9. Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP)

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

Secara teknis, LDAP hanya sebuah protokol yang mendefinisikan metode bagaimana suatu data direktori diakses. Yang juga mendefinisikan dan menjelaskan bagaimana data direpresentasikan dalam dalam layanan direktori (directory services). Dan juga LDAP mendefinisikan bagaimana data di-load (import) ke dalam dan disimpan (diekspor) dari layanan direktori (menggunakan LDIF).

LDAP berbasiskan pada standar X.500 untuk directory sharing, tetapi sedikit lebih kompleks dan membutuhkan resource yang lebih. Karena itulah, LDAP terkadanag dianggap sebagai "X.500 Lite", artinya LDAP bagaikan X.500 yang ringan
Seperti halnya X.500, LDAP mengorganisasikan informasi secara hirarki dengan menggunakan direktori-direktori data. Direktori-direktori ini dapat menyimpan berbagai macam informasi dan bahkan dapat digunakan seperti NIS (Network Information Service), yang memungkinkan siapapun dapat mengakses account mereka dari komputer manapaun dalam suatu jaringan yang terdapat LDAP server.

Dalam beberapa kasus, LDAP digunakan untuk keperluan sederhana sebagai Address Book directory, yang memungkinkan user atau pengguna dengan mudah mengkases contact information user lainnya. Namun LDAP sangat fleksibel dari pada Address Book tradisional. karena LDAP mampu mereferensikan suatu query informasi ke LDAP server -LDAP server lainnya.
LDAP sering digunakan oleh layanan layanan lain untuk authentication.

Keuntungan utama menggunakan LDAP adalah bahwa informasi keseluruhan suatu organisasi dapat dikonsolidasikan kedalam suatu central repository. Sebagai contoh, daripada menangani daftar user untuk masing-masing group dalam suatu organisasi , Anda dapat menggunakan LDAP sebagai suatu direktori data terpusat yang digunakan untuk mengkonsolidasikan berbagai informasi organisasi yang dapat diakses dari manapaun dalam jaringan. Dan karena LDAP mendukung Secure Sockets Layer (SSL) dan Transport Layer Security (TLS), maka keamanan data lebih terjaga.

Istilah dalam LDAP

- **entry** — suatu entry adalah sebuah unit tunggal dalam sebuah direktori LDAP. Setiap entri didefinisikan menggunakan suatu uniq Distinguished Name (DN).
- **attributes** — Attribute secara langsung diasosiasikan dengan suatu entry. Sebagai contoh , sebuah organisasi direpresentasikan sebagai sautu LDAP entry. Atribut-atribut yang diasosiasikan dengan organisasi seperti fax number, alamat dan seabagainya.Beberapa

atribut diperlukan, tetapi ada juga yang opsional. Suatu objectclass adalah sekumpulan definisi atribut-atribut yang diperlukan dan yang opsional untuk setiap entri.

- **Objectclass**, Definisi-definisi Objectclass dapat ditemukan dalam berbagai macam file schema, yang terletak dalam direktori /etc/openldap/schema/
- LDIF — LDAP Data Interchange Format (LDIF) adalah suatu file ASCII text yang merepresentasikan entri-entri LDAP. Format file inilah yang digunakan untuk mengimport data ke LDAP server. Format isi file LDIF seperti berikut ini:

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

- Setiap entri dapat mengandung beberapa pasangan <attrtype>: <attrvalue> . Suatu baris kosong (blank line) menunjukkan akhir dari suatu entri.

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:

```
# sudo apt-get install slapd ldap-utils
```

Atau jika menggunakan distribusi linux RedHat/CentOS, dapat menggunakan perintah berikut ini:

```
# yum install openldap-servers openldap-clients
```

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:

```
# sudo /etc/init.d/slapd status
```

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

```
# sudo /etc/init.d/slapd start
```

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

```
# sudo /etc/init.d/slapd status
```

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**)** dengan isi file sebagai berikut:

```
# 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_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 " write by
anonymous auth by self write by * none
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
```

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. Contoh** untuk membuat string password untuk root ldap yang dienkripsi **:**

```
# sudo slappasswd -s rahasia
{SSHA}drs1/MMJ9g2IB9O80zNHRSle6azZqZ8V
```

Sehingga ***olcRootPW: changeMEtoSOMETHINGbetter*** , dapat diubah menjadi
olcRootPW: {SSHA}drs1/MMJ9g2IB9O80zNHRSle6azZqZ8V

- Langkah berikut nya memuat seluruh konfigurasi tadi kedalam LDAP, dengan perintah berikut:
  ```
  $ sudo ldapadd -Y EXTERNAL -H ldapi:///
  -f /tmp/backend.nurulfikri.ac.id.ldif
  ```

Lab 9.4. Mempopulasikan data

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

```
# Create top-level object in 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
```

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

  ```
  # sudo  sudo ldapadd -Y EXTERNAL -H ldapi:/// -f
  /tmp/frontend.nurulfikri.ac.id.ldif
  ```

  Catatan:
  Jika pada saat mempopulasikan data tersebut mengalami kegagalan seperti berikut:

  ```
  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: Insufficient access (50)
        additional info: no write access to parent
  ```

Hal itu menandakan Anda tidak memiliki ijin akses melakukan populasi data kedalam LDAP backend, Maka lakukan hal berikut ini:

- Buat file **/tmp/access.ldif**, dengan isi file seperti berikut ini:

```
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=nurulfikri,dc=ac,dc=id" write by anonymous auth by * none
olcAccess: {2}to * by dn.base="cn=admin,dc=nurulfikri,dc=ac,dc=id" write by
self write by * read
```

- Selanjutnya lakukan modifikasi atribut **olcAccess** untuk **dn: olcDatabase={2}hdb,cn=config** , dengan menjalankan perintah berikut ini:

  ```
  # sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /tmp/access.ldif
  ```

- Untuk langkah terakhir , coba Anda periksa apakah data tersebut sudah terpopulasi kedalam ldap backend dengan perintah berikut:
  ```
  $ ldapsearch -x -b “dc=nurulfikri,dc=ac,dc=id” -D "cn=admin,
  dc=nurulfikri,dc=ac,dc=id" -W
  ```

- Selanjutnya cobalah Anda menambah data / entry user lainnya dengan format entry sebagai berikut:

```
dn: uid=hana,ou=people,dc=nurulfikri,dc=ac,dc=id
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: hana
sn: Zahra
givenName: Hana F Zahra
```

```
cn: hana fahmida
displayName: hana
uidNumber: 1001
gidNumber: 10000
userPassword: rahasia
gecos: Hana Fahmida Zahra
loginShell: /bin/bash
homeDirectory: /home/hana
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: hana@nurulfikri.ac.id
postalCode: 85711
l: Depok
o: Contoh saja juga
mobile: +62 (021) 8888888
homePhone: +62 08157228889
```

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:

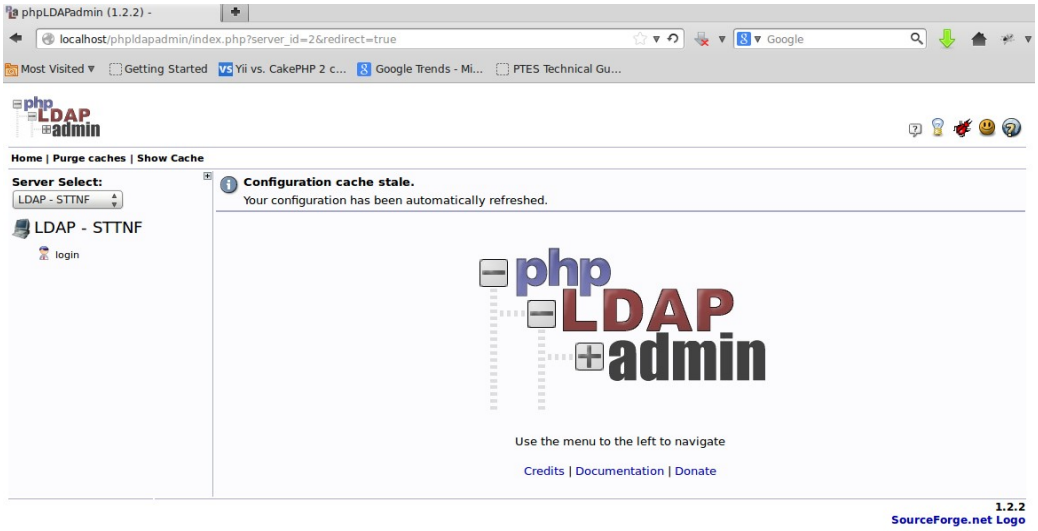
  ```
  # sudo apt-get install apache2 libapache2-mod-php5 php5-ldap phpldapadmin
  ```
- Selanjutnya restart layanan / service apache dengan perintah:

  ```
  # sudo /etc/init.d/apache2 restart
  ```

- Ubah atau sesuaikan konfigurasi phpldapadmin, dengan mengedit isi file konfigurasi phpldapadmin (/etc/phpldapadmin/config.php). **Tambahkan baris baris berikut ini pada akhir baris dari file tersebut**.

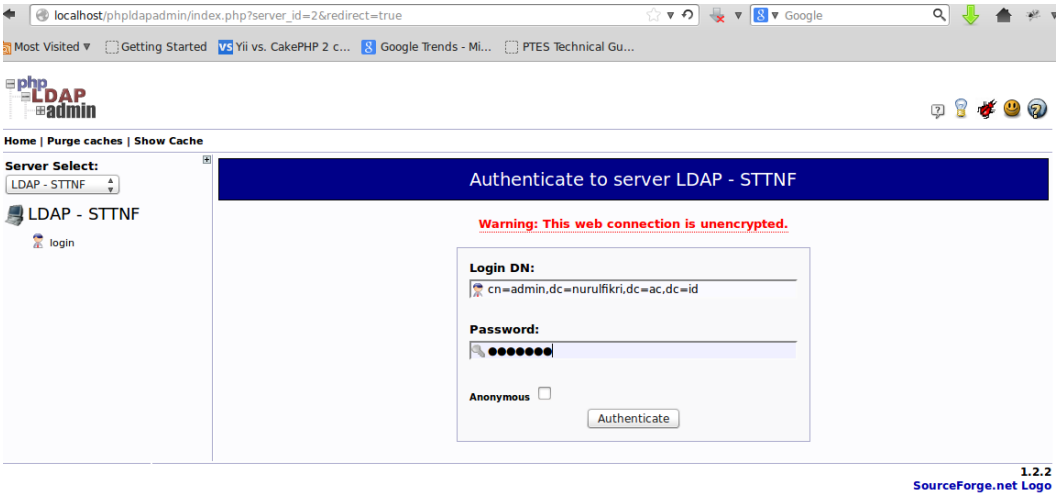
```
$servers->newServer('ldap_pla');
$servers->setValue('server','name','LDAP - STTNF');
$servers->setValue('server','host','127.0.0.1');
$servers->setValue('server','port',389);
$servers->setValue('server','base',array('dc=nurulfikri,dc=ac,dc=id'));
$servers->setValue('login','auth_type','session');
$servers->setValue('server','tls',false);
$servers->setValue('login','attr','dn');
```

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



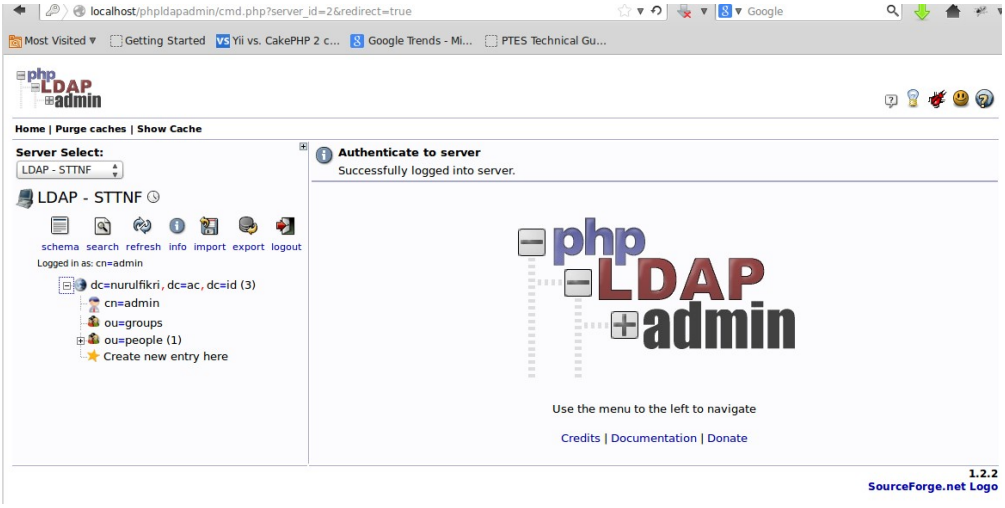
Gambar 1: phpldapadmin

- Kemudian login dengan terlebih dahulu memilih plihan server ke '**LDAP – STTN**F' (lihat gambar 1.). Dan klik hyperlink 'login' , masukkan Login dn dan password seperti tampak pada gambar 2 beriku.



Gambar 2: Login - phpldapadmin

- Selanjutnya akan tampak halaman seperti pada gambar 3 berikut:

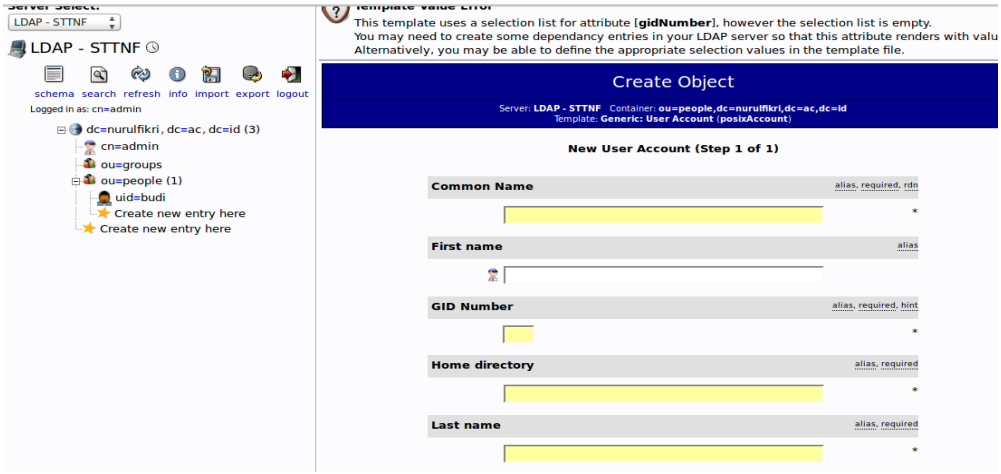


Gambar 3: Halaman utama phpldapadmin

- Coba Anda buat entry didalam ou=people,dc=nurulfikri,dc=ac,dc=id , perhatikan gambar 4 berikut:

Gambar 4: Create New Entry

- Kemudian pilih template untuk pembuatan entry/objek baru, pilihlah template "**Generic: User Account**" . Selanjutnya akan tampak form pembuatan entry/objek baru seperti tampak pada gambar 5 berikut.

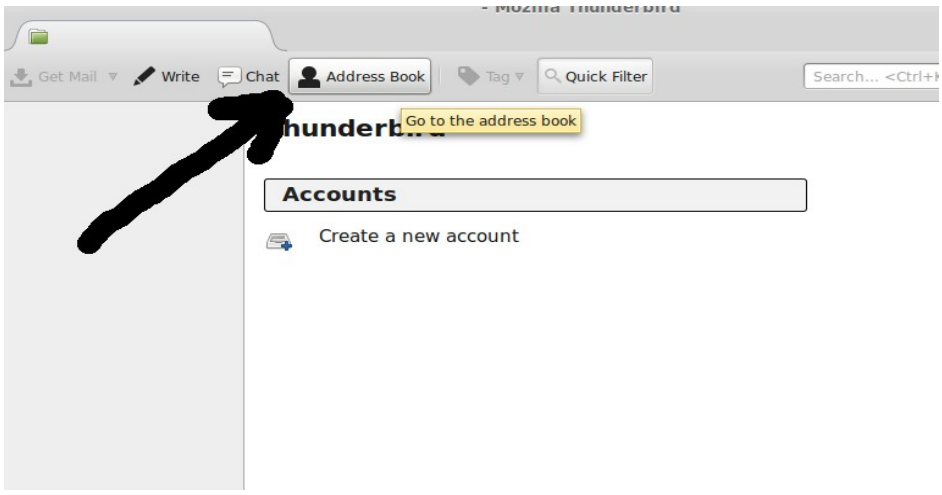


Gambar 5: Form pembuatan entry/objek baru

- Isilah atribut atribut yang terdapat pada form. Dan buktikan jika objek baru telah berhasil dibuat.

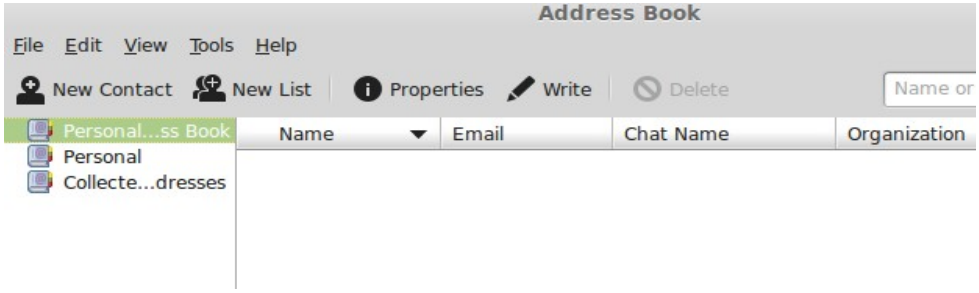
Lab 9.6. Mengakses LDAP via Aplikasi Mail Client (Thunderbird)

- Data direktori pada LDAP dapat diakses atau digunakan oleh layanan atau aplikasi lainnya.
- Coba Anda gunakan aplikasi mail client thunderbird, dimana pada aplikasi tersebut terdapat fitur Address Book. Lihat gambar 6 berikut.



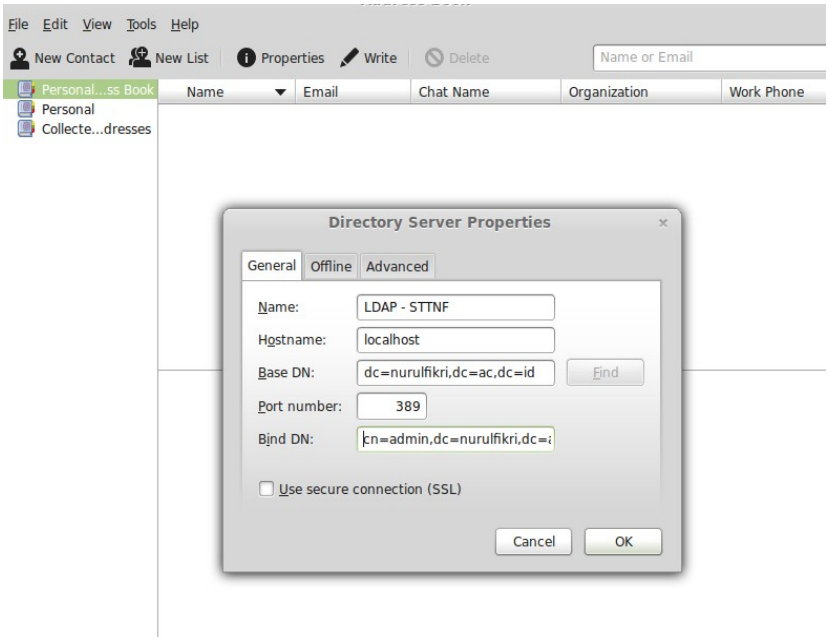
Gambar 6: Address Book - Thunderbird

- Kemudian akan muncul window baru seperti tampak pada gambar 7 berikut ini:



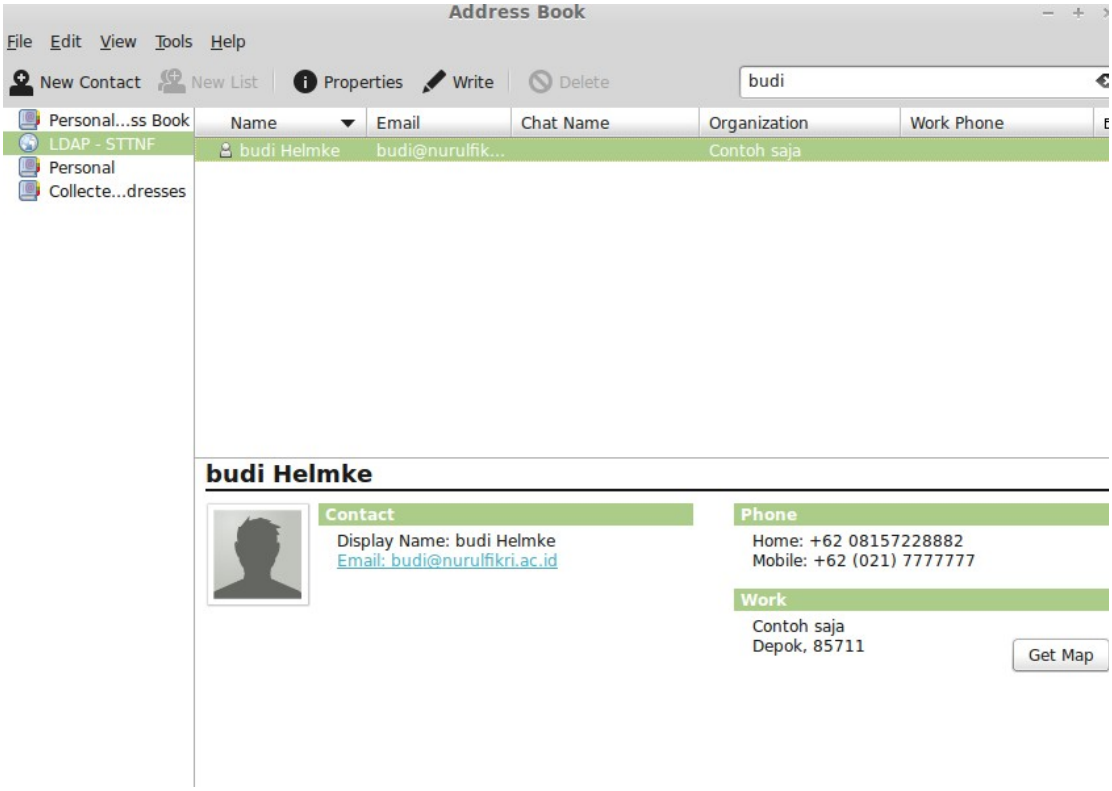
Gambar 7: Window Address Book

- Kemudian pilih menu **File -> New -> LDAP Directory**, maka akan muncul window pengaturan LDAP Directory, dan isilah seperti tampak pada gambar 8 berikut ini:



Gambar 8: New LDAP Directory

- Jika sudah membuat konfigurasi LDAP Directory, coba Anda lihat pada window Address Book pada *side pane (bagian menu sebelah kiri)* akan muncul menu 'LDAP – STTNF' . Anda klik menu tersebut, dan kemudian cobalah melakkan pencarian entry , dengan mengetikkan nama atau alamat email yang dicari pada text input pencarian di sisi atas sebelah kanan. Misal Anda ketik 'budi' kemudian tekan tombol enter, Anda akan ditanyakan password 'admin' ldap, ketikkanlah password tersebut, dan jika berhasil maka akan muncul entry yang berkaitan dengan nama 'budi' seperti tampak pada gambar 9 berikut:



Gambar 9: Pencarian (lookup) entry pada LDAP Directory