

LDAP dengan LAM (Praktikum)

Fitri Setyorini

Workshop Administrasi Jaringan

PSDKU Sumenep

Semester Genap

2023-2024

LDAP Software

- https://en.wikipedia.org/wiki/List_of_LDAP_software
- Anda dapat memilih LDAP software yang sesuai kebutuhan anda

LDAP Account Manager (LAM)

- LAM is a web application for managing various account types in an LDAP directory.
- It is written in PHP.
- LAM has two version : free and pro.
 - Pro needs commercial license
- Available at <https://www.ldap-account-manager.org/lamcms/releases>

Slapd

- Singkatan dari StandAlone LDAP Daemon (Server)
- Slapd berfungsi menunggu permintaan koneksi ke port server di nomor port 389
- Beberapa perintah slapd adalah : slapadd, slapcat, slapmodify, dst

Ldap-utils

- Adalah sekumpulan utility yang dipakai untuk melakukan query di ldap server
- Beberapa perintah ldap util adalah :
 - ldapsearch
 - ldapmodify
 - ldapadd
 - ldappasswd
 - dll

```
GNU nano 7.2 /etc/hosts *
127.0.1.1      debian12

10.252.44.139  fitri.edu
10.252.44.139  ns1.fitri.edu
10.252.44.139  www.fitri.edu
10.252.44.139  www.fitri2.edu
10.252.44.139  ldapmaster.fitri.edu
```

1. Setting DNSMasq

1. Pada PC yang diinstall ldap, cek IP addressnya

#ip addr

Misal no ip : 10.252.44.139

2. Pada PC yang diinstall dnsmasq, masukkan baris berikut di /etc/hosts

#nano /etc/hosts

Tambahkan nomor IP dan nama domain dari ldap

10.252.44.139 ldapmaster.fitri.edu

Simpan dan exit

3. Cek juga nomor IP dari server dns

#ip addr

Pada kasus ini, baik dns server dan ldap server berada pada PC yang sama, sehingga ip addressnya sama : 10.252.44.139 dengan nama domain dns : ns1.fitri.edu

3. Buka file /etc/resolv.conf dari PC dengan dns server.

Pastikan bahwa anda menambahkan nomor IP dari server dns di atas dns server utama anda

```
nameserver 10.252.44.139
```

```
nameserver <dns-server-sebelumnya>
```

Simpan dan exit

4. Test dns server dengan mengetikkan :

```
#nslookup ns1.fitri.edu
```

```
#nslookup ldapmaster.fitri.edu
```

```
root@debian12:~# nslookup ns1.fitri.edu
Server:      10.252.44.139
Address:     10.252.44.139#53

Name:   ns1.fitri.edu
Address: 10.252.44.139
```

```
GNU nano 7.2 /etc/resolv.conf
# Generated by NetworkManager
search pens.ac.id
nameserver 10.252.44.139
nameserver 202.9.85.4
nameserver 202.9.85.3
```

```
root@debian12:~# nslookup ldapmaster.fitri.edu
Server:      10.252.44.139
Address:     10.252.44.139#53

Name:   ldapmaster.fitri.edu
Address: 10.252.44.139
```

2. Install slapd & ldap-utils

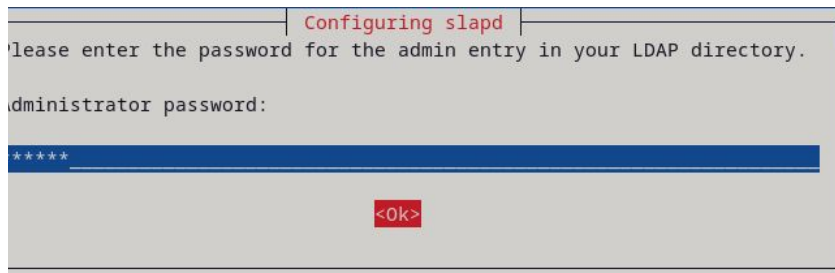
1. Update Linux

#apt update

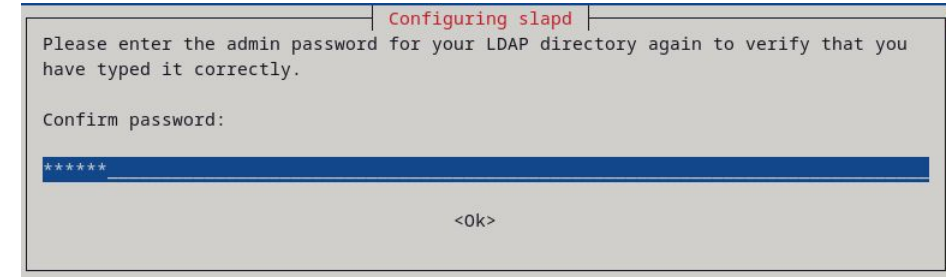
2. Install software berikut :

#apt install slapd ldap-utils

Masukkan password admin



Masukkan password yang sama



Slapd dan ldap-utils telah terinstall

```
Unpacking ldap-utils (2.5.13+dfsg-5) ...
Setting up slapd (2.5.13+dfsg-5) ...
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Setting up ldap-utils (2.5.13+dfsg-5) ...
Processing triggers for libc-bin (2.36-9+deb12u4) ...
Processing triggers for man-db (2.11.2-2) ...
```


3. Lakukan rekonfigurasi slapd

#dpkg-reconfigure slapd

Configuring slapd

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

Omit OpenLDAP server configuration?

<Yes> <No>

Configuring slapd

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

DNS domain name:

ldapmaster.fitri.edu

<Ok>

Configuring slapd

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

Organization name:

ldapmaster.fitri.edu

<Ok>

Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<Ok>

Configuring slapd

Please enter the admin password for your LDAP directory again to verify that you have typed it correctly.

Confirm 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>

```
root@debian12:~# dpkg-reconfigure slapd
\ Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.13+dfsg-5... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
```

3. Restart slapd dan cek statusnya

```
root@debian12:~# systemctl restart slapd
root@debian12:~# 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 Thu 2024-05-02 13:48:57 WIB; 7s ago
```

4. Slapcat

- Slapcat digunakan untuk melihat isi dari ldap server yang telah diinputkan ketika menginstall dan mengkonfigurasi slapd
- Beberapa informasi yang dapat dilihat adalah dn :distinguished name, o : organization, dc: domain component

```
root@debian12:~# slapcat
dn: dc=ldapmaster,dc=fitri,dc=edu
objectClass: top
objectClass: dcObject
objectClass: organization
o: ldapmaster.fitri.edu
dc: ldapmaster
structuralObjectClass: organization
entryUUID: 8fbcf80a-9ca3-103e-8bf6-93d187c54ccf
creatorsName: cn=admin,dc=ldapmaster,dc=fitri,dc=edu
createTimestamp: 20240502074433Z
entryCSN: 20240502074433.618806Z#000000#000#000000
modifiersName: cn=admin,dc=ldapmaster,dc=fitri,dc=edu
modifyTimestamp: 20240502074433Z
```

5. Menambahkan ou ke ldap server

- Buat file base.ldif

#nano base.ldif

- Tambahkan baris berikut :
- Simpan dan exit
- Pada base.ldif, dimasukkan ou:People dan ou:Groups pada dc:ldapmaster, dc=fitri, dc=edu
- Sesuaikan dc dengan nama domain anda
- Masukkan cn=admin ke file base.ldif lewat perintah ldapadd

#ldapadd -x -D cn=admin,dc=ldapmaster,dc=fitri,dc=edu -W -f base.ldif

base.ldif

dn: ou=People,dc=ldapmaster,dc=fitri,dc=edu

objectClass: organizationalUnit

ou: people

dn: ou=Groups,dc=ldapmaster,dc=fitri,dc=edu

objectClass: organizationalUnit

ou: groups

File base.ldif dan Perintah ldapadd

```
GNU nano 7.2 base.ldif
# base.ldif

dn: ou=People,dc=ldapmaster,dc=fitri,dc=edu
objectClass: organizationalUnit
ou: people

dn: ou=Groups,dc=ldapmaster,dc=fitri,dc=edu
objectClass: organizationalUnit
ou: groups
```

```
root@debian12:~# nano base.ldif
root@debian12:~# ldapadd -x -D cn=admin,dc=ldapmaster,dc=fitri,dc=edu -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=ldapmaster,dc=fitri,dc=edu"

adding new entry "ou=Groups,dc=ldapmaster,dc=fitri,dc=edu"
```

6. Mengecek ou lewat ldapsearch

- Lakukan query dengan ldapsearch untuk

dc=ldapmaster,dc=fitri,dc=edu

#ldapsearch -x -b

"ou=People,dc=ldapmaster,dc=fitri,dc=edu"

```
root@debian12:~# ldapsearch -x -b "dc=ldapmaster,dc=fitri,dc=edu" ou
# extended LDIF
#
# LDAPv3
# base <dc=ldapmaster,dc=fitri,dc=edu> with scope subtree
# filter: (objectclass=*)
# requesting: ou
#
# ldapmaster.fitri.edu
dn: dc=ldapmaster,dc=fitri,dc=edu

# People, ldapmaster.fitri.edu
dn: ou=People,dc=ldapmaster,dc=fitri,dc=edu
ou: people

# Groups, ldapmaster.fitri.edu
dn: ou=Groups,dc=ldapmaster,dc=fitri,dc=edu
ou: groups

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
```

7. Menambahkan user ke ldap server

- Untuk menambahkan user baru ke ldap server, anda harus mengeset password terenkripsi

#slappasswd

Masukkan password untuk slapd

- Buat file untuk user

#nano user.ldif

- Ketikkan baris berikut
- Save dan exit

user.ldif

```
dn: uid=debian,ou=People,dc=ldapmaster,dc=fitri,dc=edu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: debian
sn: bookworm
userPassword:
{SSHA}23rFF1ofbNo5MRxEJo6D2Z4PT2GOxeWt
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/debian
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
```

```
dn: cn=debian,ou=Groups,dc=ldapmaster,dc=fitri,dc=edu
objectClass: posixGroup
cn: debian
gidNumber: 2000
memberUid: debian
```


- Pada file user.ldif, anda menambahkan 2 dn, yaitu
- dn: uid=debian,ou=People
 - cn: debian,
 - sn: bookworm,
 - dst
- dn: cn=debian,ou=Groups
 - cn: debian
 - gidNumber: 2000
 - memberUid: debian

- Sekarang, tambahkan file user.ldif dengan cn=admin ke dc=ldapmaster,dc=fitri,dc=edu

```
#ldapadd -x -D  
cn=admin,dc=ldapmaster,dc=fitri,  
dc=edu -W -f user.ldif
```

```
root@debian12:~# ldapadd -x -D cn=admin,dc=ldapmaster,dc=fitri,dc=edu -W -f user.ldif  
Enter LDAP Password:  
adding new entry "uid=debian,ou=People,dc=ldapmaster,dc=fitri,dc=edu"  
  
adding new entry "cn=debian,ou=Groups,dc=ldapmaster,dc=fitri,dc=edu"
```

8. Mengecek user lewat ldapsearch

- Cek user yang telah dimasukkan lewat ldapsearch

```
#ldapsearch -x -b
```

```
"ou=People,dc=ldapmaster,dc=fitri,dc=edu"
```

```
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=ldapmaster,dc=fitri,dc=edu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# People, ldapmaster.fitri.edu
dn: ou=People,dc=ldapmaster,dc=fitri,dc=edu
objectClass: organizationalUnit
ou: people

# debian, People, ldapmaster.fitri.edu
dn: uid=debian,ou=People,dc=ldapmaster,dc=fitri,dc=edu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: debian
sn: bookworm
loginShell: /bin/bash
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
uid: debian

# search result
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2
```

9. Install Idap account manager (LAM)

- Install Idap account manager
#apt install ldap-account-manager
- Cek versi php
#php -v
Versi php yang dipakai adalah 8.2
- Backup dulu file berikut
#cp /etc/php/8.2/apache2/php.ini
/etc/php/8.2/apache2/php.ini.orig
- Edit file php.ini
#nano /etc/php/8.2/apache2/php.ini
Cari memory_limit, ubah menjadi 256M
- Save dan Exit

```
root@debian12:~# php -v
PHP 8.2.18 (cli) (built: Apr 11 2024 22:07:45) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.2.18, Copyright (c) Zend Technologies
    with Zend OPcache v8.2.18, Copyright (c), by Zend Technologies
root@debian12:~#
```

```
GNU nano 7.2 /etc/php/8.2/apache2/php.ini *
;max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
;max_input_vars = 1000

; How many multipart body parts (combined input variable and file uploads) may
; be accepted.
; Default Value: -1 (Sum of max_input_vars and max_file_uploads)
;max_multipart_body_parts = 1500

; Maximum amount of memory a script may consume
; https://php.net/memory-limit
memory_limit = 256M
_
```

10. Konfigurasi virtual hosting untuk LAM

- Buka file konfigurasi Apache2 untuk ldap-account-manager
/etc/apache2/conf-enabled/ldap-account-manager.conf
- Sebelumnya backup terlebih dahulu file tersebut
#cp /etc/apache2/conf-enabled/ldap-account-manager.conf
/etc/apache2/conf-enabled/ldap-account-manager.conf.orig
- Buka dengan nano
#nano /etc/apache2/conf-enabled/ldap-account-manager.conf
- Edit bagian berikut
#Require all granted
Require ip 127.0.0.1 192.168.10.0/24
- Save dan exit

```
GNU nano 7.2 /etc/apache2/conf-enabled/ldap-account-manager.conf *

Alias /lam /usr/share/ldap-account-manager

# HSTS header to enforce https:// connections (requires active mod_headers)
# Header always set Strict-Transport-Security "max-age=31536000"

<Directory /usr/share/ldap-account-manager>
  Options +FollowSymLinks
  AllowOverride None
  #Require all granted
  Require ip 127.0.0.1 10.252.44.0/24
  DirectoryIndex index.html
</Directory>
```

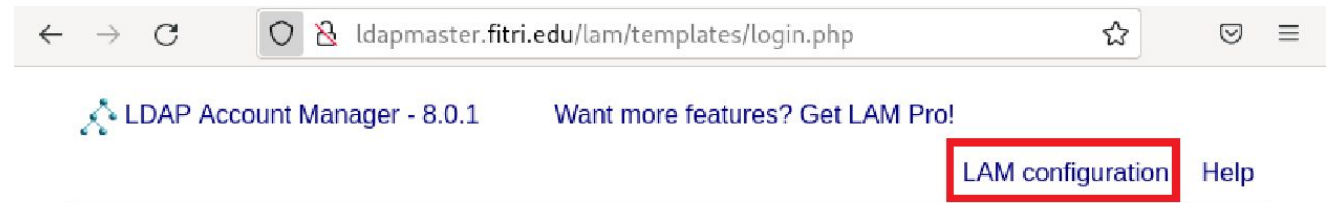
11. Merestart apache & cek statusnya

- Restart apache2 dan cek statusnya

```
root@debian12:~# systemctl restart apache2
root@debian12:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-05-02 15:01:39 WIB; 6s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 127151 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 127156 (apache2)
    Tasks: 6 (limit: 2244)
```

12. Setting Konfigurasi LAM

1. Buka browser dan ketikkan <http://ldapmaster.fitri.edu/lam>
2. Anda tidak perlu login
3. Klik LAM configuration



User name

Manager

▼

Password

Language

English (Great Britain)

▼

Login

LDAP server

ldap://localhost:389

4. Klik Edit server profiles

5. Masukkan password default
yaitu lam

profile name : lam

password : lam

Klik OK

 Edit general settings

 Edit server profiles

 Import and export configuration

Please enter your password to change the server preferences:

Profile name lam

Password

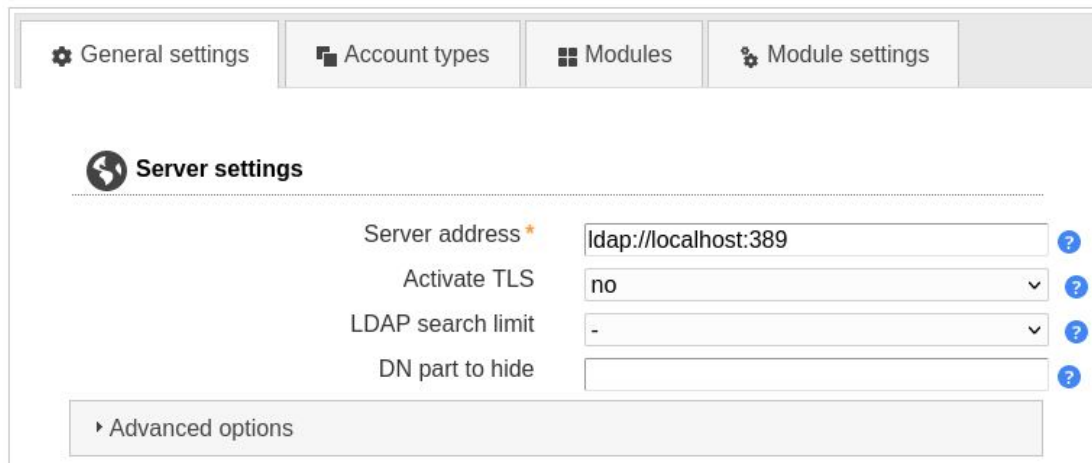
...

Ok

Manage server profiles


Konfigurasi Server profile


- Pada Tab General Setting, carilah Tool settings, Security settings dan Profile password
- Pada Profile password, masukkan password baru sesuai keinginan anda
- Jangan lupa di Save





General settings | Account types | Modules | Module settings

Server settings

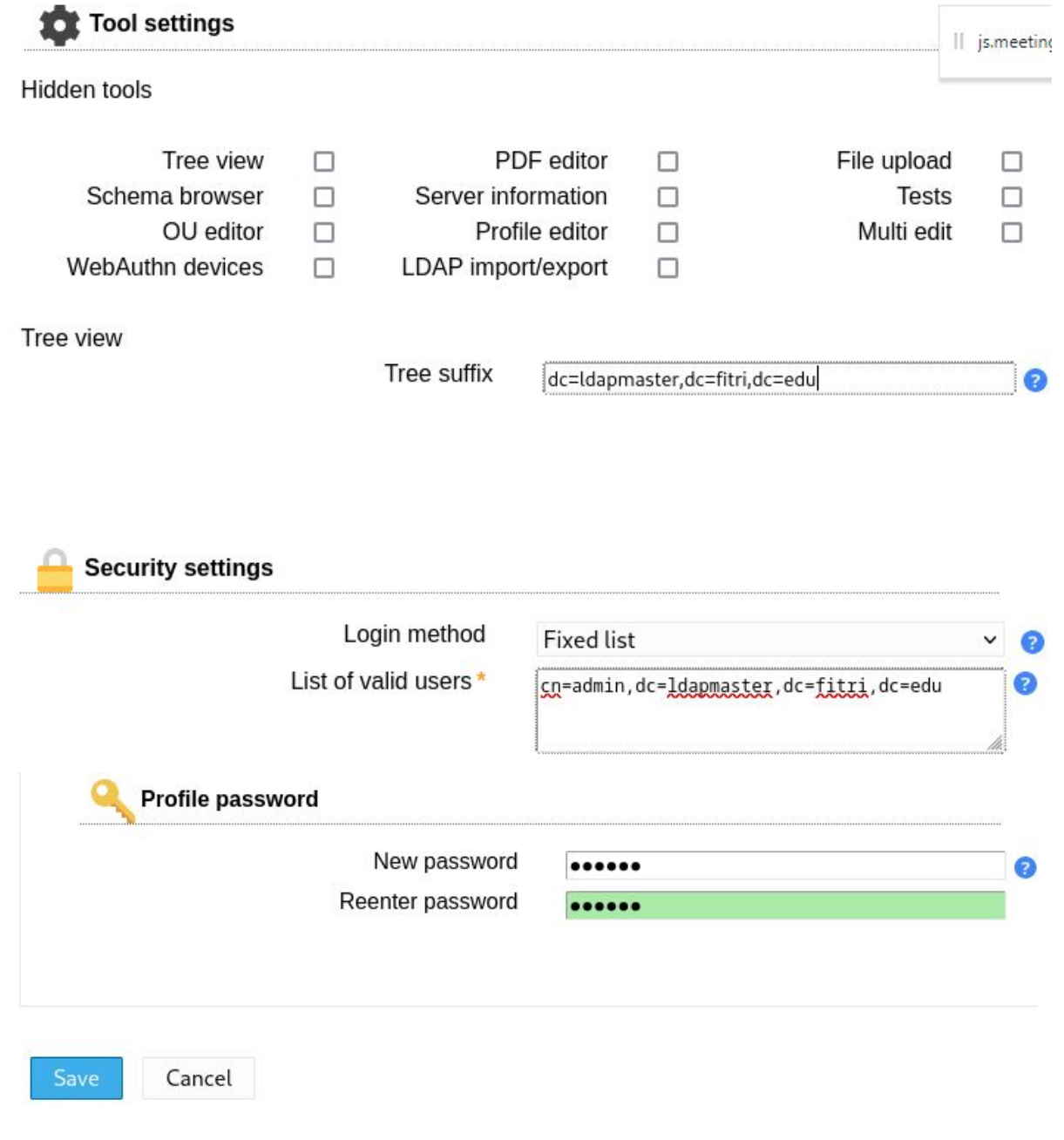
Server address  ldap://localhost:389


Activate TLS  no

LDAP search limit  -

DN part to hide 

Advanced options




Tool settings  js.meeting


Hidden tools


Tree view	<input type="checkbox"/>	PDF editor	<input type="checkbox"/>	File upload	<input type="checkbox"/>
Schema browser	<input type="checkbox"/>	Server information	<input type="checkbox"/>	Tests	<input type="checkbox"/>
OU editor	<input type="checkbox"/>	Profile editor	<input type="checkbox"/>	Multi edit	<input type="checkbox"/>
WebAuthn devices	<input type="checkbox"/>	LDAP import/export	<input type="checkbox"/>		

Tree view


Tree suffix 

Security settings

Login method 

List of valid users 

Profile password

New password 

Reenter password

Save Cancel

General settings **Account types** Modules Module settings

Active account types

Users

User accounts (e.g. Unix, Samba and Kolab)



LDAP suffix * ?

List attributes ?

Custom label ?

Additional LDAP filter ?

Hidden ☐ ?

Groups

Group accounts (e.g. Unix and Samba)



LDAP suffix * ?

List attributes ?

Custom label ?

Additional LDAP filter ?

Hidden ☐ ?

Save

Cancel

- Klik LAM Configuration
- Login dan masukkan password yang baru kita buat
 - profile name : lam
 - password : [password-baru]
- Buka tab Account Types
- Pada Active account types
- Pada kolom Users, masukkan LDAP Suffix
- Pada kolom Groups, masukkan LDAP Suffix
- Klik Save yang ada dibawah

- Ketika anda menekan save, secara otomatis konfigurasi akan disimpan dan anda akan dibawa ke login page
- Sekarang masuklah kembali dengan username: admin, dengan menggunakan password yang tadi anda set
- Sekarang klik Account, lalu Users
- Nampak user debian yang kita buat lewat file user.ldif

User name

admin

Password

•••••

Language

English (Great Britain)


Login

LDAP server

ldap://localhost:389

Server profile

lam



 admin
 [Accounts](#)
[Tools](#)
[Help](#)
[Logout](#)

Users





New user

File upload

Delete selected users

User count: 4

Actions	User name	First name	Last name	UID number	GID number
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>    	debian		bookworm	2000	2000

- Sekarang klik Account, lalu Groups
- Nampak group debian yang kita buat lewat file user.ldif

Groups





New group

File upload



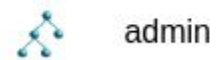
Delete selected groups

Group count: 4

Actions	Name	GID number	Group members	Group description
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>    	debian	2000	debian	

Konfigurasi user dan group

- Klik Accounts
- Pilih Users
- Klik New User



[Accounts](#) [Tools](#) [Help](#) [Logout](#)

Users

[New user](#)

[File upload](#)



User count: 0

Actions	User name	First name	Last name	UID number	GID number
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Membuat Group

- Klik Accounts
- Pilih Groups
- Klik New Group
- Buat 3 grup: dosen, siswa dan administrasi
- Isikan Group name dan GID number
Group nama : dosen
GID number : 10000
- GID dimulai dari 10000
- Klik Save

The screenshot displays the 'Groups' management page in an LDAP interface. At the top, there's a navigation bar with 'admin' and links for 'Accounts', 'Tools', 'Help', and 'Logout'. Below this, the 'Groups' section has a 'New group' button (highlighted with a red box) and a 'File upload' button. A 'Group count: 0' indicator is present. A table lists existing groups with columns for 'Actions', 'Group name', 'GID number', 'Group members', and 'Group description'. Below the table, the 'New group' form is shown. It includes a 'Suffix' field with the value 'group > fitri > edu' and an 'RDN identifier' field with the value 'cn'. The 'Group name' field is filled with 'dosen' and the 'GID number' field is filled with '10000', both highlighted with red boxes. There is also a 'Description' field and an 'Edit members' button. At the bottom, a blue message box states 'LDAP operation successful. Account was created successfully.' Below this, there are four buttons: 'Back to group list', 'Create another group', 'Create PDF file', and 'Edit again'. On the right side, there's a 'default profile' dropdown menu.

admin Accounts Tools Help Logout

Groups

New group File upload

Group count: 0

Actions	Group name	GID number	Group members	Group description
Sort sequence				
<input type="checkbox"/> Filter ▾				

New group

Suffix group > fitri > edu
RDN identifier cn ?

Unix

Group name * dosen ?

GID number 10000 ?

Description ?

Group members Edit members ?

admin Accounts Tools Help Logout

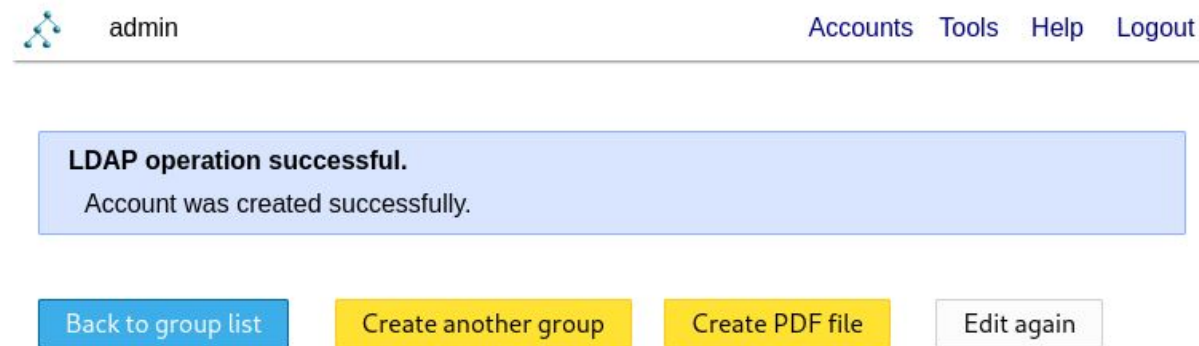
elp Logout

default profile ?

LDAP operation successful.
Account was created successfully.

Back to group list Create another group Create PDF file Edit again

- Akan muncul pesan bahwa pembuatan grup sukses



- Klik Create another group untuk membuat grup baru
- Buat 2 grup lagi yaitu siswa dan administrasi

Group name ^{*} ?

GID number ?

Description ?

Group members ?


Group name ^{*} ?

GID number ?

Description ?

Group members ?

- Klik Save
- Jika sudah terbentuk 3 grup baru, maka klik Back to group list

 admin [Accounts](#) [Tools](#) [Help](#) [Logout](#)

LDAP operation successful.
Account was created successfully.

- Untuk melihat list grup yang dibuat

Groups













New group

File upload



Delete selected groups

Group count: 3

Actions	Group name	GID number	Group members	Group description
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>    	administrasi	10002		
<input type="checkbox"/>    	dosen	10000		
<input type="checkbox"/>    	siswa	10001		

Membuat User

- Klik Accounts
- Pilih Users
- Pada tab Personal, pastikan informasi seperti diatas
- Pada tab Unix, masukkan username dan primary group
- Untuk user siska, masukkan ke grup siswa
- Klik Save

The screenshot shows the 'New user' form with the 'Personal' tab selected. The 'Suffix' is set to 'People > fitri > edu' and the 'RDN identifier' is 'cn'. The 'First name' is 'Siska' and the 'Last name' is 'Indira'. The 'Initials' and 'Description' fields are empty. The 'Personal' tab is highlighted with a red box.

The screenshot shows the 'New user' form with the 'Unix' tab selected. The 'Personal' tab is also visible. The 'Unix' tab is highlighted with a red box.

The screenshot shows the 'New user' form with the 'Unix' tab selected. The 'User name' is 'siska' and the 'Common name' is 'Siska Indira'. The 'UID number' and 'Gecos' fields are empty. The 'Primary group' is 'siswa'. The 'Create group with same name' button is visible. The 'Additional groups' section has an 'Edit groups' button. The 'Home directory' is '/home/\$user' and the 'Login shell' is '/bin/bash'. The 'User name' and 'Primary group' fields are highlighted with red boxes.

admin

[Accounts](#) [Tools](#) [Help](#) [Logout](#)

Save

Set password

Delete

Reset changes

default

Load profile

Back to user list

Membuat User

- Ada 3 tab, Personal, Unix dan Shadow
- Isi tab Personal seperti disamping
 - Isi First Name dan Last Name
- Klik tab Unix di sebelah kiri
 - Isi User name, UID number dan Primary Group

The screenshot shows the 'New user' form. On the left, there are three tabs: 'Personal' (selected), 'Unix', and 'Shadow'. The 'Personal' tab contains fields for 'First name' (Siska), 'Last name' (Indira), 'Initials', and 'Description'. The breadcrumb navigation at the top reads 'People > fitri > edu'. The 'Suffix' and 'RDN identifier' are both set to 'cn'.

The screenshot shows the user profile for 'Siska Indira'. The 'Unix' tab is selected and highlighted with a red box. The 'Personal' tab is also visible. The 'Unix' tab contains fields for 'User name' (siska), 'Common name' (Siska Indira), 'UID number' (10000), 'Gecos', 'Primary group' (mahasiswa), 'Additional groups', 'Home directory' (/home/\$user), and 'Login shell' (/bin/bash). The 'User name', 'UID number', and 'Primary group' fields are highlighted with red boxes. The breadcrumb navigation at the top reads 'People > Idapmaster > fitri > edu'. The 'Suffix' and 'RDN identifier' are both set to 'cn'.

- Jika sudah lakukan setting password

- Masukkan password untuk user
- Klik OK
- Klik Save

admin

Save Set password Back to user list

Set password

Password ?

Repeat password ?

Force password change ☐ ?

☒ Unix

Ok Set random password Cancel

Accounts Tools Help Logout

default

Save Set password Back to user list

- Setelah tersimpan, maka anda ditawarkan untuk membuat user baru lagi atau kembali ke listing user
- Klik Create another user jika anda membuat user baru
- Buatlah 2 user baru untuk group administrasi dan dosen
- Untuk melihat user yang telah diciptakan, anda bisa mengklik Back to user list

admin Accounts Tools Help Logout

LDAP operation successful.
Account was created successfully.

Back to user list Create another user Create PDF file Edit again

Users

New user File upload

Delete selected users

User count: 3

Actions	User name	First name	Last name	UID number	GID number
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	arhan	Arhan	Pratama	10002	10002
<input type="checkbox"/>	sinta	Sinta	Saskia	10001	10000
<input type="checkbox"/>	siska	Siska	Indira	10000	10001

Instalasi ldap-client

- Buka PC baru / VM baru.

PC baru atau VM baru ini akan kita jadikan ldap-client

- Install software berikut untuk ldap-client

```
#apt install libnss-ldapd libpam-ldapd ldap-utils
```

- Setelah instalasi, anda akan diminta mengkonfigurasi libnss-ldap
- Ikuti langkah berikut

Configuring nslcd

Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://<hostname_or_IP_address>:<port>". Alternatively, "ldaps://" or "ldapi://" can be used.

When using an ldap or ldapi URI, you must specify the LDAP server URI to avoid failures when doing lookups.

Multiple URIs can be specified by separating them with spaces.

LDAP server URI:

ldap:///ldapmaster.fitri.edu

<Ok>

Configuring libnss-ldapd

For this package to work, you need to modify the /etc/nsswitch.conf file to use the ldap datasources.

Make sure that the LDAP lookups are enabled. The new LDAP configuration file is located in /etc/nsswitch.conf. Please review these changes.

PAM configuration

One or more of the files /etc/pam.d/common-{auth,account,password,session} have been locally modified. Please indicate whether these local changes should be overridden using the system-provided configuration. If you decline this option, you will need to manage your system's authentication configuration by hand.

Override local changes to /etc/pam.d/common-*?

<Yes>

<No>

Please enter the distinguished name of the LDAP search base. For example, if the components of their domain name are "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

LDAP server search base:

dc=ldapmaster,dc=fitri,dc=edu

<Ok>

<Cancel>

Konfigurasi libnss-ldap

Configuring libnss-ldap

Please enter the Uniform Resource Identifier of the LDAP server. The format is 'ldap://<hostname_or_IP>:<port>/'. Alternatively, 'ldaps://' or 'ldapi://' can be used. The port number is optional.

Using an IP address is recommended to avoid failures when domain name services are unavailable.

LDAP server URI:

1

ldap://192.168.220.128

<Ok>

Configuring libnss-ldap

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example,

Configuring nslcd

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as search base.

LDAP server search base:

dc=ldapmaster,dc=fitri,dc=edu

<Ok>

Configuring libnss-ldap

Please choose the version of the LDAP protocol that should be used by ldaps. Using the highest available version number is recommended.

LDAP version to use:

3

2

<Ok>

Configuring libnss-ldap

Please choose which account will be used for nss requests with root privileges.

Note: For this to work the account needs permission to access the attributes in the LDAP directory that are related to the users' shadow entries as well as users' and groups' passwords.

Account for root:

dc=fitri,dc=edu

4

Configuring nslcd

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

LDAP server search base:

dc=ldapmaster,dc=fitri,dc=edu

1

Configuring libnss-ldap

Please enter the password to use when libnss-ldap tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/libnss-ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

<Ok>

2

Configuring libnss-ldap

nsswitch.conf not managed automatically

For the libnss-ldap package to work, you need to modify your /etc/nsswitch.conf to use the "ldap" datasource. There is an example file at /usr/share/doc/libnss-ldap/examples/nsswitch.ldap which can be used as an example for your nsswitch setup, or it can be copied over your current setup.

Also, before removing this package, it is wise to remove the "ldap" entries from nsswitch.conf to keep basic services functioning.

<Ok>

6

Konfigurasi libpam-ldap

- Sekarang lakukan konfigurasi libpam-ldap

Configuring libpam-ldap

This option will allow password utilities that use PAM to change local passwords.

The LDAP admin account password will be stored in a separate file which will be made readable to root only.

If /etc is mounted by NFS, this option should be disabled.

Allow LDAP admin account to behave like local root?

☒ <Yes> ☐ <No> 1

Configuring libpam-ldap

Please choose whether the LDAP server enforces a login before retrieving entries.

Such a setup is not usually needed.

Does the LDAP database require login? 2

☐ <Yes> ☒ <No>

Configuring libpam-ldap

Please enter the name of the LDAP administrative account.

This account will be used automatically for database management, so it must have the appropriate administrative privileges.

LDAP administrative account:

3

cn=admin,dc=fitri,dc=edu

<Ok>

Configuring libpam-ldap

Please enter the password of the administrative account.

The password will be stored in the file /etc/pam_ldap.secret. This will be made readable to root only, and will allow libpam-ldap to carry out automatic database management logins.

If this field is left empty, the previously stored password will be re-used.

LDAP administrative password:

4

<Ok>

#apt install libpam-ldap

Configuring nslcd

Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://<hostname_or_IP_address>:<port>". Alternatively, "ldaps://" or "ldapi://" can be used. The port number is optional.

When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name services are unavailable.

Multiple URIs can be separated by spaces.

LDAP server URI:

ldapi:///

<Ok>

Configuring libnss-ldapd

For this package to work, you need to modify the /etc/nsswitch.conf file to use the ldap datasource.

You can select the services that should have LDAP lookups enabled. The new LDAP lookups will be added as the last datasource. Be sure to review these changes.

Name services to configure:

- ☒ [*] passwd
- ☒ [*] group
- ☒ [*] shadow
- ☐ [] hosts
- ☐ [] networks
- ☐ [] ethers

PAM configuration

Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are handled on the system, as well as allowing configuration of additional actions to take when starting user sessions.

Some PAM module packages provide profiles that can be used to automatically adjust the behavior of all PAM-using applications on the system. Please indicate which of these behaviors you wish to enable.

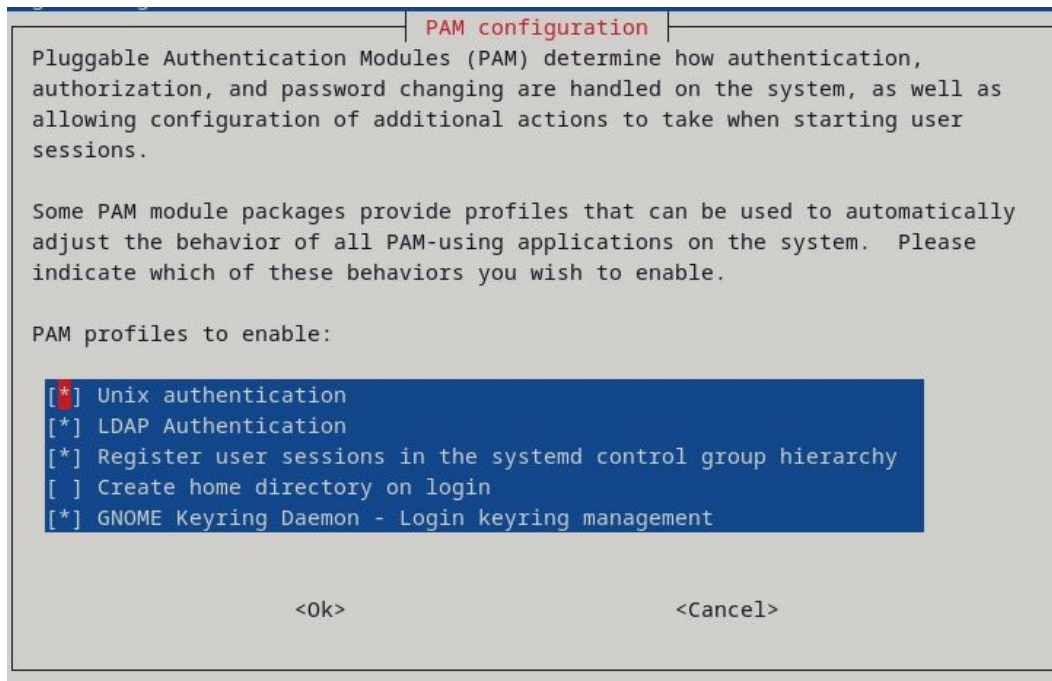
PAM profiles to enable:

- ☒ Unix authentication
- ☒ LDAP Authentication
- ☒ Register user sessions in the systemd control group hierarchy
- ☐ Create home directory on login
- ☒ GNOME Keyring Daemon - Login keyring management

<Ok>

<Cancel>

#pam-auth-update



Konfigurasi Name Service Switch (nsswitch)

- Nsswitch bertugas mengkoneksikan PC dengan berbagai konfigurasi database dan resolusi domain
- Nsswitch biasanya digunakan oleh file /etc/passwd, /etc/group, /etc/hosts, Domain Name System (DNS), Network Information Service (NIS, NIS+), dan LDAP.
- Sekarang, backup dulu nsswitch.conf

#cp /etc/nsswitch.conf /etc/nsswitch.conf.orig

- Lakukan file konfigurasi nsswitch.conf

#nano /etc/nsswitch.conf

Hapus atau beri tanda # pada passwd,
group dan shadow

Masukkan

passwd: compat ldap

group: compat ldap

shadow: compat ldap

```
GNU nano 5.4 /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
# `info libc "Name Service Switch"' for information about this file.

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

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

protocols:  db files
services:   db files
ethers:     db files
```

Konfigurasi File common-password

- Sekarang, backup dulu common-password

```
#cp /etc/pam.d/common-password /etc/pam.d/common-password.orig
```

Lakukan konfigurasi pada file common-password. Anda dapat menggunakan nano

```
#nano +26 /etc/pam.d/common-password
```

nano akan bergerak ke baris 26

- Hapus use_authtok di baris 26,

```
password [success=1 user_unknown=ignore default=die] pam_ldap.so use_authtok try_first_pass
```

- Edit seperti baris dibawah :

```
password [success=1 user_unknown=ignore default=die] pam_ldap.so try_first_pass
```

- Simpan dan exit

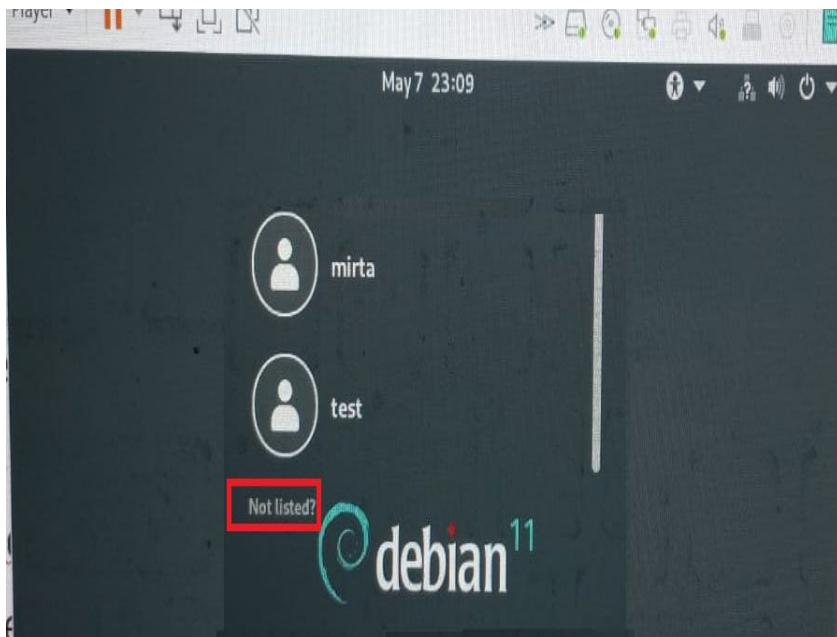
Konfigurasi File common-session

- Sekarang, backup dulu common-session
`#cp /etc/pam.d/common-session /etc/pam.d/common-session.orig`
- Lakukan konfigurasi pada file common-password. Anda dapat menggunakan nano
`#nano /etc/pam.d/ common-session`
- Carilah baris terakhir sebelum `#end of pam-auth-update config`
- Tambahkan

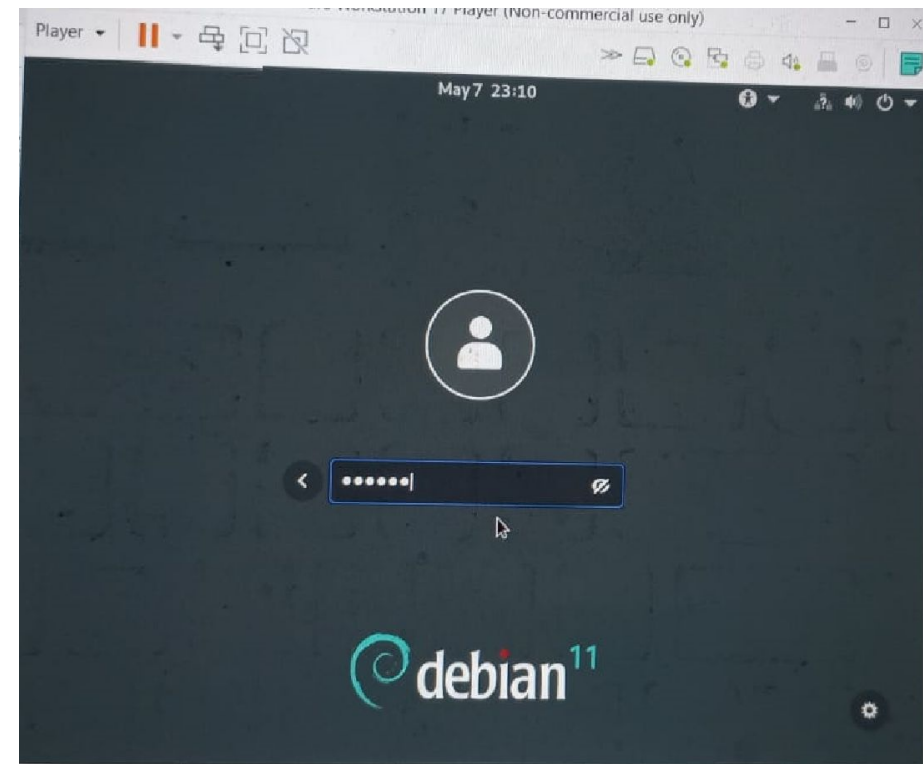
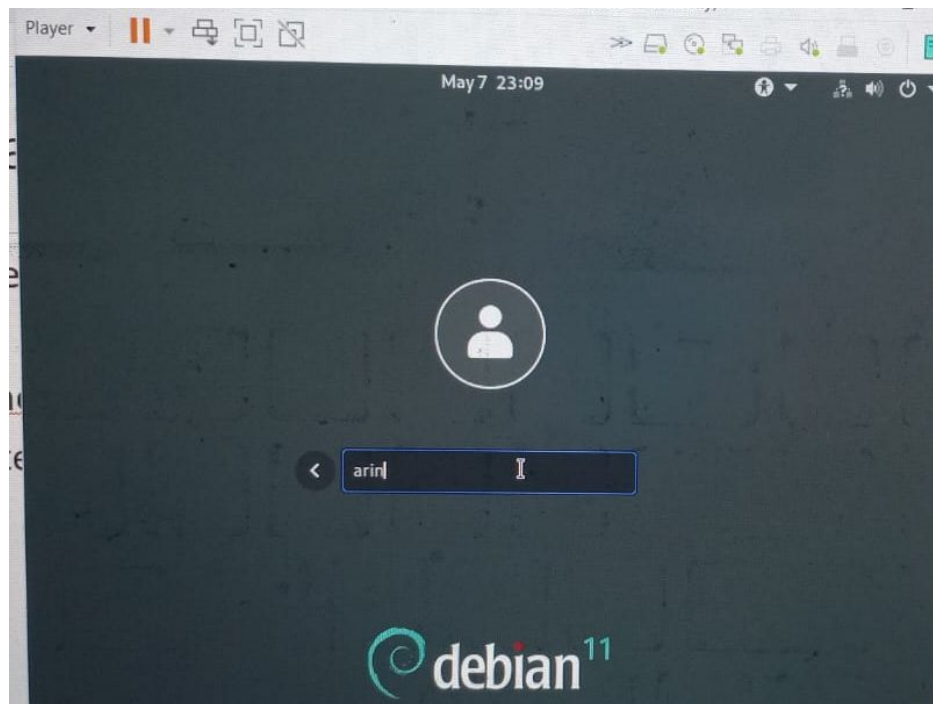
```
session optional pam_mkhomedir.so skel=/etc/skel umask=077  
# end of pam-auth-update config
```

- Simpan dan exit

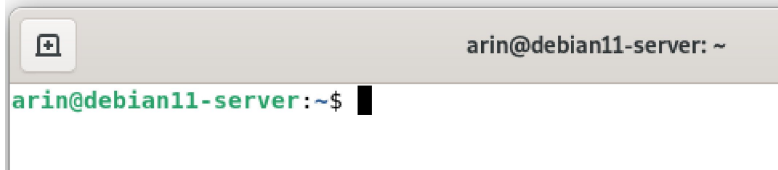
- Sekarang reboot PC-ldap client anda
#reboot
- Ketika muncul ke screen awal Debian, klik Not listed ?



- Masukkan salah satu user
- Disini dimasukkan arin
- Masukkan password untuk arin



- Ketika berhasil login, maka LDAP client akan membuat directory /home/arin di server
- Buka terminal. Ternyata anda sudah diarahkan ke home directory arin



```
arin@debian11-server: ~  
arin@debian11-server:~$
```

Ketikkan :

\$pwd



```
arin@debian11-server: ~  
arin@debian11-server:~$ pwd  
/home/arin  
arin@debian11-server:~$
```

Maka akan nampak, anda berada di /home/arin yang berada di server

- Sekarang, ketikkan id dan whoami. Perhatikan hasilnya :

```
arin@debian11-server: ~  
arin@debian11-server:~$ id  
uid=10002(arin) gid=10002(administrasi) groups=10002(administrasi)  
arin@debian11-server:~$ whoami  
arin
```

- Coba login sebagai root, install finger

```
$su - root
```

```
#apt install finger
```

- Sekarang balik lagi sebagai arin

```
#su - arin
```

```
$finger arin
```

```
arin@debian11-server:~$ su - root  
Password:  
root@debian11-server:~# apt install finger  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

```
root@debian11-server:~# su - arin  
arin@debian11-server:~$ finger arin  
Login: arin                                Name: Arin Himura  
Directory: /home/arin                      Shell: /bin/bash  
On since Sun May  7 23:34 (WIB) on tty3 from tty3  
    1 hour 42 minutes idle  
No mail.  
No Plan.  
arin@debian11-server:~$
```

- Anda dapat melihat baik perintah id, whoami dan finger memberikan informasi yang sama seperti waktu kita membuat user arin di LDAP server.
- Ini berarti LDAP client mengambil informasi di LDAP server tentang user arin
- Berpindahlah dari user arin ke user siska

\$su – siska

- DAP client akan membuat directory /home/siska di server
- Lakukan beberapa perintah berikut pada user-user lainnya

\$pwd

\$id

\$whoami

\$finger

Pustaka

- <https://www.linuxbabe.com/debian/set-up-openldap-server-debian>
 - <https://www.howtoforge.com/how-to-install-openldap-server-on-debian-12/>
 - <https://computingforgeeks.com/how-to-configure-ubuntu-as-ldap-client/>
- <https://www.flofaber.com/log/debian-ldap-auth>
- <https://ubuntu.com/server/docs/how-to-set-up-sssd-with-ldap>

Configuring nslcd

Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://hostname_or_IP_address:<port>". Alternatively, "ldaps://" or "ldapi://" can be used. The port number is optional.

When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name services are unavailable.

Multiple URIs can be separated by spaces.

LDAP server URI:

ldapi:///ldapmaster.fitri.edu

<Ok> <Cancel>

Configuring nslcd

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

LDAP server search base:

dc=ldapmaster,dc=fitri,dc=edu

<Ok> <Cancel>

Configuring libnss-ldapd

For this package to work, you need to modify the /etc/nsswitch.conf file to use the ldap datasource.

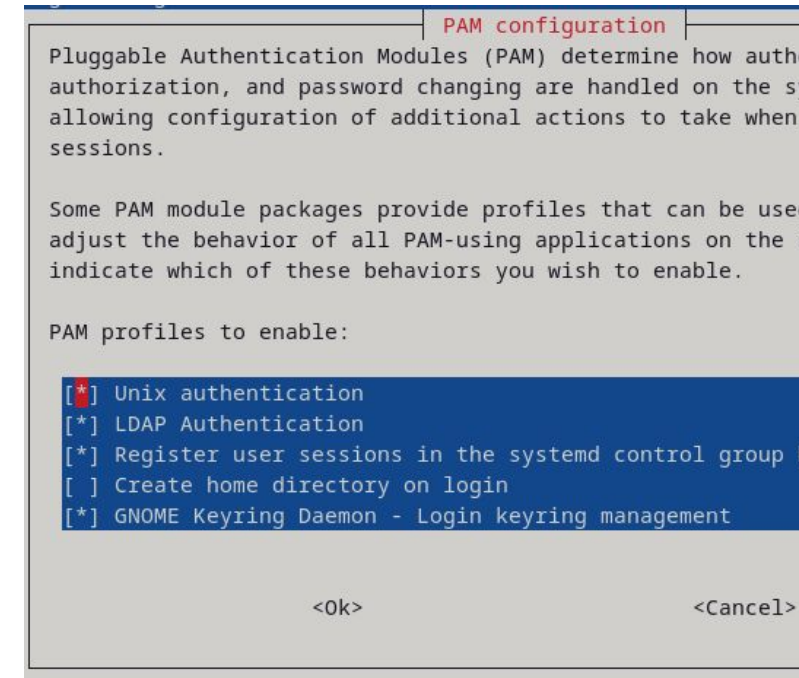
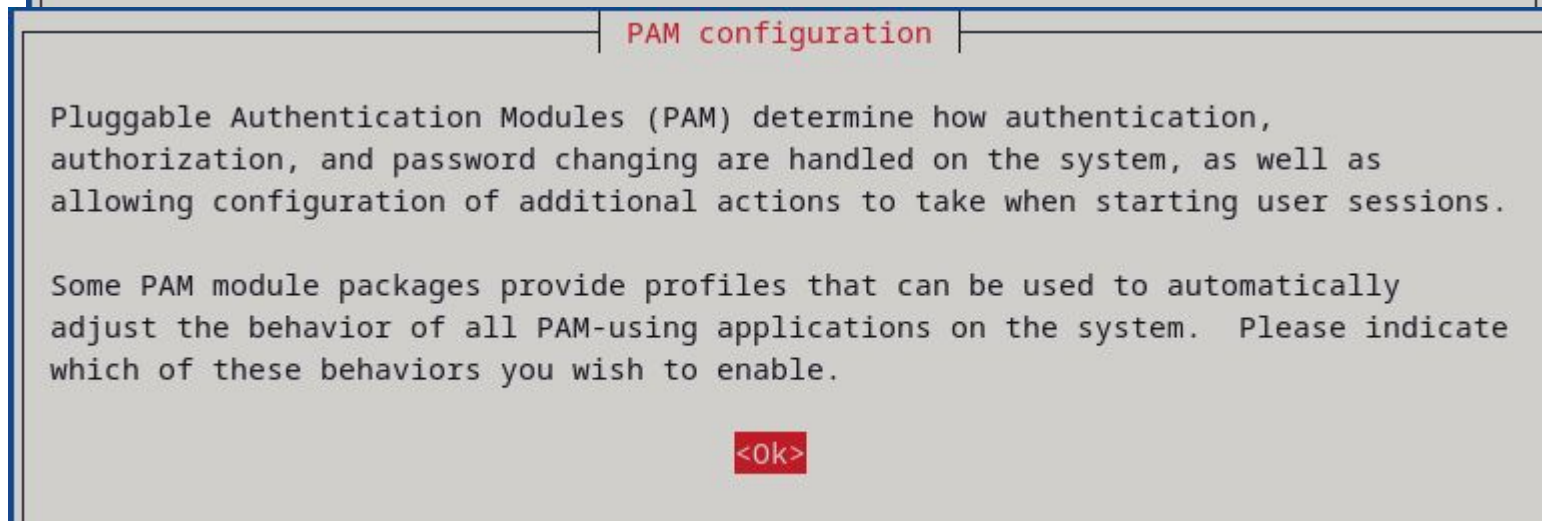
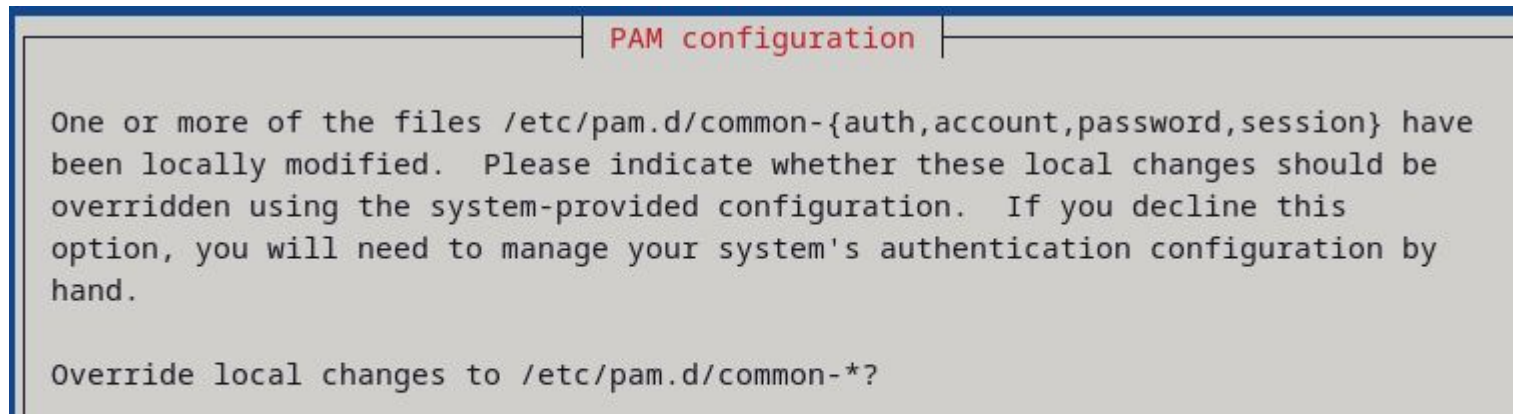
You can select the services that should have LDAP lookups enabled. The new LDAP lookups will be added as the last datasource. Be sure to review these changes.

Name services to configure:

- ☒ passwd
- ☒ group
- ☒ shadow
- ☐ hosts
- ☐ networks
- ☐ ethers

```
Adding system user `nslcd' (UID 115) ...
Adding new group `nslcd' (GID 122) ...
Adding new user `nslcd' (UID 115) with group `nslcd' .
Not creating home directory `/run/nslcd'.
Setting up libpam-ldapd:amd64 (0.9.12-4) ...
Setting up nslcd-utils (0.9.12-4) ...
Setting up libnss-ldapd:amd64 (0.9.12-4) ...
/etc/nsswitch.conf: enable LDAP lookups for group
/etc/nsswitch.conf: enable LDAP lookups for passwd
/etc/nsswitch.conf: enable LDAP lookups for shadow
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u7) ...
root@debian12:~#
```


#pam-auth-update



Rafael Struick

Suffix

People > Idapmaster > fitri > edu

RDN identifier

cn

Personal

Unix

Shadow

Co

P

Add

Hor

Set password

Password

••••

?

Repeat password

••••

Force password change ☐ ?

Unix

☒ Unix

Ok

Set random password

Cancel

Configuring nslcd

Please enter the Uniform Resource Identifier of the LDAP server. The format is "ldap://<hostname_or_IP_address>:<port>/" . Alternatively, "ldaps://" or "ldapi://" can be used. The port number is optional.

When using an ldap or ldaps scheme it is recommended to use an IP address to avoid failures when domain name services are unavailable.

Multiple URIs can be separated by spaces.

LDAP server URI:

ldapi://192.168.220.132

<Ok>

<Cancel>

Configuring nslcd

Please enter the distinguished name of the LDAP search base components of their domain names for this purpose. For example "example.net" would use "dc=example,dc=net" as the distinguished search base.

LDAP server search base:

dc=ldapmaster,dc=fitri,dc=edu

<Ok>

<Cancel>

Configuring nslcd

Please choose what type of authentication the LDAP database should require (if any):

- * none: no authentication;
- * simple: simple bind DN and password authentication;
- * SASL: any Simple Authentication and Security Layer mechanism.

Configuring nslcd

Please enter the name of the account that will be used to log in to the LDAP database. This value should be specified as a DN (distinguished name).

LDAP database user:

user.ldif

Configuring nslcd

Please enter the password that will be used to log in to the

LDAP user password:

Configuring nslcd

Please choose whether the connection to the LDAP server should use StartTLS to encrypt the connection.

Use StartTLS?

<Yes>

<No>