Partea 1:

Studierea si (re)configurarea unui serviciu deja instalat (ex. ssh) #verificati existenta userilor "user1" si "user2" si resetati parolele

```
aso@aso-b:~$ sudo useradd -c "user1" -m -d /home/user1 -s /bin/bash -p $(op
enssl passwd -1 -salt 146 user1pass) user1
aso@aso-b:~$ sudo useradd -c "user2" -m -d /home/user2 -s /bin/bash -p $(op
enssl passwd -1 -salt 146 user2pass) user2
aso@aso-b:~$
```

```
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
user1:x:1001:1001:user1:/home/user1:/bin/bash
user2:x:1002:1002:user2:/home/user2:/bin/bash
aso@aso-b:~$
```

1. Studierea fisierului de configurare PAM(/etc/pam.conf)

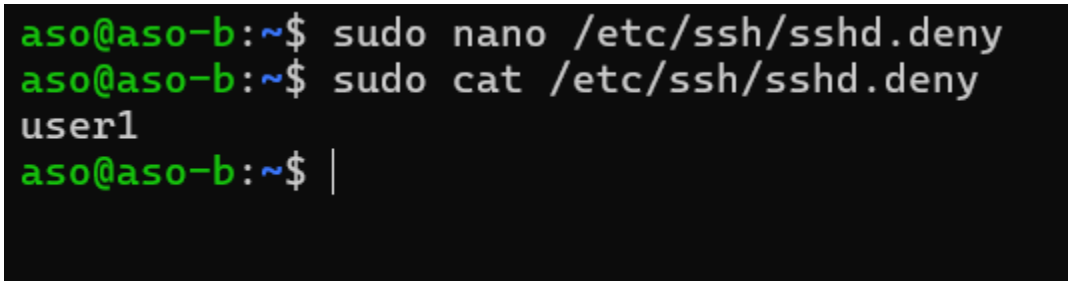
```
aso@aso-b:~$ cat /etc/pam.conf
# ------------------------------------------------------------------------#
# /etc/pam.conf                                                           #
# ------------------------------------------------------------------------#
#
# NOTE
# ----
#
# NOTE: Most program use a file under the /etc/pam.d/ directory to setup their
# PAM service modules. This file is used only if that directory does not exist.
# ------------------------------------------------------------------------#

# Format:
# serv. module     ctrl       module [path]     ...[args..]                 #
# name  type       flag                                                     #

aso@aso-b:~$
```

```
aso@aso-b:~$ cat /etc/pam.d/sshd
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
@include common-auth

# Disallow non-root logins when /etc/nologin exists.
account    required     pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so

# Standard Un*x authorization.
@include common-account

# SELinux needs to be the first session rule.  This ensures that any
# lingering context has been cleared.  Without this it is possible that a
# module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so close

# Set the loginuid process attribute.
session    required     pam_loginuid.so

# Create a new session keyring.
session    optional     pam_keyinit.so force revoke

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional     pam_motd.so  motd=/run/motd.dynamic
session    optional     pam_motd.so noupdate

# Print the status of the user's mailbox upon successful login.
session    optional     pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session    required     pam_limits.so

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session    required     pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session    required     pam_env.so user_readenv=1 envfile=/etc/default/locale

# SELinux needs to intervene at login time to ensure that the process starts
# in the proper default security context.  Only sessions which are intended
# to run in the user's context should be run after this.
session [success=ok ignore=ignore module_unknown=ignore default=bad]        pam_selinux.so open

# Standard Un*x password updating.
@include common-password
aso@aso-b:~$
```

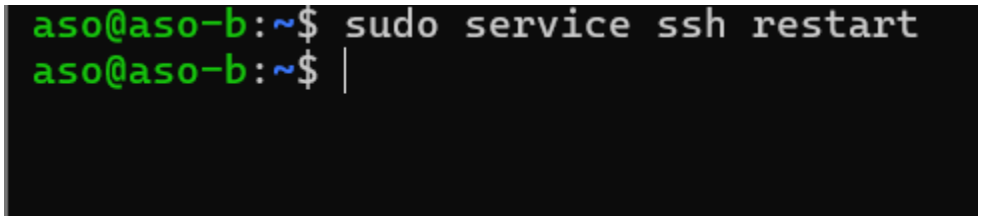
2. Restricționarea accesului unui utilizator specificat
   2.1. Adăugați: "auth required pam_listfile.so item=user sense=deny file=/etc/ssh/sshd.deny onerr=succeed"

```
aso@aso-b:~$ sudo nano /etc/pam.d/sshd
aso@aso-b:~$ cat /etc/pam.d/sshd
# PAM configuration for the Secure Shell service
auth required pam_listfile.so item=user sense=deny file=/etc/ssh/sshd.deny onerr=s
ucceed
```

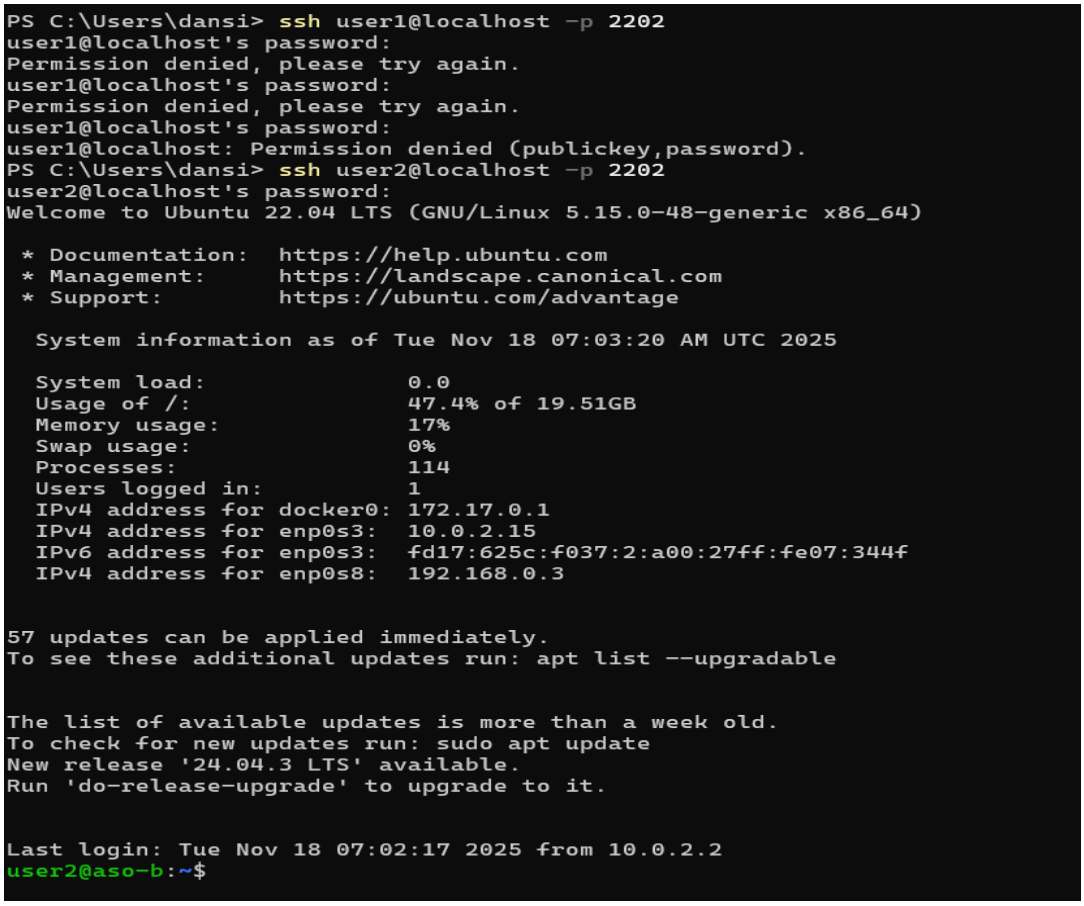
2.2. Adăugați "user1" in "/etc/ssh/sshd.deny".




2.3. Reporniți serviciul ssh: "sudo service ssh restart".




2.4. Verificați conectarea cu user1 si user2 pe serviciul ssh folosit comanda ssh user<N>@localhost



3. Restricționarea completă a unui serviciu (toți utilizatorii)
   3.1. Comentați regula din pasul precedent.
   3.2. Adăugați: "auth required pam_deny.so"

```
aso@aso-b:~$ sudo nano /etc/pam.d/sshd
aso@aso-b:~$ cat /etc/pam.d/sshd
# PAM configuration for the Secure Shell service
#auth required pam_listfile.so item=user sense=deny file=/etc/ssh/sshd.deny onerr=succeed
auth required pam_deny.so
```

   3.3. Reporniți serviciul ssh: "sudo service ssh restart".

```
aso@aso-b:~$ sudo service ssh restart
aso@aso-b:~$
```

   3.4. Verificați conectarea cu user1 si user2 pe serviciul ssh.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements!
 https://aka.ms/PSWindows

PS C:\Users\dansi> ssh user1@localhost -p 2202
user1@localhost's password:
Permission denied, please try again.
user1@localhost's password:
Permission denied, please try again.
user1@localhost's password:
user1@localhost: Permission denied (publickey,password).
PS C:\Users\dansi> ssh user2@localhost -p 2202
user2@localhost's password:
Permission denied, please try again.
user2@localhost's password:
Permission denied, please try again.
user2@localhost's password:
user2@localhost: Permission denied (publickey,password).
PS C:\Users\dansi>
```

4. Adăugarea modulului de restrictionare acces pam_time

4.1. Adăugați regula: "account required pam_time.so" in fisierul "/etc/pam.d/sshd".

```
aso@aso-b:~$ sudo nano /etc/pam.d/sshd
aso@aso-b:~$ sudo cat /etc/pam.d/sshd
# PAM configuration for the Secure Shell service
#auth required pam_listfile.so item=user sense=deny file=/etc/ssh/sshd.deny onerr=succeed
#auth required pam_deny.so
account required pam_time.so

# Standard Un*x authentication.
```

4.2. Adăugați restricție de timp in fisierul "/etc/security/time.conf".

4.3. Studiați exemplelor din "/etc/security/time.conf".

4.4. Restrictionati serviciul "sshd" pentru user1 in ziua de Vineri intre orele 17-20.

```
aso@aso-b:~$ sudo nano /etc/security/time.conf
aso@aso-b:~$ sudo cat /etc/security/time.conf
# this is an example configuration file for the pam_time module. Its syntax
# was initially based heavily on that of the shadow package (shadow-960129).
#
# the syntax of the lines is as follows:
#
#       services;ttys;users;times
#
# white space is ignored and lines maybe extended with '\\n' (escaped
# newlines). As should be clear from reading these comments,
# text following a '#' is ignored to the end of the line.
#
# the combination of individual users/terminals etc is a logic list
# namely individual tokens that are optionally prefixed with '!' (logical
# not) and separated with '&' (logical and) and '|' (logical or).
#
# services
#       is a logic list of PAM service names that the rule applies to.
#
# ttys
#       is a logic list of terminal names that this rule applies to.
#
# users
#       is a logic list of users or a netgroup of users to whom this
#       rule applies.
#
# NB. For these items the simple wildcard '*' may be used only once.
#
# times
#       the format here is a logic list of day/time-range
#       entries the days are specified by a sequence of two character
#       entries, MoTuSa for example is Monday Tuesday and Saturday. Note
#       that repeated days are unset MoMo = no day, and MoWk = all weekdays
#       bar Monday. The two character combinations accepted are
#
#               Mo Tu We Th Fr Sa Su Wk Wd Al
#
#       the last two being week-end days and all 7 days of the week
#       respectively. As a final example, AlFr means all days except Friday.
#
#       each day/time-range can be prefixed with a '!' to indicate "anything
#       but"
#
#       The time-range part is two 24-hour times HHMM separated by a hyphen
#       indicating the start and finish time (if the finish time is smaller
#       than the start time it is deemed to apply on the following day).
#
# for a rule to be active, ALL of service+ttys+users must be satisfied
# by the applying process.
#

#
# Here is a simple example: running blank on tty* (any ttyXXX device),
# the users 'you' and 'me' are denied service all of the time
#

#blank;tty* & !ttyp*;you|me;!Al0000-2400

# Another silly example, user 'root' is denied xsh access
# from pseudo terminals at the weekend and on mondays.

#xsh;ttyp*;root;!WdMo0000-2400

#
# End of example file.
#

sshd;*;user1;Fr1700-2000
aso@aso-b:~$
```

4.5. Verificati accesul cu user1 și user2.

```
PS C:\Users\dansi> ssh user1@localhost -p 2202
user1@localhost's password:
Connection closed by 127.0.0.1 port 2202
PS C:\Users\dansi> ssh user2@localhost -p 2202
user2@localhost's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Nov 18 07:22:31 AM UTC 2025

  System load:              0.0
  Usage of /:               47.4% of 19.51GB
  Memory usage:             17%
  Swap usage:               0%
  Processes:                114
  Users logged in:          1
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for enp0s3:  10.0.2.15
  IPv6 address for enp0s3:  fd17:625c:f037:2:a00:27ff:fe07:344f
  IPv4 address for enp0s8:  192.168.0.3


57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Nov 18 07:11:10 2025 from 10.0.2.2
user2@aso-b:~$ exit
```

5. Adăugarea modulului de stabilire a restrictilor privind parola pam_cracklib

5.1. Instalati modulul libpam-cracklib

```
aso@aso-b:~$ sudo apt-get install libpam-cracklib
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 wamerican
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-cracklib wamerican
0 upgraded, 4 newly installed, 0 to remove and 341 not upgraded.
Need to get 429 kB of archives.
After this operation, 1,898 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ro.archive.ubuntu.com/ubuntu jammy/main amd64 libcrack2
amd64 2.9.6-3.4build4 [29.6 kB]
Get:2 http://ro.archive.ubuntu.com/ubuntu jammy/main amd64 cracklib-r
untime amd64 2.9.6-3.4build4 [149 kB]
Get:3 http://ro.archive.ubuntu.com/ubuntu jammy/main amd64 wamerican
all 2020.12.07-2 [236 kB]
Get:4 http://ro.archive.ubuntu.com/ubuntu jammy-updates/main amd64 li
bpam-cracklib amd64 1.4.0-11ubuntu2.6 [13.5 kB]
Fetched 429 kB in 1s (298 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libcrack2:amd64.
(Reading database ... 114359 files and directories currently installe
d.)
```

5.2. Adaugati modulul cu parametrii "retry=3" si "minlen=6" in fisierul /etc/pam.d/common-password

```
aso@aso-b:~$ sudo nano /etc/pam.d/common-password
aso@aso-b:~$ sudo cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-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 the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# 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.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_cracklib.so retry=3 minlen=6
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password        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
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
aso@aso-b:~$
```

5.3. Anulati restrictiile din time.conf pentru user1

```
#
# Here is a simple example: running blank on tty* (any ttyXXX device),
# the users 'you' and 'me' are denied service all of the time
#

#blank;tty* & !ttyp*;you|me;!Al0000-2400

# Another silly example, user 'root' is denied xsh access
# from pseudo terminals at the weekend and on mondays.

#xsh;ttyp*;root;!WdMo0000-2400

#
# End of example file.
#

#sshd;*;user1;Fr1700-2000
aso@aso-b:~$
```

5.4. Resetati parola pentru user1 si testati parametrii de la pasul precedent.

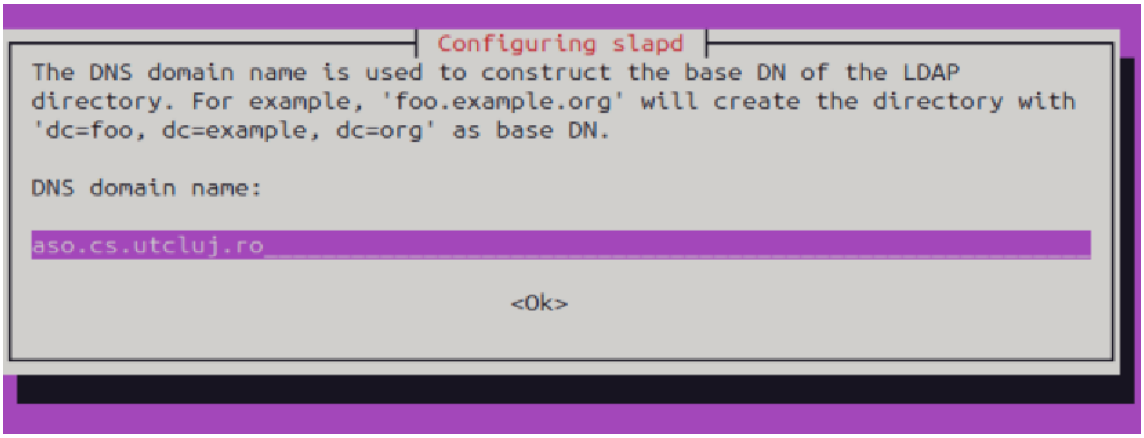
```
user1@aso-b:~$ passwd
Changing password for user1.
Current password:
New password:
BAD PASSWORD: it is WAY too short
New password:
BAD PASSWORD: it is WAY too short
New password:
BAD PASSWORD: it is WAY too short
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
user1@aso-b:~$ passwd
Changing password for user1.
Current password:
New password:
BAD PASSWORD: it is based on a dictionary word
New password:
BAD PASSWORD: it is based on a dictionary word
New password:
Retype new password:
passwd: password updated successfully
user1@aso-b:~$
```

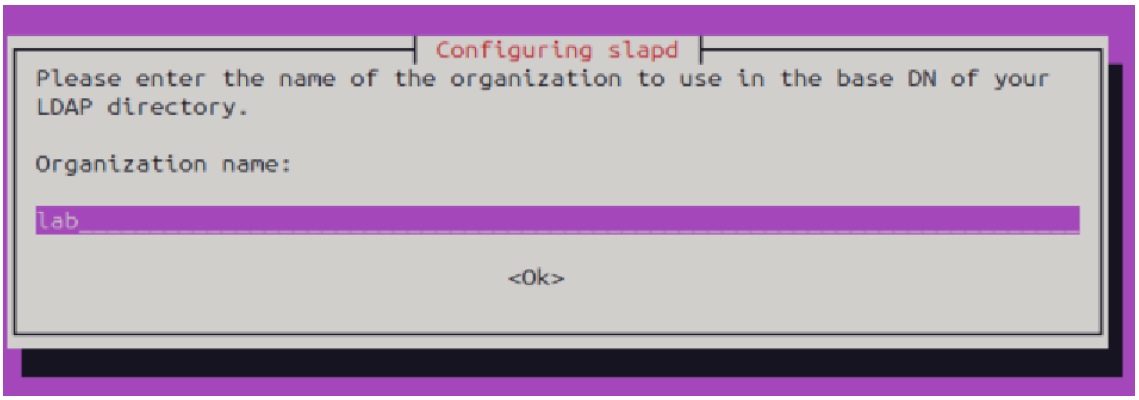
Partea2

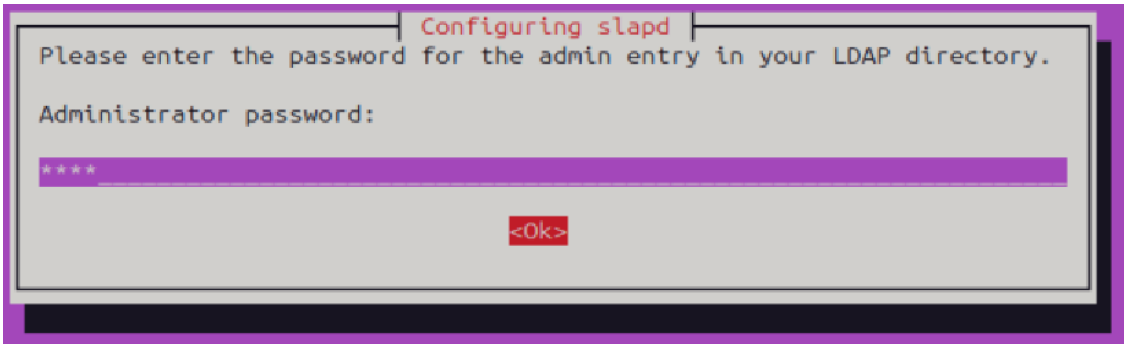
1. Instalare și configurare OpenLDAP
    1.1. Instalați pachetele "slapd" și "ldap-utils" (NOTĂ: la finalul instalării se solicită setarea parolei de admin)

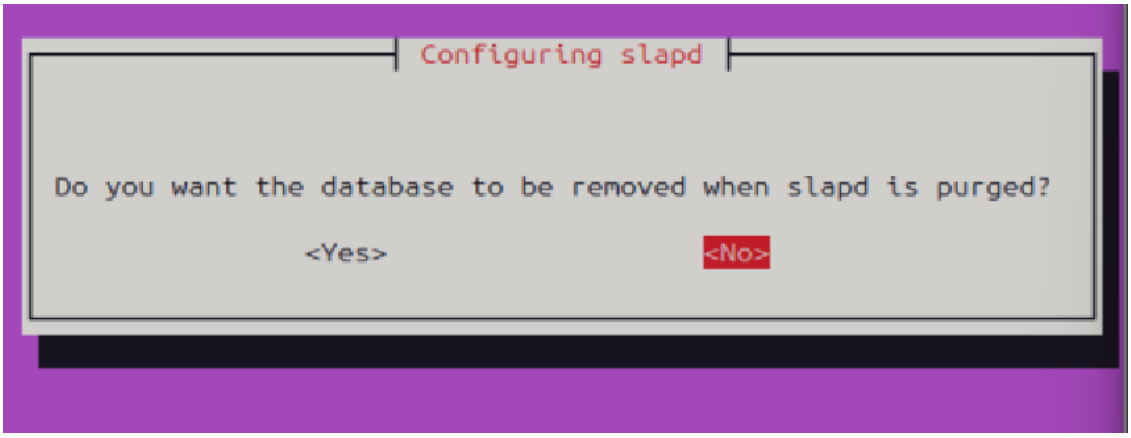
```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
slapd is already the newest version (2.6.7+dfsg-1~exp1ubuntu8.2).
ldap-utils is already the newest version (2.6.7+dfsg-1~exp1ubuntu8.2).
The following packages were automatically installed and are no longer required:
  libaio1t64 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7t64
  libevent-pthreads-2.1-7t64 libfcgi-bin libfcgi-perl libfcgi0t64
  libhtml-template-perl libmecab2 libprotobuf-lite32t64 mecab-ipadic
  mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0
  mysql-common mysql-server-8.0 mysql-server-core-8.0
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 83 not upgraded.
```

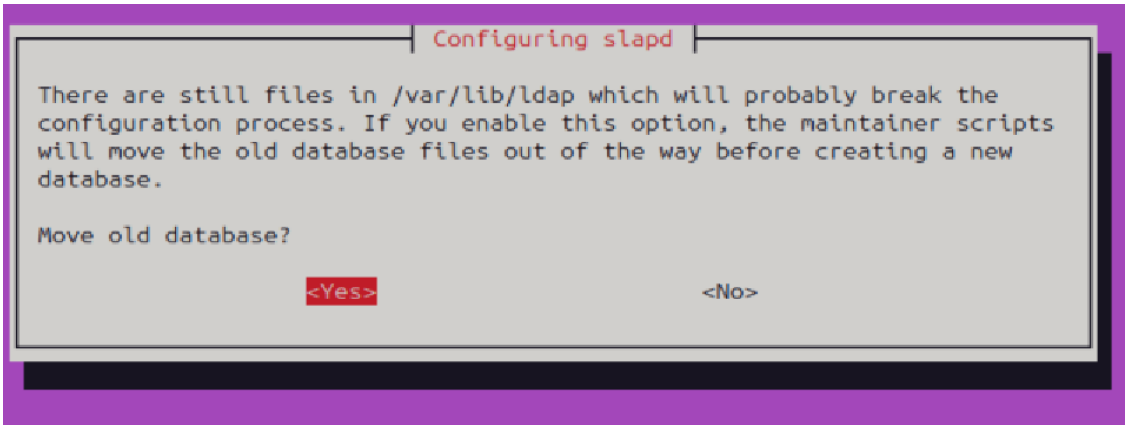
    1.2. Configurați pachetul "slapd" prin executarea comenzii "sudo dpkg-reconfigure slapd"




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


Configuring slapd
Do you want the database to be removed when slapd is purged?
<Yes>
<No>


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>

2. Instalrea și configurarea interfeței Web (phpLDAPadmin) pentru gestiunea LDAP

2.1. Identificati versiunea de php pe care package manager-ul apt il ofera:

```
ubuntu@ubuntu-VirtualBox:~$ apt-cache search php
exuberant-ctags - build tag file indexes of source code definitions
libapache2-mod-php - server-side, HTML-embedded scripting language (Apache 2 module) (default)
libapache2-mod-php8.3 - server-side, HTML-embedded scripting language (Apache 2 module)
libct4 - libraries for connecting to MS SQL and Sybase SQL servers
libcups2-dev - Common UNIX Printing System(tm) - Development files CUPS library
libgtksourceview-5-common - common files for the GTK 4 syntax highlighting widget
libnet-libidn-perl - Perl bindings for GNU Libidn
php - server-side, HTML-embedded scripting language (default)
php-all-dev - package depending on all supported PHP development packages
php-cgi - server-side, HTML-embedded scripting language (CGI binary) (default)
php-cli - command-line interpreter for the PHP scripting language (default)
php-common - Common files for PHP packages
php-curl - CURL module for PHP [default]
php-dev - Files for PHP module development (default)
php-gd - GD module for PHP [default]
php-gmp - GMP module for PHP [default]
php-ldap - LDAP module for PHP [default]
php-mysql - MySQL module for PHP [default]
php-odbc - ODBC module for PHP [default]
php-pear - PEAR Base System
php-pgsql - PostgreSQL module for PHP [default]
php-pspell - pspell module for PHP [default]
php-snmp - SNMP module for PHP [default]
php-sqlite3 - SQLite3 module for PHP [default]
php-tidy - tidy module for PHP [default]
php-xml - DOM, SimpleXML, WDDX, XML, and XSL module for PHP [default]
php8.3 - server-side, HTML-embedded scripting language (metapackage)
php8.3-cgi - server-side, HTML-embedded scripting language (CGI binary)
php8.3-cli - command-line interpreter for the PHP scripting language
php8.3-common - documentation, examples and common module for PHP
php8.3-curl - CURL module for PHP
php8.3-dev - Files for PHP8.3 module development
php8.3-gd - GD module for PHP
php8.3-gmp - GMP module for PHP
php8.3-ldap - LDAP module for PHP
```

2.2. Instalați pachetele "apache2", "php", "php-ldap", "libapache2-mod-php"

A fost nevoie sa dezinstalez tot:

# Oprește Apache
sudo systemctl stop apache2

# Dezactivează modulul PHP 5.6
sudo a2dismod php5.6

# Dezinstalare completă PHP 5.6
sudo apt-get purge -y php5.6 php5.6-* libapache2-mod-php5.6

# Curățare
sudo apt-get autoremove -y
sudo apt-get autoclean

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get install -y php7.4 php7.4-ldap libapache2-mod-php7.4 php7.4-xml php7.4-mbstring php7.4-gd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libsodium23 php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php7.4 libsodium23 php-common php7.4 php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-opcache php7.4-readline php7.4-xml
0 upgraded, 13 newly installed, 0 to remove and 117 not upgraded.
```

Am activat PHP 7.4 in Apache:

```
ubuntu@ubuntu-VirtualBox:~$ sudo a2enmod php7.4
Considering dependency mpm_prefork for php7.4:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php7.4:
Module php7.4 already enabled
ubuntu@ubuntu-VirtualBox:~$
```

2.3. Instalați pachetul "phpldapadmin" folosind comanda

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get install --reinstall phpldapadmin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  phpldapadmin
```

2.3.1 Puteți observa în directorul "/etc/phpldapadmin" fișierele de configurare instalate

```
ubuntu@ubuntu-VirtualBox:~$ ls -l /etc/phpldapadmin/
total 40
-rw-r--r-- 1 root root       992 Jan 21  2024 apache.conf
-rw-r--r-- 1 root www-data 28390 Nov 23 11:55 config.php
drwxr-xr-x 4 root www-data  4096 Nov 23 11:54 hooks
drwxr-xr-x 4 root www-data  4096 Nov 23 11:55 templates
```

2.3.2. Puteți observa activarea configurației modulului phpldapadmin în serverul apache:

```
ubuntu@ubuntu-VirtualBox:~$ ls -l /etc/apache2/conf-enabled/phpldapadmin.conf
lrwxrwxrwx 1 root root 35 Nov 23 11:55 /etc/apache2/conf-enabled/phpldapadmin.conf -> ../conf-available/phpldapadmin.conf
ubuntu@ubuntu-VirtualBox:~$ ls -l /etc/apache2/conf-available/phpldapadmin.conf
lrwxrwxrwx 1 root root 29 Nov 23 11:55 /etc/apache2/conf-available/phpldapadmin.conf -> /etc/phpldapadmin/apache.conf
ubuntu@ubuntu-VirtualBox:~$
```

2.4. Modificați în fișierul "/etc/phpldapadmin/config.php" liniile de mai jos cu conținutul indicat:

```
$servers->setValue('server','host','127.0.0.1');

/* 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=aso,dc=cs,dc=utcluj,dc=ro'));
```

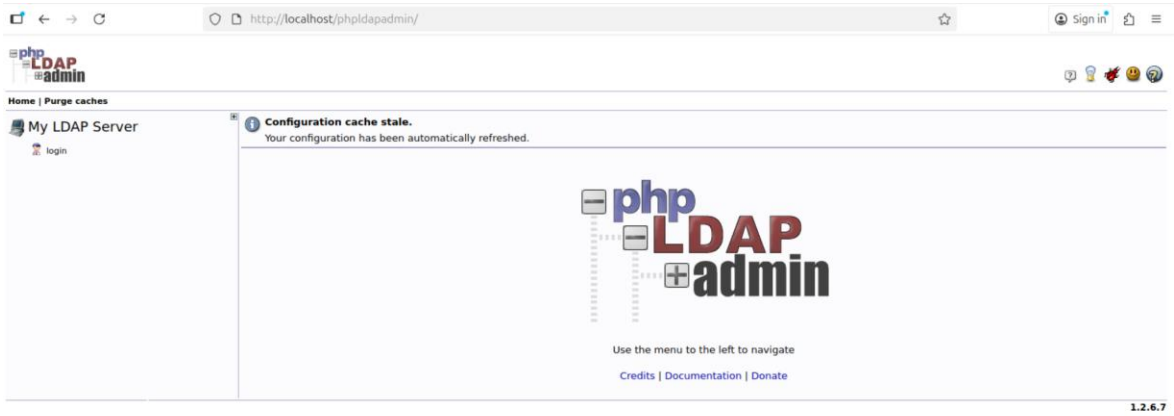
```
/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie','session' or 'sasl' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS
   BLANK. If you specify a login_attr in conjunction with a cookie or session
   auth_type, then you can also specify the bind_id/bind_pass here for searching
   the directory for users (ie, if your LDAP server does not allow anonymous
   binds. */
$servers->setValue('login','bind_id','cn=admin,dc=aso,dc=cs,dc=utcluj,dc=ro');
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

```
/* Hide the warnings for invalid objectClasses/attributes in templates. */
$config->custom->appearance['hide_template_warning'] = true;
```

```
ubuntu@ubuntu-VirtualBox:~$ sudo nano /etc/phpldapadmin/config.php
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl restart apache2
ubuntu@ubuntu-VirtualBox:~$
```

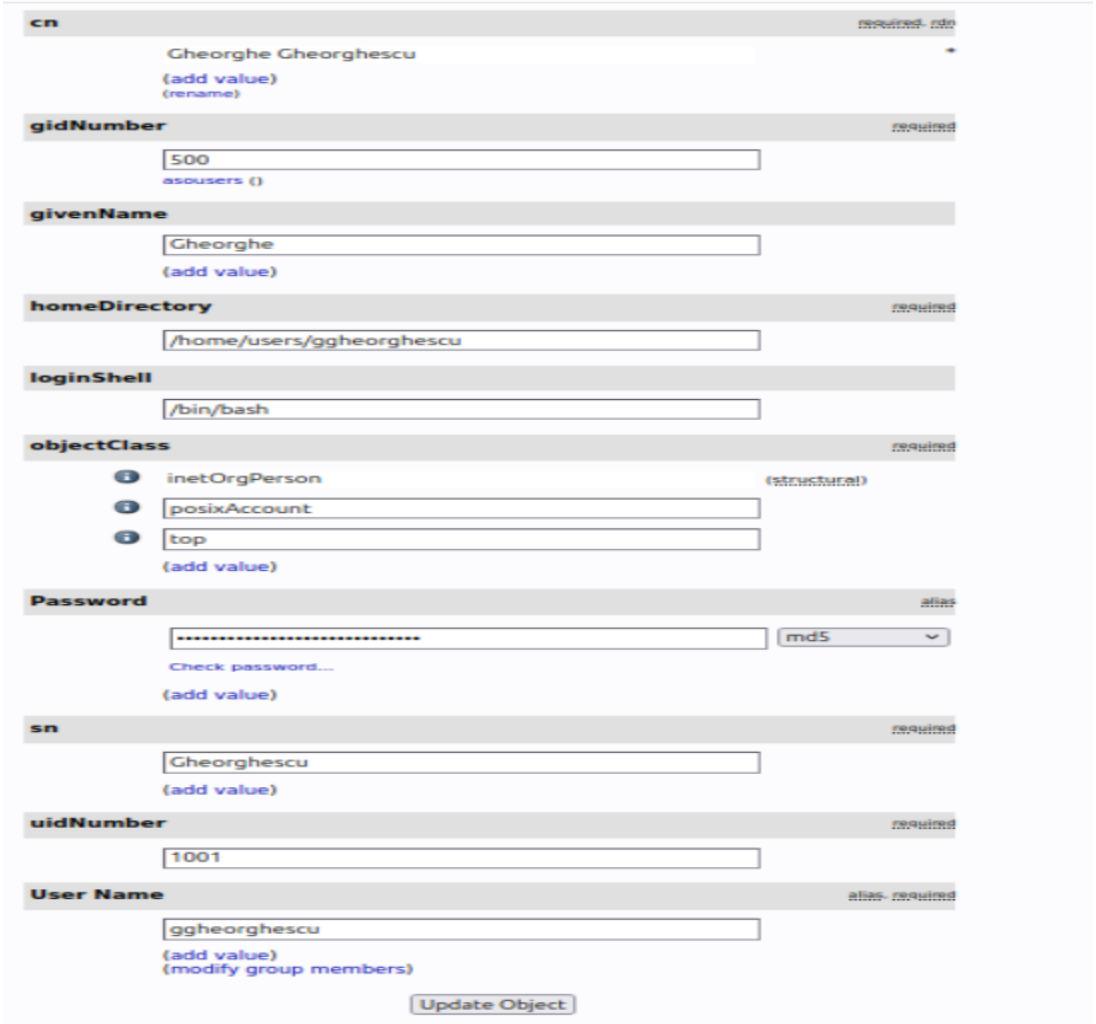
A trebuit sa modific si fisierul asta:
sudo nano /usr/share/phpldapadmin/lib/functions.php
la lini 361 sa schimb din:
[$int, $mod] = [intval($match[1]), $match[2]]; in
$int = intval($match[1]);
$mod = $match[2];
Pentru ca sintaxa nu era compatibila

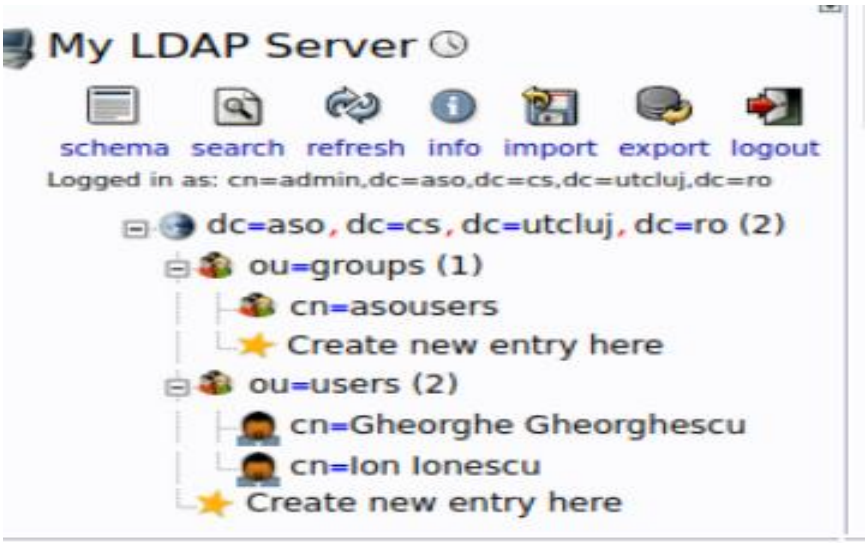
2.5. Folosind "Firefox Web Browser" accesati pagina




2.6. Conectațivă folosind utilizatorul "admin" și parola setată inițial.
m-am conectat cu: cn=admin,dc=aso,dc=cs,dc=utcluj,dc=ro si parola setata

3. Creați următoarele intrări (grupuri și utilizatori POSIX):
   I-am create din interfata web, ex:



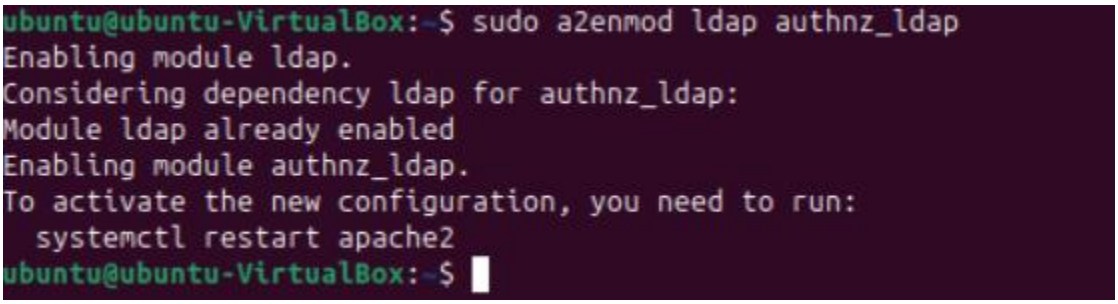
4. Folosiți comanda pentru a verifica configurația utilizatorilor existenți în baza de date LDAP.

```
ubuntu@ubuntu-VirtualBox:~/Desktop$ ldapsearch -x -b "dc=aso,dc=cs,dc=utcluj,dc=ro" -s sub "cn=*"
# extended LDIF
#
# LDAPv3
# base <dc=aso,dc=cs,dc=utcluj,dc=ro> with scope subtree
# filter: cn=*
# requesting: ALL
#

# Ion Ionescu, users, aso.cs.utcluj.ro
dn: cn=Ion Ionescu,ou=users,dc=aso,dc=cs,dc=utcluj,dc=ro
givenName: Ion
sn: Ionescu
uid: iionescu
uidNumber: 1000
gidNumber: 500
homeDirectory: /home/users/iionescu
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: Ion Ionescu

# Gheorghe Gheorghescu, users, aso.cs.utcluj.ro
dn: cn=Gheorghe Gheorghescu,ou=users,dc=aso,dc=cs,dc=utcluj,dc=ro
givenName: Gheorghe
sn: Gheorghescu
uid: ggheorghescu
uidNumber: 1001
gidNumber: 500
homeDirectory: /home/users/ggheorghescu
loginShell: /bin/bash
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: Gheorghe Gheorghescu

# asousers, groups, aso.cs.utcluj.ro
dn: cn=asousers,ou=groups,dc=aso,dc=cs,dc=utcluj,dc=ro
gidNumber: 500
objectClass: posixGroup
objectClass: top
cn: asousers

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
ubuntu@ubuntu-VirtualBox:~/Desktop$
```

5. Configurarea *apache2* pentru autentificarea prin Open LDAP
    5.1. Accesati https://localhost #observati ca nu se cere autentificare

    A trebuit sa accesez http://localhost, nu varianta https

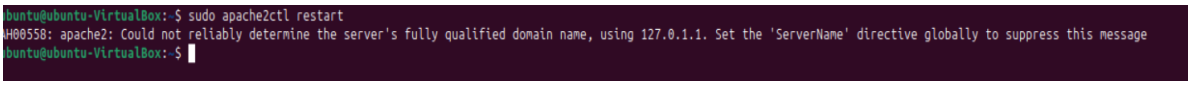
5.2. Din terminal activati modulul ldap folosind comanda



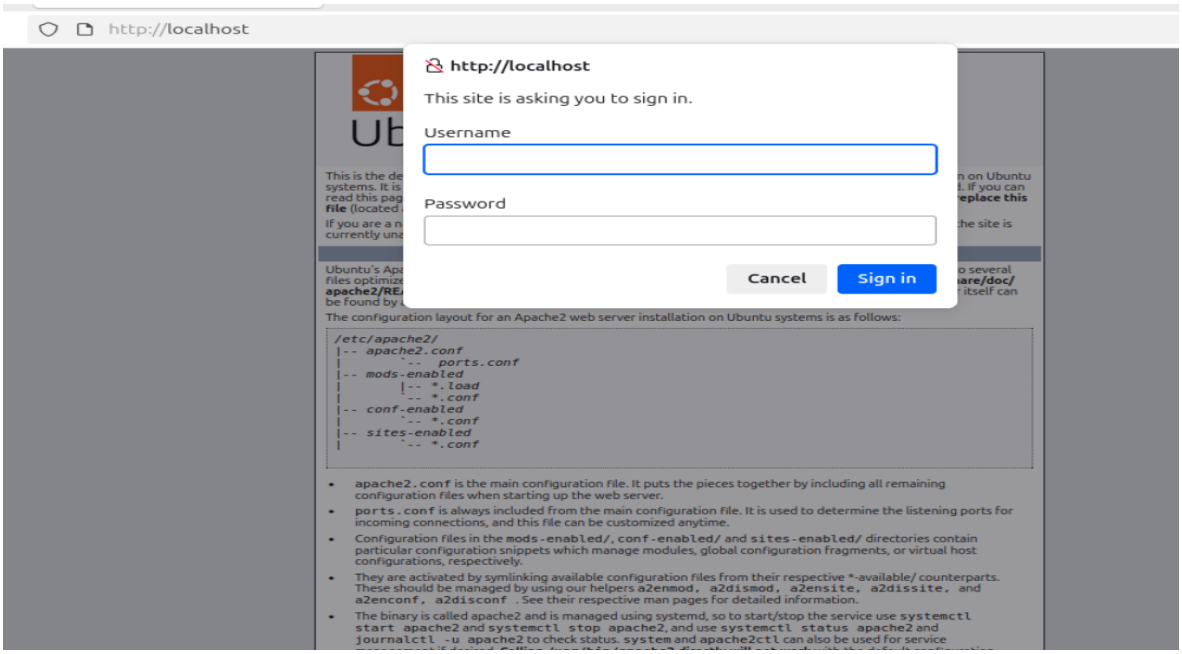

5.3. Creați fișierul "/etc/apache2/conf-enabled/auth_ldap.conf" cu conținutul de mai jos.

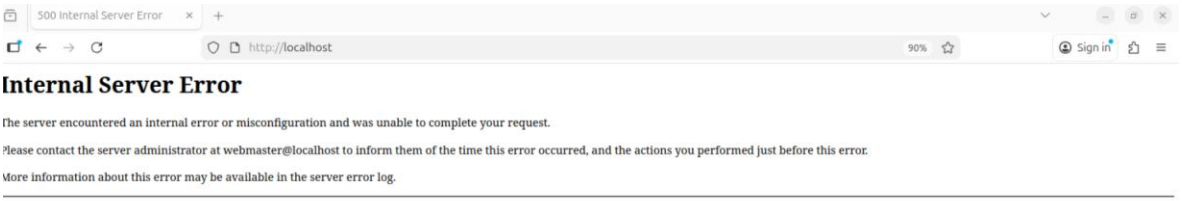
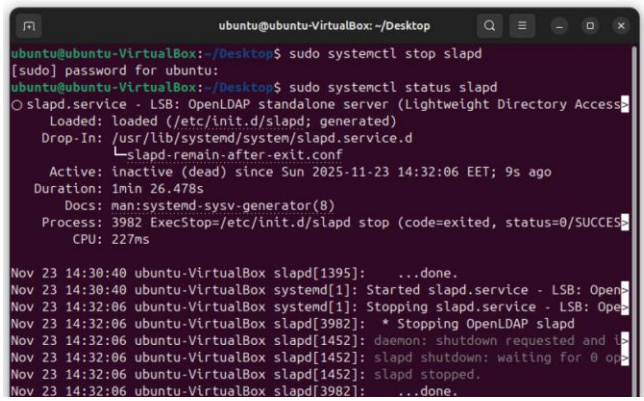
Metoda cu "/etc/apache2/conf-enabled/auth_ldap.conf e invechita, a trebuit sa fa ca in poza de mai sus si dupa:
Creare symlink: sudo a2enconf auth_ldap

5.4. Reporniti serverul de apache



5.5. Acesati iarasi https://localhost #observati ca se solicita autentificare.Folositi un user adaugat cu *phpLDAPadmin*




```
ubuntu@ubuntu-VirtualBox:~/Desktop$ curl -u iionescu:1234 http://localhost

    Caution: You are using the Snap version of curl.
    Due to Snap's sandbox nature, this version has some limitations.
    For example, it may not be able to access hidden folders in your home directory
    or other restricted areas of the os.

    Which means you may encounter errors when using snap curl to download and execute some script.
    For those cases, you might want to use the native curl package.
    For details, see: https://github.com/boukendesho/curl-snap/issues/1

    To stop seeing this message, run the following command:
    $ curl.snap-acked

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;
```

5.6. Opriți serviciu slapd, apoi încercați să vă autentificați pe apache.Mai functionează?