you specify a login_attr in conjunction with a cookie or session auth_type, then you can also specify the bind_id/bind_pass here for searching
auth_type.

$ servers->setValue('login','bind_dn','');
$ servers->setValue('login','bind_pass','');
$ servers->setValue('login','bind_id','');
$ servers->setValue('login','bind_attr','');
$ servers->setValue('login','bind_type','');
$ servers->setValue('login','bind_scope','');
$ servers->setValue('login','bind_base','');
$ servers->setValue('login','bind_ldap','');
```

Then, to secure communication between the browser and phpLDAPAdmin I implemented SSL on the Apache web server. I enabled SSL module with `sudo a2enmod ssl` command:

```
ldapadmin@ldap-server:~$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
ldapadmin@ldap-server:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

I opened the default SSL configuration file `sudo nano /etc/apache2/sites-available/default-ssl.conf`:

```
ldapadmin@ldap-server:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

There, I put `SSLCertificateFile` to `/etc/ldap/ssl/ldap_cert.pem` and `SSLCertificateKeyFile` to `/etc/ldap/ssl/ldap_key.pem`:

The screenshot shows a terminal window titled "OpenLDAP Server [Running] - Oracle VirtualBox". The window contains the Apache configuration file /etc/apache2/sites-available/default-ssl.conf. The code includes sections for SSL Engine, Certificate Chain, and Certificate Authority (CA). The configuration is set up for port 443, using self-signed certificates from /etc/ldap/ssl/.

```

GNU nano 7.2                               /etc/apache2/sites-available/default-ssl.conf *
<VirtualHost *:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    # SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile      /etc/ldap/ssl/ldap_cert.pem
    SSLCertificateKeyFile  /etc/ldap/ssl/ldap_key.pem

    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convenience.
    #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

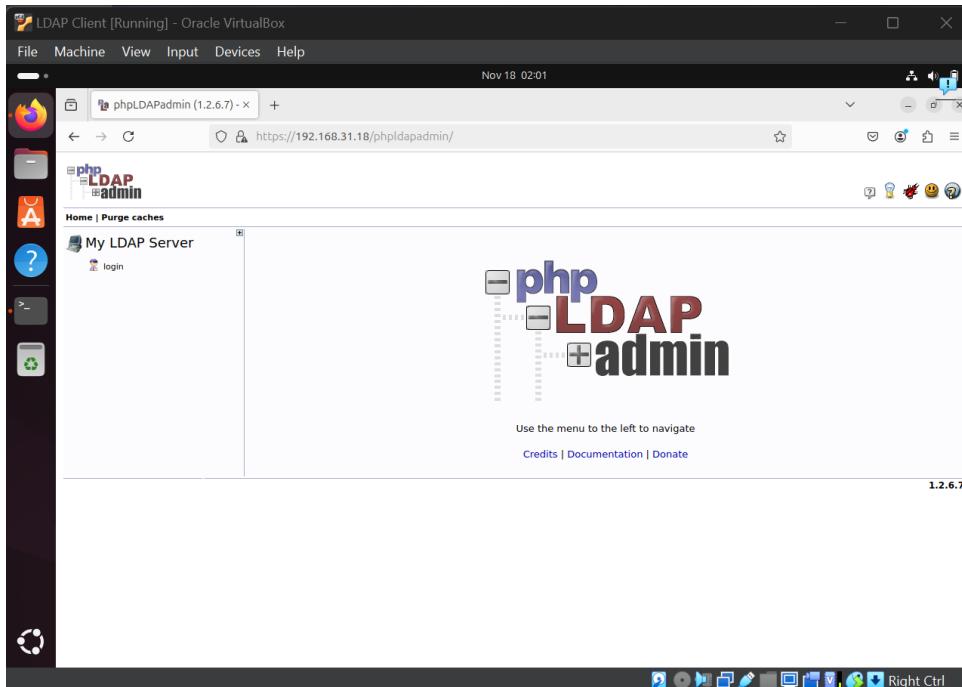
    # Certificate Authority (CA):
    # Set the CA certificate verification path where to find CA
    # certificates for client authentication or alternatively one
    # huge file containing all of them (file must be PEM encoded)

```

I restarted service with `sudo systemctl restart apache2` command to apply the changes:

```
ldapadmin@ldap-server:~$ sudo systemctl restart apache2
```

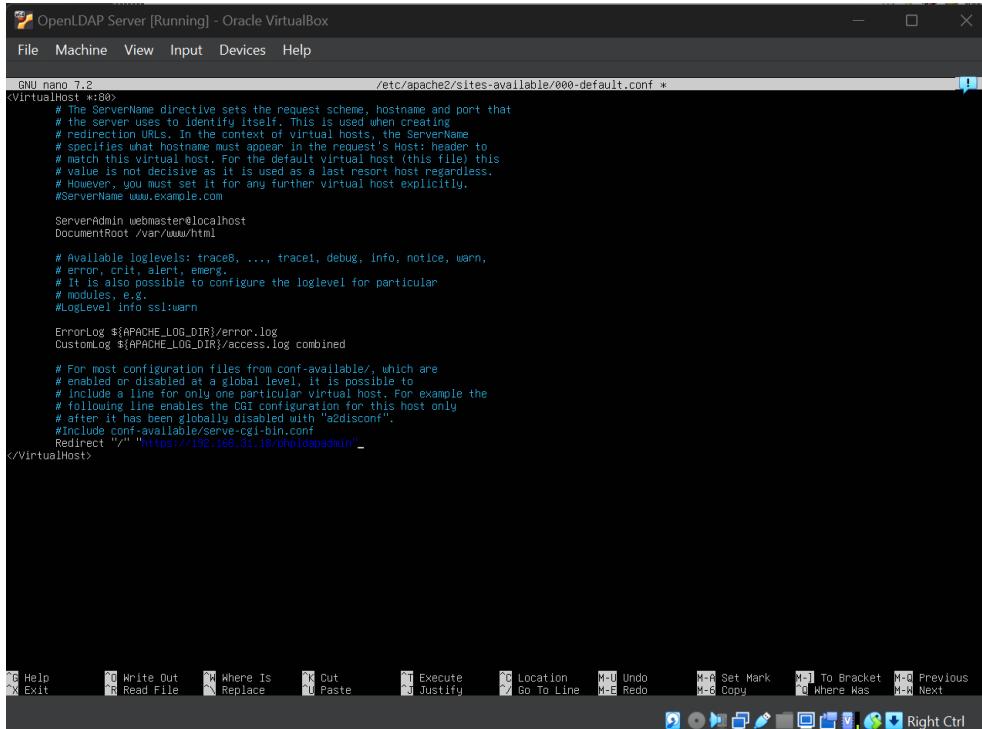
This configuration enabled secure access to phpLDAPAdmin via HTTPS:



I also did that only via https it could be accessed by editing `sudo nano /etc/apache2/sites-available/000-default.conf`:

```
ldapadmin@ldap-server:~$ sudo nano /etc/apache2/sites-available/000-default.conf
```

I added a redirect rule to automatically redirect all HTTP requests to the HTTPS phpLDAPAdmin page:



```
GNU nano 7.2  /etc/apache2/sites-available/000-default.conf *
```

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

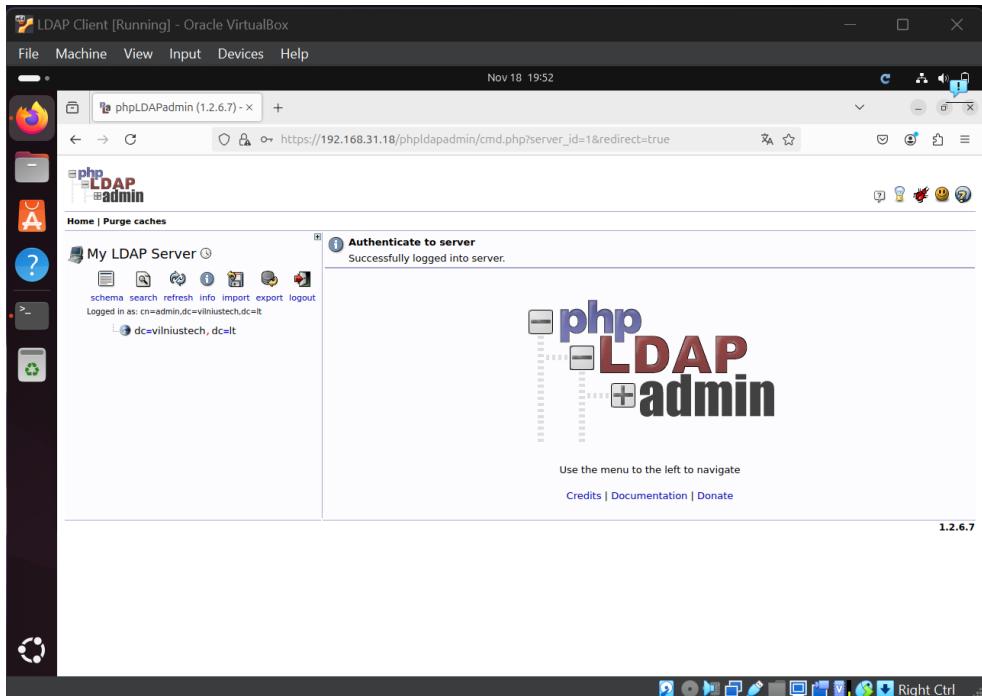
    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the cgi configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
    Redirect "/" "https://192.168.31.18/phpLDAPadmin"
</VirtualHost>
```

Help    Write Out    Where Is    Cut    Execute    Location    Undo    Set Mark    To Bracket    Previous  
Exit    Read File    Replace    Paste    Justify    Go To Line    Redo    Copy    Where Was    Next

Once again, I restarted apache2 with `sudo systemctl restart apache2`:

```
ldapadmin@ldap-server:~$ sudo systemctl restart apache2
```

I logged in to phpLDAPAdmin with admin account:



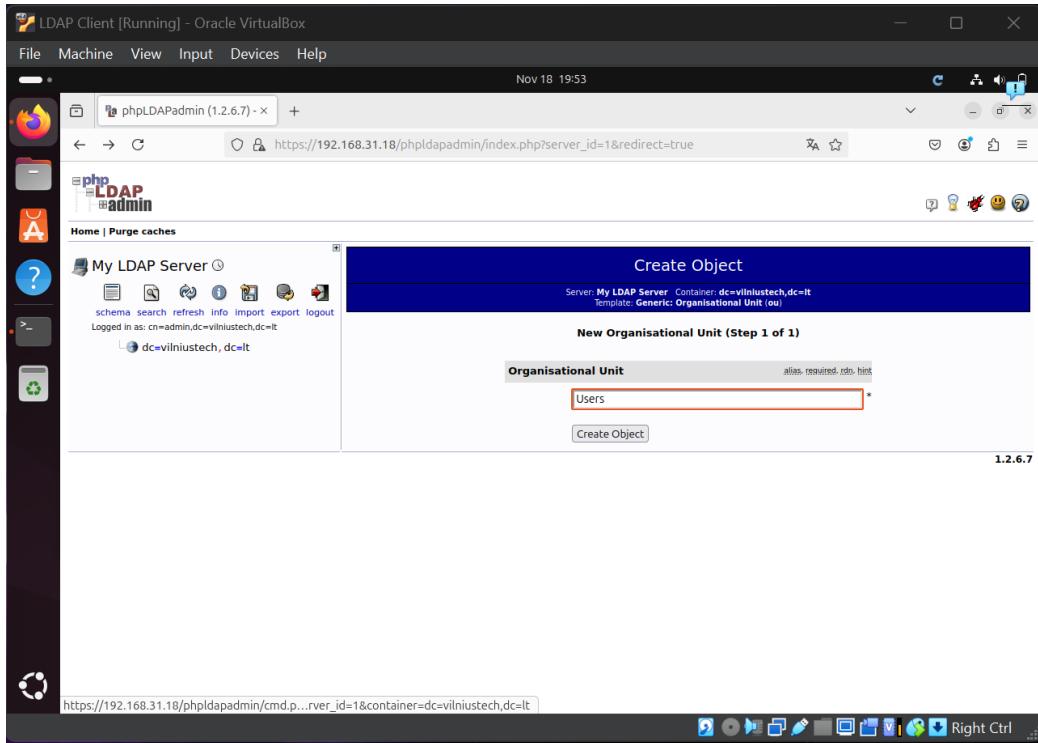
Then, for `dc=vilniustech, dc=lt` I created a child entry:

The screenshot shows the phpLDAPAdmin interface in a web browser. The URL is `https://192.168.31.18/phpldapadmin/crud.php?server_id=1&redirect=true`. The main title bar says "My LDAP Server". The left sidebar shows "My LDAP Server" with a list of operations: schema, search, refresh, info, import, export, logout. Below this, it shows the current container: `dc=vilniustech, dc=lt`. The main panel has a title "dc=vilniustech" and a sub-header "Server: My LDAP Server Distinguished Name: dc=vilniustech,dc=lt Template: Default". It contains several buttons: 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. A note says "Hint: To delete an attribute, empty the text field and click save." Another note says "Hint: To view the schema for an attribute, click the attribute name." Below these are three input fields: "dc" with value "vilniustech" and a "(rename)" link; "o" with value "Vilnius Tech" and a "(add value)" link; and "objectClass" with values "top" and "dcObject". At the bottom are standard browser navigation buttons.

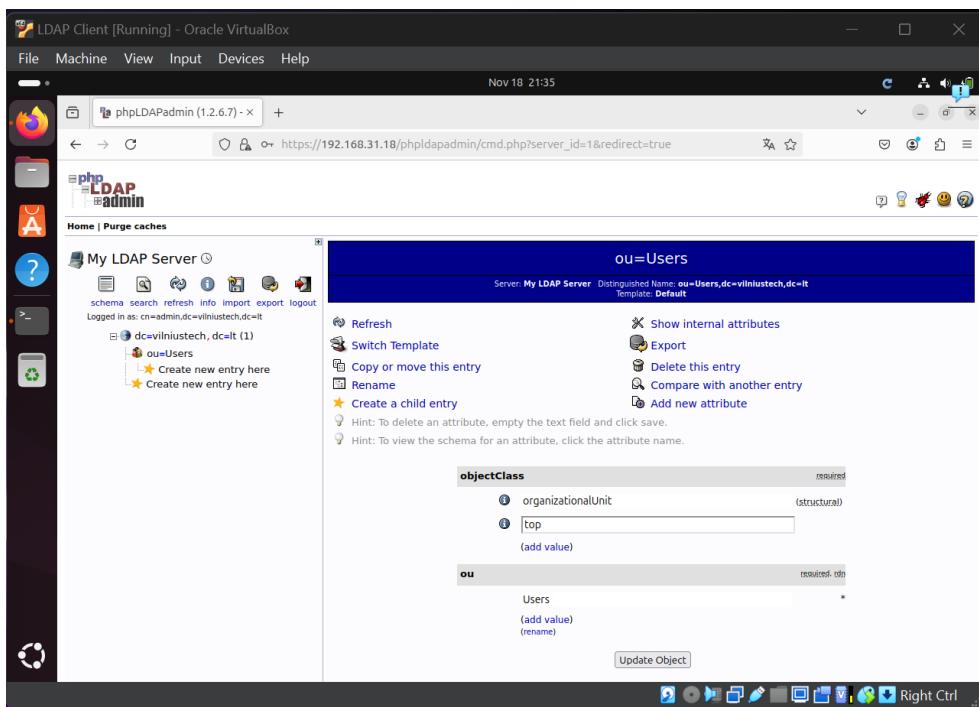
I selected “Generic: Organisational Unit”:

The screenshot shows the "Create Object" page of phpLDAPAdmin. The title bar says "Create Object" and the sub-header says "Server: My LDAP Server Container: dc=vilniustech,dc=lt". The main content area is titled "Select a template for the creation process". It lists "Templates:" on the left and various object types on the right, each with a radio button. The templates listed are: 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: Domain, Samba: Group Mapping, Samba: Machine, Sendmail: Alias, Sendmail: Cluster, Sendmail: Domain, Sendmail: Relays, Sendmail: Virtual Domain, Sendmail: Virtual Users, Thunderbird: Address Book Entry, and Default. At the bottom right of the template list is the version "1.2.6.7". The browser address bar shows the URL `https://192.168.31.18/phpldapadmin/crud.php?server_id=1&container=dc=vilniustech,dc=lt`.

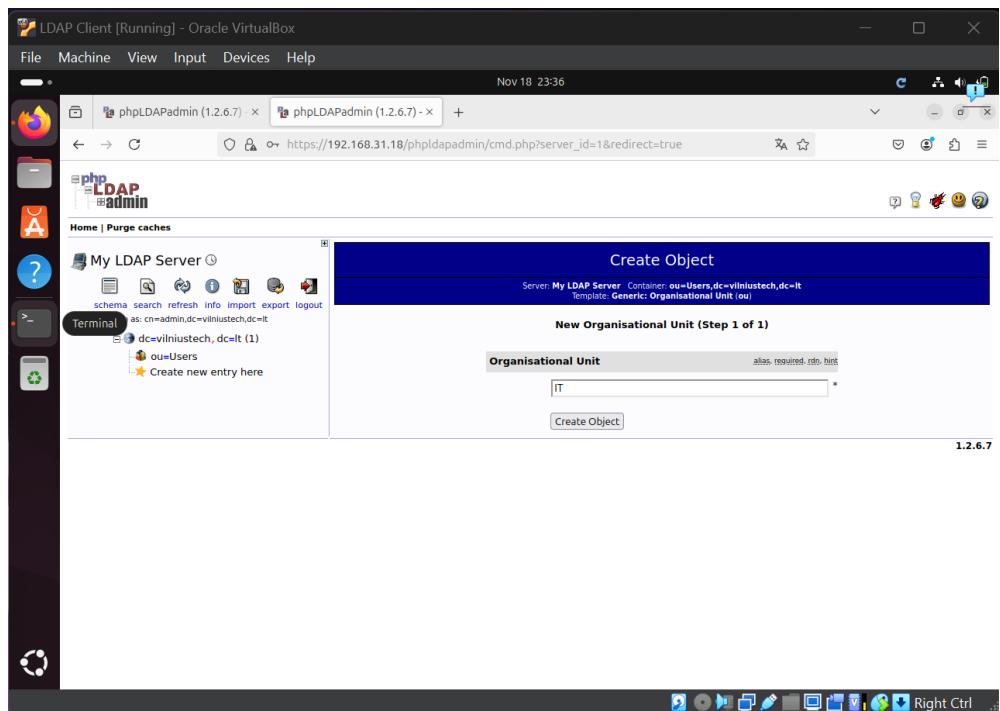
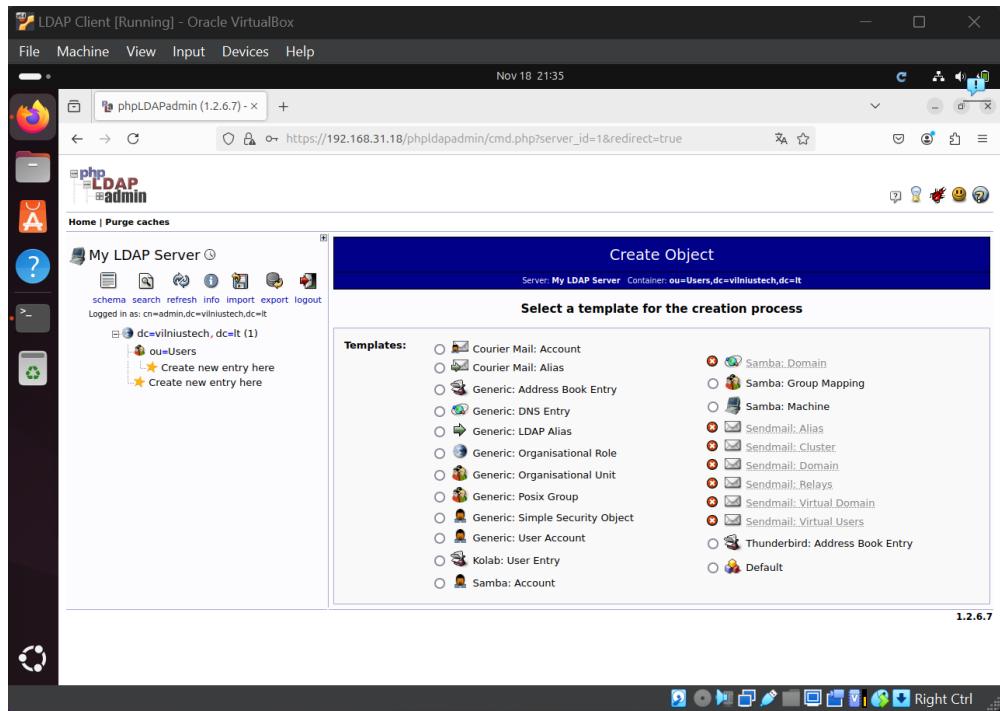
Then, I named that unit as “Users”:

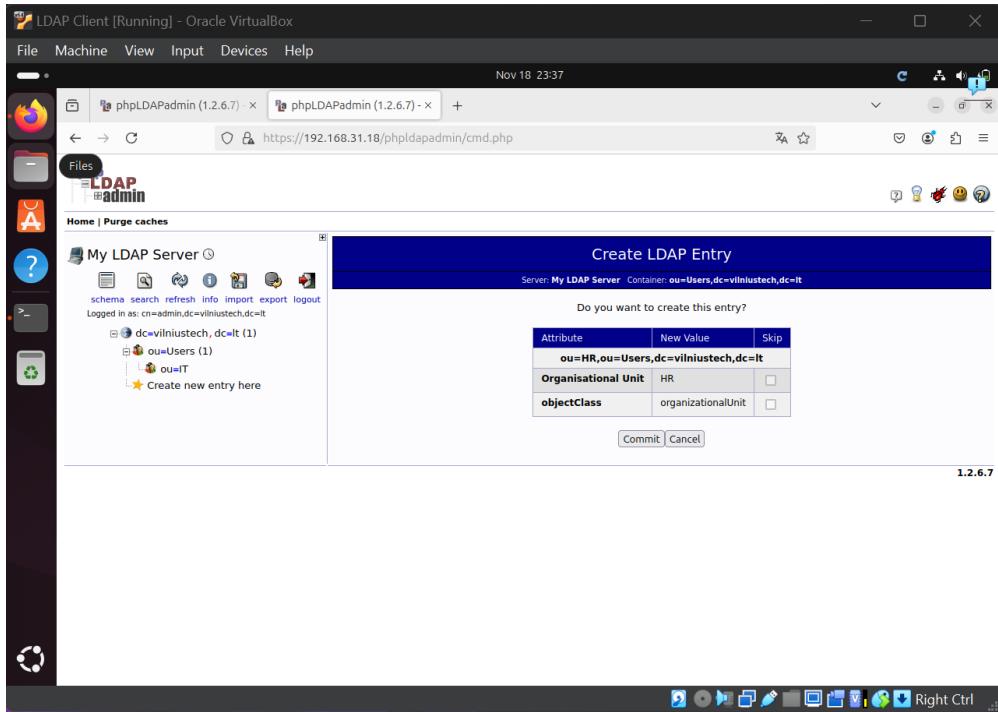


It was created successfully:

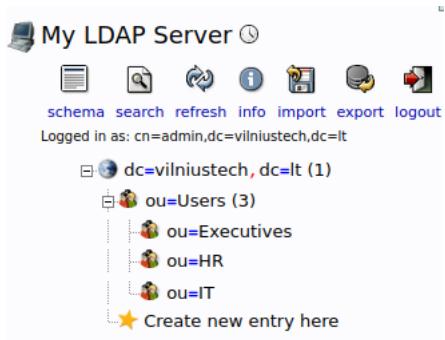


Then, I created “Generic: Organisational Unit” for Users – IT, HR, and Executives. Each OU represents a department, making it easier to manage users based on their roles and responsibilities.

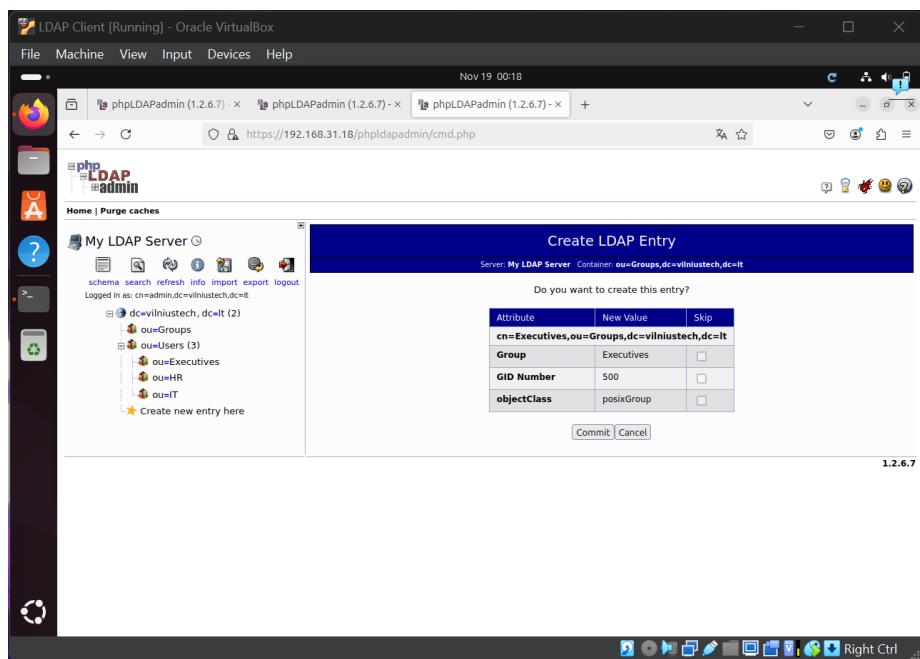
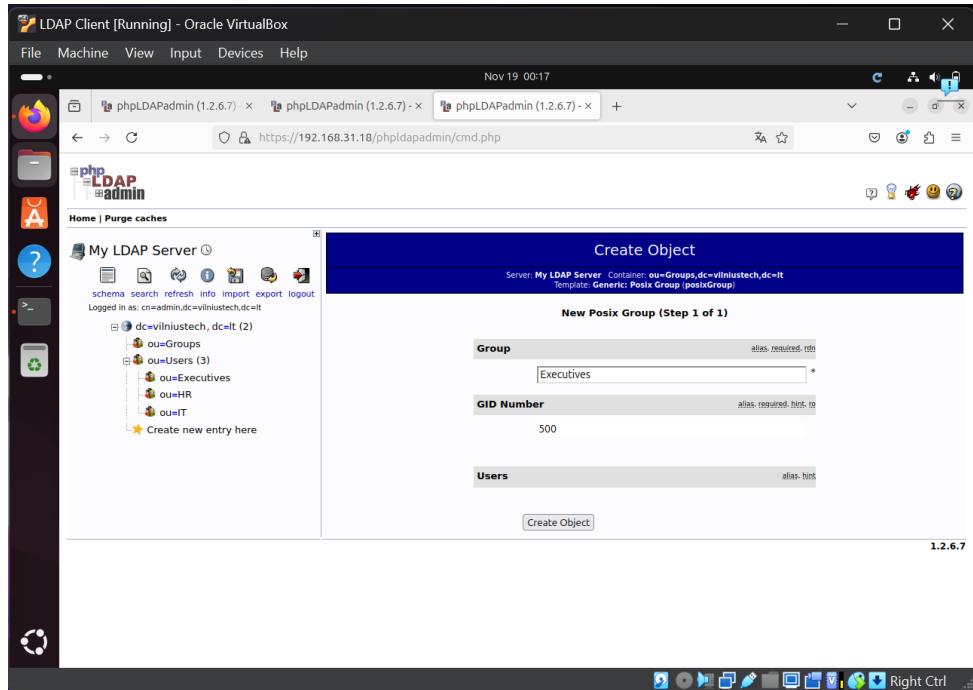




When everything was created it looked like this:



Then, I created an organizational unit for groups to create posix groups with GID numbers so I could add users:



As the groups were created I started creating user accounts:

The screenshot shows the phpLDAPadmin interface running in a Firefox browser window titled "LDAP Client [Running] - Oracle VirtualBox". The URL is <https://192.168.31.18/phpldapadmin/cmd.php>. The left sidebar shows the LDAP tree structure under "My LDAP Server". The main panel displays the "Create Object" form for a "New User Account (Step 1 of 1)". The form fields are as follows:

Field	Value	Type
First name	[Empty]	alias
Last name	[Empty]	alias, required
Common Name	[Empty]	alias, required, rdn
User ID	[Empty]	alias, required
Password	[Empty]	alias, hint

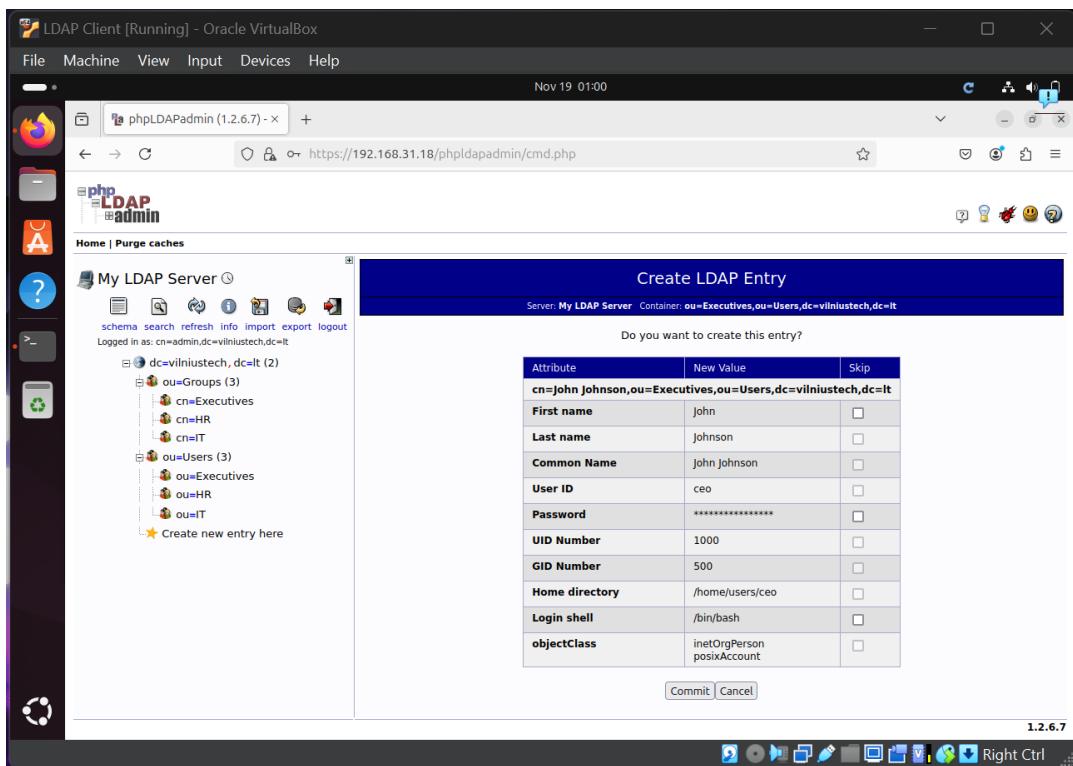
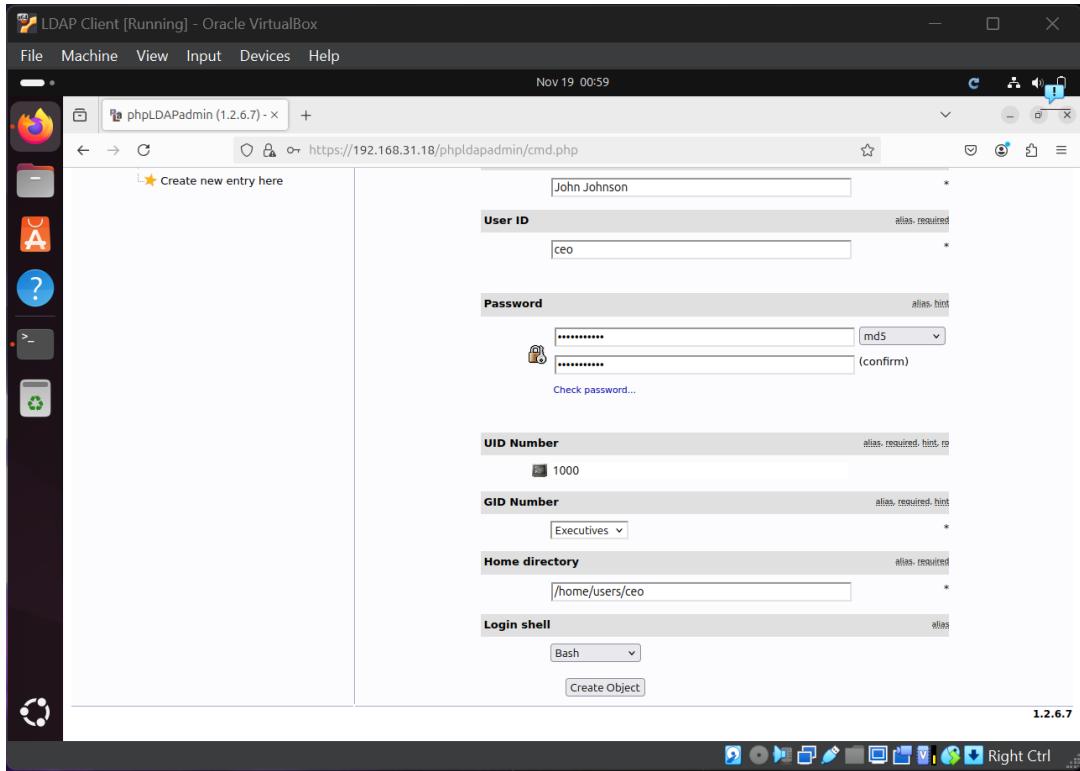
The "User ID" field has a dropdown menu set to "md5" and a "confirm" field below it. The "Common Name" field is highlighted in yellow.

Here, I would fill the details, give user id and select group from created groups:

The screenshot shows the phpLDAPadmin interface running in a Firefox browser window titled "LDAP Client [Running] - Oracle VirtualBox". The URL is <https://192.168.31.18/phpldapadmin/cmd.php>. The left sidebar shows the LDAP tree structure under "My LDAP Server". The main panel displays the "Create Object" form for a "New User Account (Step 1 of 1)". The form fields are as follows:

Field	Value	Type
First name	John	alias
Last name	Johnson	alias, required
Common Name	John Johnson	alias, required, rdn
User ID	ceo	alias, required
Password	[Redacted]	alias, hint

The "Last name" and "Common Name" fields have been populated with "Johnson". The "User ID" field contains "ceo". The "Password" field is filled with a redacted value. The "User ID" dropdown menu is still set to "md5".



I also added additional attributes, such as titles:

The screenshot shows the phpLDAPadmin interface on a Windows desktop. The title bar reads "LDAP Client [Running] - Oracle VirtualBox". The main window displays a tree view of the LDAP schema under "My LDAP Server". A context menu is open over a newly created entry "cn=John Johnson,cn=Users,dc=vilniustech,dc=lt". The menu includes options like Refresh, Switch Template, Copy or move this entry, Rename, Create a child entry, and Add Attribute. The "Add Attribute" section is expanded, showing fields for "cn" (with value "John Johnson") and "gidNumber" (with value "500"). The status bar at the bottom right shows "Right Ctrl".

The screenshot shows the phpLDAPadmin interface on a Windows desktop. The title bar reads "LDAP Client [Running] - Oracle VirtualBox". The main window displays a tree view of the LDAP schema under "My LDAP Server". A context menu is open over an entry "cn=John Johnson,cn=Users,dc=vilniustech,dc=lt". The menu includes options like Refresh, Switch Template, Copy or move this entry, Rename, Create a child entry, and Add Attribute. The "Add Attribute" section is expanded, showing fields for "cn" (with value "John Johnson") and "gidNumber" (with value "500"). The status bar at the bottom right shows "Right Ctrl".

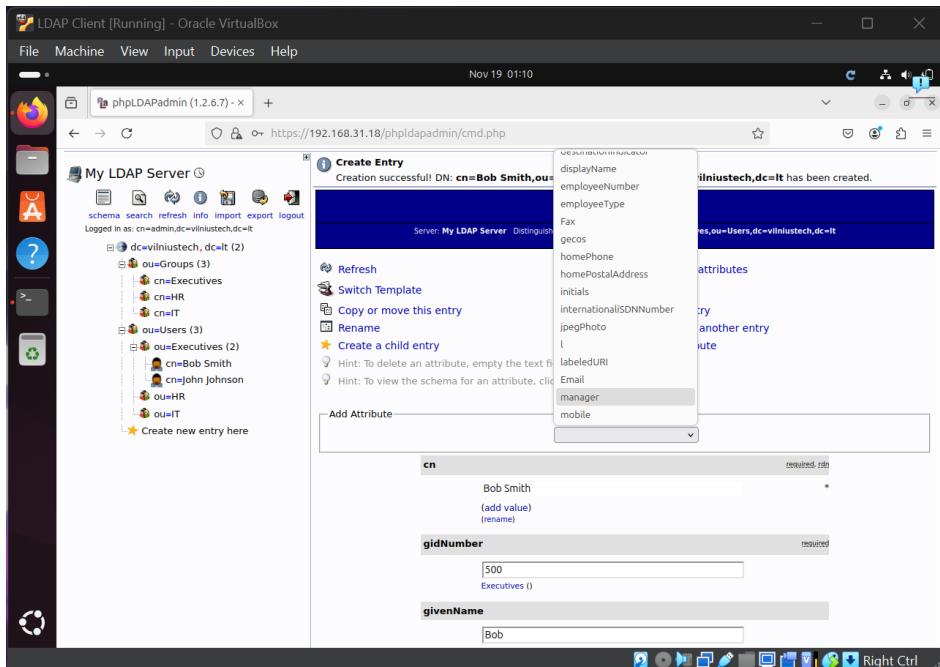
I also added additional attributes such as emails:

The screenshot shows the phpLDAPadmin interface running in Oracle VirtualBox. The left sidebar displays the LDAP tree structure under 'My LDAP Server'. The main panel shows the entry for 'cn=John Johnson, ou=Users, dc=vilniustech, dc=it'. The 'Email' attribute is currently set to 'john.johnson@vilniustech.lt'. A tooltip at the bottom left of the 'Email' input field states: 'An attribute (Email) was modified and is highlighted below.'

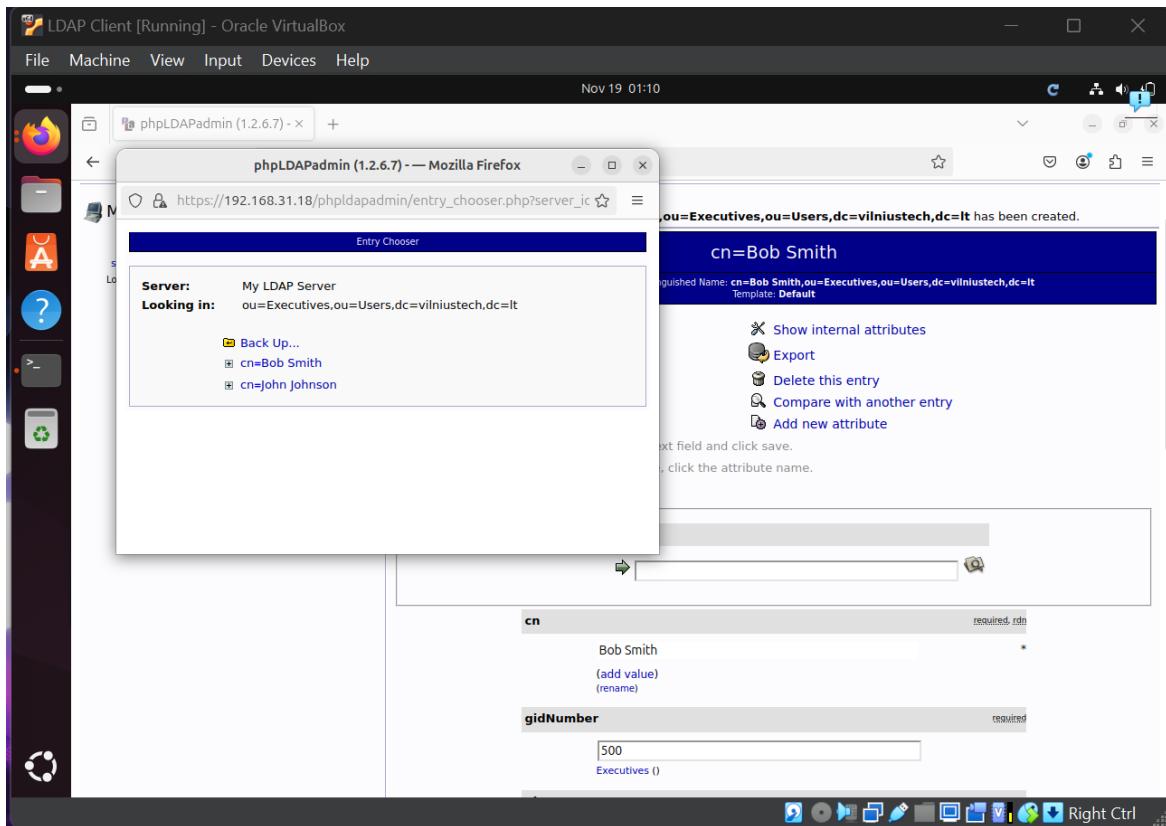
Then, I added new attributes by clicking “Add new attribute”:

The screenshot shows the phpLDAPadmin interface running in Oracle VirtualBox. The left sidebar displays the LDAP tree structure under 'My LDAP Server'. The main panel shows the entry for 'cn=John Johnson, ou=Users, dc=vilniustech, dc=it'. A new attribute 'managers' has been added below 'Email', with a placeholder value '(add value)'.

For hierarchy, I added “managers”:



I made hierarchy so that CTO would have manager CEO, HR lead would have manager CEO, HRs would have manager HR lead, IT Team Lead would have manager CTO and other IT team members would have manager IT Team Lead:



LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:11

phpLDAPAdmin (1.2.6.7) - + https://192.168.31.18/phpLDAPadmin/cmd.php

My LDAP Server

schema search refresh info import export logout

Logged in as: cn=admin,dc=vilniustech,dc=lt

dc=vilniustech, dc=lt (2)

- ou=Groups (3)
  - cn=Executives
  - cn=HR
  - cn=IT
- ou=Users (3)
  - ou=Executives (2)
    - cn=Bob Smith
    - cn=John Johnson
  - ou=HR
  - ou=IT

Create new entry here

Create Entry

Creation successful! DN: cn=Bob Smith,ou=Executives,ou=Users,dc=vilniustech,dc=lt has been created.

cn=Bob Smith

Server: My LDAP Server Distinguished Name: cn=Bob Smith,ou=Executives,ou=Users,dc=vilniustech,dc=lt 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.  
Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

manager

cn Bob Smith required, rdn  
(add value)  
(rename)

gidNumber 500 required  
500 Executives

Right Ctrl

The screenshot shows the phpLDAPAdmin interface after creating a new entry. The entry 'cn=Bob Smith' was successfully created under the 'ou=Executives' container. The 'cn' attribute is set to 'Bob Smith' and the 'gidNumber' attribute is set to '500'.

LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:11

phpLDAPAdmin (1.2.6.7) - + https://192.168.31.18/phpLDAPadmin/cmd.php

Home | Purge caches

My LDAP Server

schema search refresh info import export logout

as: cn=admin,dc=vilniustech,dc=lt

dc=vilniustech, dc=lt (2)

- ou=Groups (3)
  - cn=Executives
  - cn=HR
  - cn=IT
- ou=Users (3)
  - ou=Executives (2)
    - cn=Bob Smith
    - cn=John Johnson
  - ou=HR
  - ou=IT

Create new entry here

cn=Bob Smith

Server: My LDAP Server Distinguished Name: cn=Bob Smith,ou=Executives,ou=Users,dc=vilniustech,dc=lt

You want to make these changes?

Attribute	Old Value	New Value	Skip
manager	[attribute doesn't exist]	cn=John Johnson,ou=Executives,ou=Users,dc=vilniustech,dc=lt	<input type="checkbox"/>

Update Object Cancel

1.2.6.7

Right Ctrl

The screenshot shows a confirmation dialog for updating the 'manager' attribute of the 'cn=Bob Smith' entry. The 'New Value' field contains the full distinguished name 'cn=John Johnson,ou=Executives,ou=Users,dc=vilniustech,dc=lt'.

LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:15

phpLDAPAdmin (1.2.6.7) - x + https://192.168.31.18/phpLDAPAdmin/cmd.php

schema search refresh info import export logout

Logged in as: cn=admin,dc=vilniustech,dc=lt

Server: My LDAP Server Distinguished Name: cn=Laura Adams,ou=HR,ou=Users,dc=vilniustech,dc=lt Template: Default

dc=vilniustech, dc=lt (2)

- ouGroups (3)
  - cn=Executives
  - cn=HR
  - cn=IT
- ouUsers (3)
  - ou=Executives (2)
    - cn=Bob Smith
    - cn=John Johnson
  - ou=HR (1)
    - cn=Laura Adams
  - ou=IT

Create new entry here

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

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

manager

cn Laura Adams (add value) (rename)

gidNumber 501 HR ()

givenName Laura

Right Ctrl

The screenshot shows the phpLDAPAdmin interface on a Linux desktop. The left sidebar shows the LDAP tree structure under 'My LDAP Server'. The main panel displays the creation of a new user entry 'cn=Laura Adams'. The 'Add Attribute' section has 'manager' selected, with the value 'cn=John Johnson,ou=Executives,ou=Users,dc=vilniustech,dc=lt'. Other fields like 'cn', 'gidNumber', and 'givenName' are also visible. A success message at the top right indicates the entry was created successfully.

LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:17

phpLDAPAdmin (1.2.6.7) - x + https://192.168.31.18/phpLDAPAdmin/cmd.php

My LDAP Server

schema search refresh info import export logout

Logged in as: cn=admin,dc=vilniustech,dc=lt

dc=vilniustech, dc=lt (2)

- ouGroups (3)
  - cn=Executives
  - cn=HR
  - cn=IT
- ouUsers (3)
  - ou=Executives (2)
    - cn=Bob Smith
    - cn=John Johnson
  - ou=HR (2)
    - cn=Laura Adams
    - cn=Sarah Lee
  - ou=IT

Create new entry here

i Create Entry Creation successful! DN: cn=Sarah Lee,ou=HR,ou=Users,dc=vilniustech,dc=lt has been created.

cn=Sarah Lee

Server: My LDAP Server Distinguished Name: cn=Sarah Lee,ou=HR,ou=Users,dc=vilniustech,dc=lt Template: Default

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

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

manager

cn cn=Sarah Lee (add value) (rename)

gidNumber 501 HR ()

givenName

Right Ctrl

This screenshot shows the continuation of the user creation process. The 'Create Entry' message from the previous step is still visible. The 'Add Attribute' section now shows 'cn' with the value 'cn=Sarah Lee'. The 'gidNumber' field is set to 501. The 'givenName' field is empty. The 'Right Ctrl' button is highlighted at the bottom right of the interface.

LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:19

phpLDAPadmin (1.2.6.7) https://192.168.31.19/phpLDAPadmin/cmd.php

My LDAP Server

Home | Purge caches

My LDAP Server Distinguished Name: cn=jon jones,ou=HR,ou=Users,dc=vilniustech,dc=lt

Logged in as: cn=admin,dc=vilniustech,dc=lt

schema search refresh info import export logout

Attribute Old Value New Value Skip

manager [attribute doesn't exist] cn=Laura Adams,ou=HR,ou=Users,dc=vilniustech,dc=lt

Do you want to make these changes?

Update Object Cancel

1.2.6.7

Right Ctrl

This screenshot shows the phpLDAPadmin interface on a Linux desktop. A dialog box is open for modifying the user entry 'cn=jon jones'. The 'manager' attribute is being updated from its non-existent state to 'cn=Laura Adams,ou=HR,ou=Users,dc=vilniustech,dc=lt'. The 'Skip' checkbox is unchecked. Below the dialog, a message asks if the user wants to make these changes, with 'Update Object' and 'Cancel' buttons.

LDAP Client [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Nov 19 01:22

phpLDAPadmin (1.2.6.7) https://192.168.31.18/phpLDAPadmin/cmd.php

My LDAP Server

cn=Petras Petraitis

Server: My LDAP Server Distinguished Name: cn=Petras Petraitis,ou=IT,ou=Users,dc=vilniustech,dc=lt Template: Default

Refresh Switch Template Export Delete this entry Rename Compare with another entry Add new attribute

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

manager

cn Petras Petraitis (add value) (rename)

gidNumber 502 IT ()

givenName Petras

Right Ctrl

This screenshot shows the phpLDAPadmin interface on a Linux desktop. A dialog box is open for creating a new entry 'cn=Petras Petraitis'. The 'manager' attribute is set to 'cn=Bob Smith,ou=Executives,ou=Users,dc=vilniustech,dc=lt'. The 'cn' attribute is set to 'Petras Petraitis'. The 'gidNumber' attribute is set to '502'. The 'givenName' attribute is set to 'Petras'. The 'Add Attribute' section shows other attributes like 'cn' and 'gidNumber' with their current values and edit buttons.



I also tried to search in server for users whose manager is “Petras Petraitis”:

```
ldapadmin@ldap-server:~$ ldapsearch -H ldaps://localhost -x -D "cn=admin,dc=vilniustech,dc=lt" -w password123 -b "dc=vilniustech,dc=lt" "(manager=cn=Petras Petraitis,ou=IT,ou=Users,dc=vilniustech,dc=lt)"
```

```
OpenLDAP Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

uid: it_designer
userPassword:: e01ENX1TQ31CSGFYnRMHRTWC82bUVrZU9BPT0=
uidNumber: 1007
gidNumber: 502
homeDirectory: /home/users/it_designer
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
manager: cn=Petras Petraitis,ou=IT,ou=Users,dc=vilniustech,dc=lt

# John Doe, IT, Users, vilniustech.lt
dn: cn=John Doe,ou=IT,ou=Users,dc=vilniustech,dc=lt
givenName: John
sn: Doe
cn: John Doe
uid: it_productowner
userPassword:: e01ENX1TQ31CSGFYnRMHRTWC82bUVrZU9BPT0=
uidNumber: 1008
gidNumber: 502
homeDirectory: /home/users/it_productowner
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
manager: cn=Petras Petraitis,ou=IT,ou=Users,dc=vilniustech,dc=lt

# Vardenis Pavardenis, IT, Users, vilniustech.lt
dn: cn=Vardenis Pavardenis,ou=IT,ou=Users,dc=vilniustech,dc=lt
givenName: Vardenis
sn: Pavardenis
cn: Vardenis Pavardenis
uid: it_qa
userPassword:: e01ENX1TQ31CSGFYnRMHRTWC82bUVrZU9BPT0=
uidNumber: 1009
gidNumber: 502
homeDirectory: /home/users/it_qa
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
manager: cn=Petras Petraitis,ou=IT,ou=Users,dc=vilniustech,dc=lt

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
ldapadmin@ldap-server:~$
```

Lastly, I tried to login with each user in ldap client:

```
cto@ldap-client:~  
ldap-client@ldap-client:~$ su - it_teamlead  
Password:  
Creating directory '/home/users/it_teamlead'.  
it_teamlead@ldap-client:~$ su - it_developer  
Password:  
Creating directory '/home/users/it_developer'.  
it_developer@ldap-client:~$ su - it_designer  
Password:  
Creating directory '/home/users/it_designer'.  
it_designer@ldap-client:~$ su - it_productowner  
Password:  
Creating directory '/home/users/it_productowner'.  
it_productowner@ldap-client:~$ su - it_qa  
Password:  
Creating directory '/home/users/it_qa'.  
it_qa@ldap-client:~$ su - hr_manager  
Password:  
Creating directory '/home/users/hr_manager'.  
hr_manager@ldap-client:~$ su - hr_recruiter  
Password:  
Creating directory '/home/users/hr_recruiter'.  
hr_recruiter@ldap-client:~$ su - hr_payroll  
Password:  
Creating directory '/home/users/hr_payroll'.  
hr_payroll@ldap-client:~$ su - ceo  
Password:  
Creating directory '/home/users/ceo'.  
ceo@ldap-client:~$ su - cto  
Password:  
Creating directory '/home/users/cto'.  
cto@ldap-client:~$
```