

Laporan Praktikum 9

Administrasi Sistem

LDAP



Muhammad Azhar Rasyad

0110217029

Teknik Informatika 1

Sekolah Tinggi Teknologi Terpadu Nurul Fikri

2018

LDAP

LDAP (Lightweight Directory Access Protocol) adalah adalah sebuah protokol aplikasi untuk mengakses dan memelihara informasi direktori terdistribusi.

Berikut merupakan **implementasi dari LDAP** dan sistem operasi yang digunakan adalah **Ubuntu 16.04 LTS** :

Lab 9.1 Menginstal openldap server

- Untuk menerapkan layanan data direktori (directory services) menggunakan LDAP, maka pada sistem komputer linux Anda harus terlebih dahulu diinstal perangkat lunak LDAP server yaitu salah satunya adalah openldap. Untuk instalasi openldap dapat menggunakan perintah seperti berikut ini:

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ sudo apt-get install slapd ldap-utils  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
ldap-utils is already the newest version (2.4.42+dfsg-2ubuntu3.4).  
slapd is already the newest version (2.4.42+dfsg-2ubuntu3.4).  
The following packages were automatically installed and are no longer required:  
  linux-headers-4.15.0-39 linux-headers-4.15.0-39-generic  
  linux-headers-4.4.0-140 linux-headers-4.4.0-140-generic  
  linux-image-4.15.0-39-generic linux-image-4.4.0-140-generic  
  linux-image-extra-4.4.0-140-generic linux-modules-4.15.0-39-generic  
  linux-modules-extra-4.15.0-39-generic  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
mazharrasyad@mazharrasyad:~$
```

Lab 9.2 Mengaktifkan LDAP server

- Setelah LDAP server terinstall, mungkin LDAP server tidak serta merta berjalan atau aktif, untuk itu Anda dapat memeriksanya dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~  
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access  
  Loaded: loaded (/etc/init.d/slapd; bad; vendor preset: enabled)  
  Active: inactive (dead) since Mon 2019-01-06 10:44:57 WIB; 1s ago  
  Docs: man:systemd-sysv-generator(8)  
  Process: 6458 ExecStop=/etc/init.d/slapd stop (code=exited, status=0/SUCCESS)  
  
Jan 06 10:30:57 mazharrasyad systemd[1]: Started LSB: OpenLDAP standalone server  
Jan 06 10:44:57 mazharrasyad systemd[1]: Stopping LSB: OpenLDAP standalone serve  
Jan 06 10:44:57 mazharrasyad slapd[6458]: * Stopping OpenLDAP slapd  
Jan 06 10:44:57 mazharrasyad slapd[5211]: daemon: shutdown requested and initiat  
Jan 06 10:44:57 mazharrasyad slapd[5211]: slapd shutdown: waiting for 0 operatio  
Jan 06 10:44:57 mazharrasyad slapd[5211]: DIGEST-MD5 common mech free  
Jan 06 10:44:57 mazharrasyad slapd[5211]: DIGEST-MD5 common mech free  
Jan 06 10:44:57 mazharrasyad slapd[5211]: slapd stopped.  
lines 1-14
```

- Jika LDAP server belum aktif, maka lakukan perintah berikut ini untuk mengaktifkannya.

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo systemctl start slapd
mazharrasyad@mazharrasyad:~$
```

- Lakukan pemeriksaan apakah LDAP server kini telah berjalan/aktif , dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access
   Loaded: loaded (/etc/init.d/slapd; bad; vendor preset: enabled)
   Active: active (running) since Mon 2019-01-06 10:45:28 WIB; 16s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6458 ExecStop=/etc/init.d/slapd stop (code=exited, status=0/SUCCESS)
  Process: 6505 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/slapd.service
           └─6512 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap

Jan 06 10:45:28 mazharrasyad systemd[1]: Starting LSB: OpenLDAP standalone serve
Jan 06 10:45:28 mazharrasyad slapd[6505]: * Starting OpenLDAP slapd
Jan 06 10:45:28 mazharrasyad slapd[6511]: @(#) $OpenLDAP: slapd (Ubuntu) (Oct 2
                               builddd@lgw01-amd64-005:/build/
Jan 06 10:45:28 mazharrasyad slapd[6512]: slapd starting
Jan 06 10:45:28 mazharrasyad slapd[6505]: ...done.
Jan 06 10:45:28 mazharrasyad systemd[1]: Started LSB: OpenLDAP standalone server
lines 1-16/16 (END)
```

Lab 9.3 Mengatur (konfigurasi) LDAP server

- Secara default, slapd mungkin berjalan dengan konfigurasi opsi yang minimum untuk menjalankan daemon ldap. Maka dibutuhkan konfigurasi tambahan agar LDAP server kita berjalan / bekerja sesuai yang kita inginkan.
- Langkah pertama, buat sebuah file yang diberi nama **backend.nurulfikri.ac.id.ldif** (letakkan di direktori **/tmp**) :

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo nano /tmp/backend.nurulfikri.ac.id.ldif
```

- Isi file seperti gambar dibawah ini kecuali untuk olcRootPW :
- Pastikan untuk atribut olcRootPW menunjukkan password root ldap, untuk itu diubah nilainya dengan string password yang Anda inginkan, atau dapat juga Anda menggunakan string password yang sudah dienkripsi, dengan menggunakan tool slappasswd.

```
mazharrasyad@mazharrasyad: ~
GNU nano 2.5.3 File: /tmp/backend.nurulfikri.ac.id.ldif Modified

# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=nurulfikri,dc=ac,dc=id
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=nurulfikri,dc=ac,dc=id
olcRootPW: changeMEtoSOMETHINGbetter
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lik_max_objects 1500
olcDbConfig: set_lik_max_locks 1500
olcDbConfig: set_lik_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=nurulfikri,dc=ac,dc=id" wri$
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=nurulfikri,dc=ac,dc=id" write by * read

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

- Sehingga isi filenya seperti berikut :

```
mazharrasyad@mazharrasyad: ~
GNU nano 2.5.3 File: /tmp/backend.nurulfikri.ac.id.ldif Modified

# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=nurulfikri,dc=ac,dc=id
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=nurulfikri,dc=ac,dc=id
olcRootPW: {SSHA}/4rfFtVXdh0qpcqcSIFp4qp24URPdB7m
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=nurulfikri,dc=ac,dc=id " wr$
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=nurulfikri,dc=ac,dc=id " write by * read

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

- Langkah berikut nya memuat seluruh konfigurasi tadi kedalam LDAP, dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/backe
nd.nurulfikri.ac.id.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"

adding new entry "olcDatabase=hdb,cn=config"
ldap_add: Invalid syntax (21)
    additional info: objectClass: value #1 invalid per syntax
mazharrasyad@mazharrasyad:~$
```

Lab 9.4 Mempopulasikan data

- LDAP backend sudah siap, sekarang Anda butuh mempopulasikan data kedalam LDAP direktori.
- Buatlah file dengan nama frontend.nurulfikri.ac.id.ldif (disimpan dalam direktori /tmp)

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ sudo nano /tmp/frontend.nurulfikri.ac.id.ldif
```

- Dengan isi file sebagai berikut:

```
GNU nano 2.5.3 File: /tmp/frontend.nurulfikri.ac.id.ldif Modified  
  
# Create top level object n domain  
dn: dc=nurulfikri,dc=ac,dc=id  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: STT Terpadu Nurul Fikri  
dc: nurulfikri  
description: LDAP Root Directory of STT NF  
  
# Admin user.  
dn: cn=admin,dc=nurulfikri,dc=ac,dc=id  
objectClass: simpleSecurityObject  
objectClass: organizationalRole  
cn: admin  
description: LDAP administrator  
userPassword: changeMEtoSOMETHINGbetter  
dn: ou=people,dc=nurulfikri,dc=ac,dc=id  
objectClass: organizationalUnit  
ou: people  
dn: ou=groups,dc=nurulfikri,dc=ac,dc=id  
objectClass: organizationalUnit  
ou: groups  
dn: uid=budi,ou=people,dc=nurulfikri,dc=ac,dc=id  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
  
uid: budi  
sn: Boy  
givenName: budi  
cn: budi keren  
displayName: budi keren  
uidNumber: 1000  
gidNumber: 10000  
userPassword: changeMEtoSOMETHINGbetter  
gecos: budi keren  
loginShell: /bin/bash  
homeDirectory: /home/budi  
shadowExpire: 1  
shadowFlag: 0  
shadowWarning: 7
```



```
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: budi@nurulfikri.ac.id
postalCode: 85711
l: Depok
o: Contoh saja
mobile: +62 (021) 7777777
homePhone: +62 08157228882
```

```
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

- Kemudian muat atau insert kedalam LDAP backend dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/front
end.nurulfikri.ac.id.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "dc=nurulfikri,dc=ac,dc=id"
ldap_add: Server is unwilling to perform (53)
        additional info: no global superior knowledge
mazharrasyad@mazharrasyad:~$
```

- Jika pada saat mempopulasikan data tersebut mengalami kegagalan seperti diatas, Hal itu menandakan Anda tidak memiliki ijin akses melakukan populasi data kedalam LDAP backend, Maka Buat file **/tmp/access.ldif** :

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo nano /tmp/access.ldif
```

- Dengan isi file seperti berikut ini :

```
mazharrasyad@mazharrasyad: ~
GNU nano 2.5.3      File: /tmp/access.ldif
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to *
    by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" write
    by * none
olcAccess: {1}to attrs=userPassword by self write by dn.base="cn=admin,dc=nurul$
olcAccess: {2}to * by dn.base="cn=admin,dc=nurulfikri,dc=ac,dc=id" write by sel$

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

- Selanjutnya lakukan modifikasi dengan menjalankan perintah berikut ini:

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /tmp/access.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}hdb,cn=config"
ldap_modify: No such object (32)
    matched DN: cn=config
mazharrasyad@mazharrasyad:~$
```

- Untuk langkah terakhir, coba Anda periksa apakah data tersebut sudah terpopulasi kedalam ldap backend dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo ldapsearch -x -b "dc=nurulfikri,dc=ac,dc=id" -D "cn=admin,dc=nurulfikri,dc=ac,dc=id" -W
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
mazharrasyad@mazharrasyad:~$
```

Lab 9.5 Manajemen LDAP (phpldapadmin)

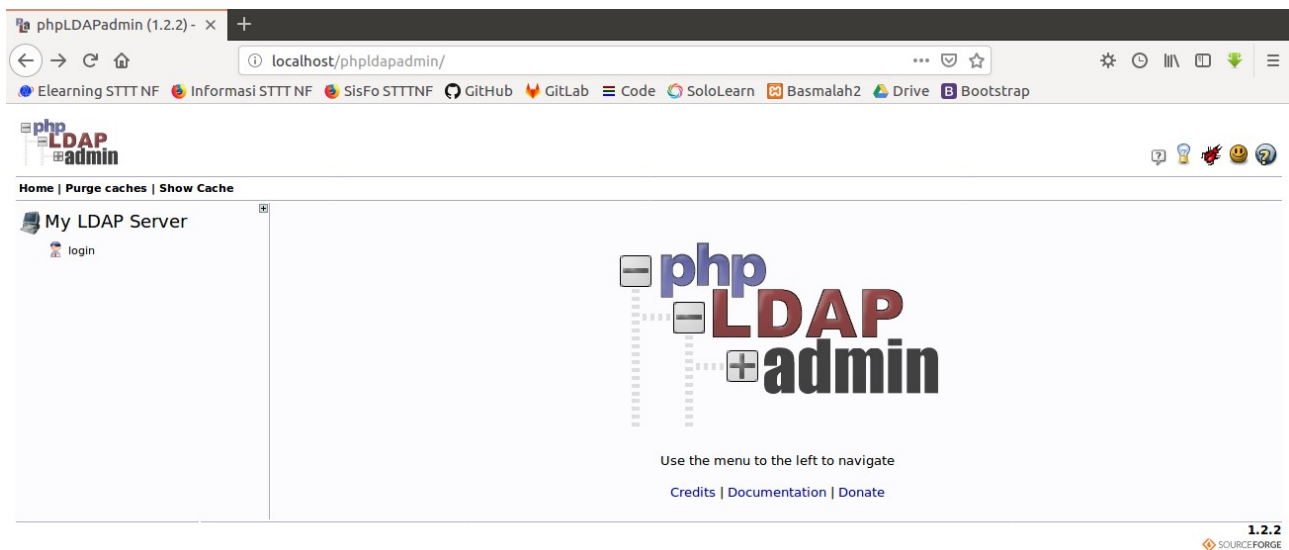
- Untuk kemudahan dalam melakukan manajemen direktori data ldap dapat menggunakan aplikasi yang menyediakan antarmuka grafis ataupun berbasis web. Salah satu aplikasi tersebut adalah aplikasi phpldapadmin. Aplikasi ini tersedia dalam repositori ubuntu .
- Lakukan instalasi phpldapadmin dengan perintah berikut:

```
mazharrasyad@mazharrasyad: ~
mazharrasyad@mazharrasyad:~$ sudo apt-get install apache2 libapache2-mod-php7.0 php7.0-ldap phpldapadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.18-2ubuntu3.9).
phpldapadmin is already the newest version (1.2.2-5.2ubuntu2.1).
libapache2-mod-php7.0 is already the newest version (7.0.33-1+ubuntu16.04.1+deb.sury.org+1).
php7.0-ldap is already the newest version (7.0.33-1+ubuntu16.04.1+deb.sury.org+1).
The following packages were automatically installed and are no longer required:
  libirs141 linux-headers-4.15.0-39 linux-headers-4.15.0-39-generic
  linux-headers-4.4.0-140 linux-headers-4.4.0-140-generic
  linux-image-4.15.0-39-generic linux-image-4.4.0-140-generic
  linux-image-extra-4.4.0-140-generic linux-modules-4.15.0-39-generic
  linux-modules-extra-4.15.0-39-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
mazharrasyad@mazharrasyad:~$
```

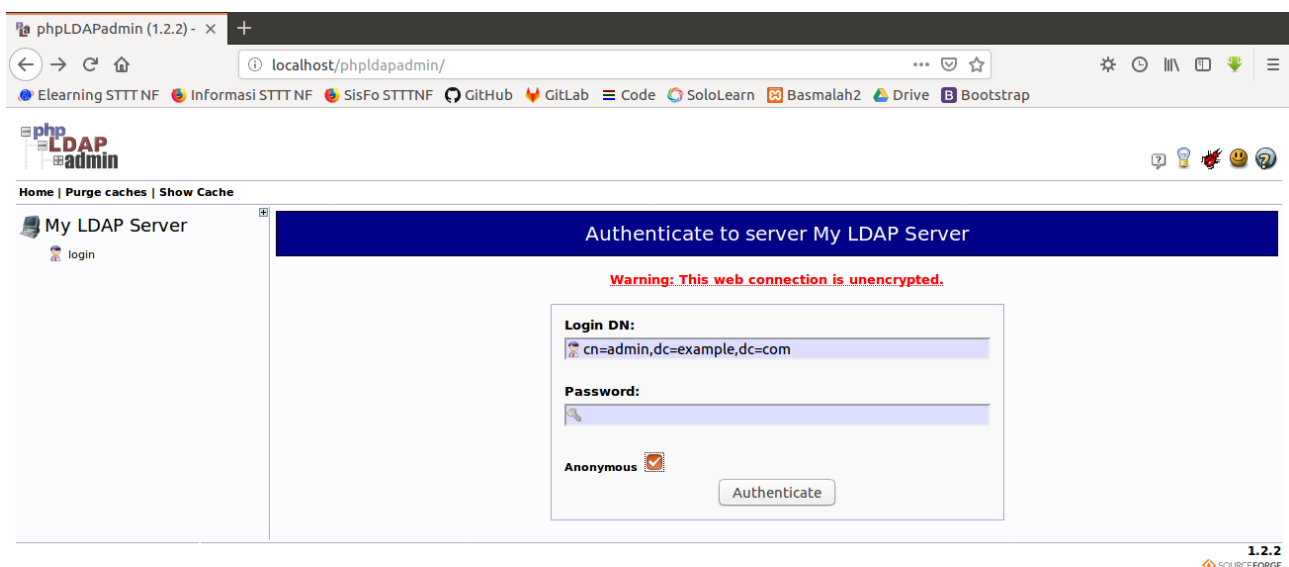

- Selanjutnya restart layanan / service apache dengan perintah:

```
mazharrasyad@mazharrasyad: ~  
mazharrasyad@mazharrasyad:~$ sudo systemctl restart apache2  
mazharrasyad@mazharrasyad:~$
```

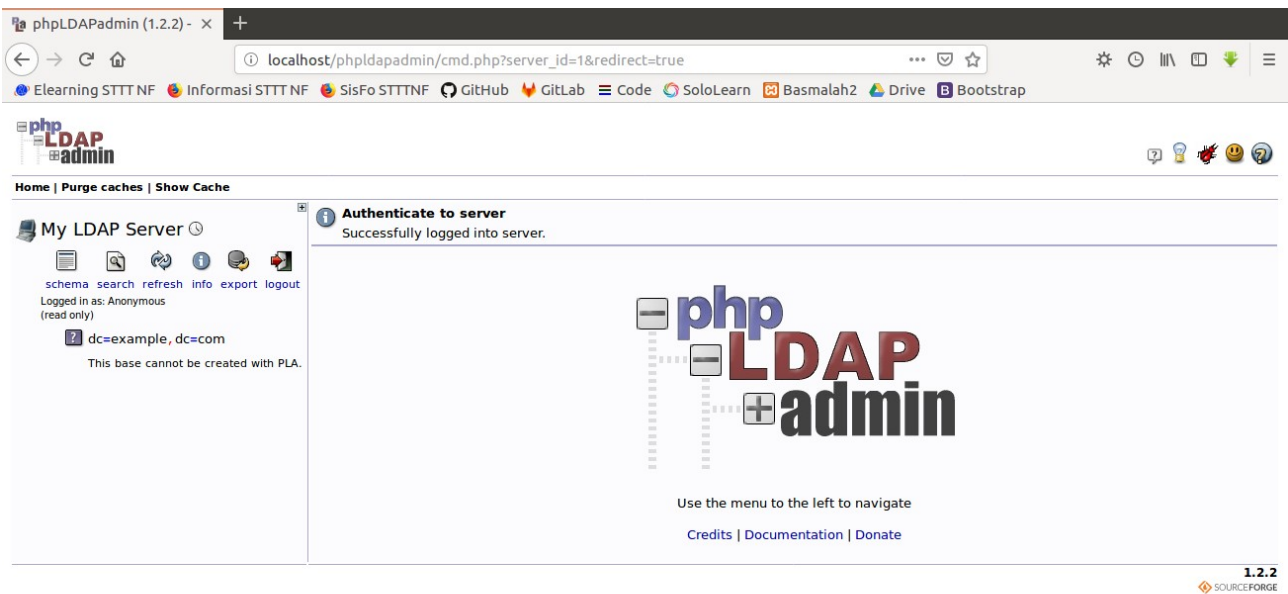
- Kemudian coba Anda akses phpldapadmin dengan menggunakan web browser dan mengetikkan alamat `http://localhost/phpldapadmin` . Kemudian Anda akan mendapatkan halaman seperti gambar berikut:



- Kemudian pada menu My LDAP Server klik tombol login hingga muncul gambar berikut :



- Kemudian tekan tombol Authenticate sebagai Anonymous hingga muncul gambar berikut :



----- *Selesai* -----

Referensi

- Modul praktikum Administrasi sistem dan jaringan – STT NF (Disusun oleh: Henry Saptono, S.Si, M.Kom)