

Pengenalan LDAP

Ratdhian Cipta Sukmana

ratdix@yahoo.com

<http://ratdix.wordpress.com>

Lisensi Dokumen:

Copyright © 2003-2006 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pendahuluan

LDAP (*Light Weight Directory Access Protocol*) adalah sebuah protokol yang mengatur mekanisme pengaksesan layanan direktori (*Directory Service*) yang dapat digunakan untuk mendeskripsikan banyak informasi seperti informasi tentang *people, organizations, roles, services* dan banyak entitas lainnya. LDAP menggunakan model client-server, dimana client mengirimkan *identifier* data kepada server menggunakan protokol TCP/IP dan server mencoba mencarinya pada *DIT (Directory Information Tree)* yang tersimpan di server. Bila di temukan maka hasilnya akan dikirimkan ke client tersebut namun bila tidak maka hasilnya berupa pointer ke server lain yang menyimpan data yang di cari. Terdapat dua service utama pada LDAP yaitu *slapd* yang merupakan *LDAP daemon* dan *slurpd* yang merupakan *replication daemon*. *Slapd* melayani request dari client, query dan berkomunikasi dengan backend database sedangkan *slurpd* melayani replikasi data agar terus terjadi sinkronisasi data antara client dan server, dan untuk memfasilitasi pengisian dan perubahan informasi data dalam direktori di gunakanlah *LDIF (LDAP Data Interchange Format)*.

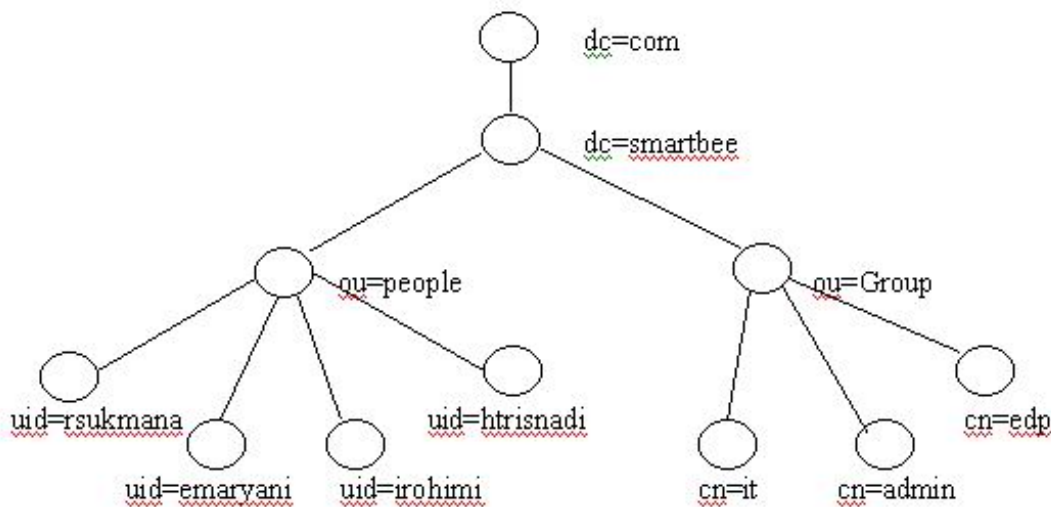
Konsep dasar

Untuk mempelajari LDAP, sangatlah penting apabila anda memahami arti dari direktori dan untuk apa dia digunakan. Mungkin tanpa sadar anda sudah terbiasa dengan direktori. Direktori dapat berupa *personal address book, phone book, yellow pages* bahkan *web direktori* seperti *Yahoo*. Direktori dapat membantu anda untuk

Komunitas eLearning IlmuKomputer.Com
Copyright © 2003-2006 IlmuKomputer.Com

menemukan informasi yang anda butuhkan, sebagai contoh *yellow pages*. Di sana anda dapat mencari alamat lengkap, nomor telepon, alamat website dan e-mail dari suatu perusahaan hanya dengan mencarinya berdasarkan 'nama' dari perusahaan yang telah disusun secara alfabetis pada direktori *yellow pages*.

Dalam terminologi komputer, *directory service* bisa dikatakan sebagai suatu database tempat penyimpanan data, yang dapat di gunakan untuk memberikan informasi-informasi yang berkaitan dengan objeknya. Bagian direktori mungkin dapat berisi kumpulan informasi tentang *user* seperti *sure name*, *first name*, *phone number*, *User ID*, *mail address* dan lain sebagainya. Untuk memudahkan pemahaman anda tentang konsep direktori ini, saya akan mencontohkan model seperti gambar berikut :



Secara prinsip struktur database pada suatu *directory service* adalah hierarki seperti yang di tunjukkan pada gambar di atas. Suatu *directory service* akan memiliki item yang di jadikan sebagai root. Untuk sebuah titik root, secara umum di tunjukkan dengan suatu atribut *dc* (*Domain Component*) atau *o* (*Organization*) mungkin juga *ou* (*Organization Unit*). Kemudian pada titik daun (leaf) biasanya akan berisi item dengan atribut *uid* (*User ID*) ataupun *cn* (*Common Name*). *Directory service* biasanya menyimpan informasi dalam bentuk struktur *tree* yang dinamakan *Directory Information Tree (DIT)*. Setiap titik pada *DIT* diberi suatu alamat, baik secara relatif maupun secara absolut. Untuk suatu alamat relatif sering disebut sebagai *RDN* (*Relative Distinguish Name*) sedangkan alamat yang absolut di sebut sebagai *DN* (*Distinguish Name*). Jadi apabila anda ingin mendapatkan informasi tentang user *rsukmana* pada gambar diatas, dapat di tuliskan dengan pengalamatan "*dn=uid=rsukmana,ou=people,dc=smartbee,dc=com*". Konsep seperti inilah yang di gunakan oleh direktori LDAP.

Schema, *objectClass* dan *attribute* adalah tiga hal yang sebaiknya anda ketahui dalam membangun sebuah server LDAP.

- **Schema** mendefinisikan seperangkat aturan yang mendeskripsikan jenis data apa saja yang akan di simpan, schema sangat membantu untuk menjaga konsistensi dan kualitas data sehingga mengurangi terjadinya duplikasi data.
- **ObjectClass** merupakan sekumpulan entri yang menginformasikan jenis group, dan membutuhkan atribut yang biasanya terdiri atas *attribute names*, *attribute type* dan *attribute syntax* yang semuanya terkumpul dalam suatu data valid pada setiap kelasnya.
- **Attribute** merupakan entri yang bersifat unik seperti *uid*, *cn*, *sn*, *ou*, *o*, *dc* dan lain sebagainya, attribute sendiri dapat merupakan *single value* maupun *multiple value*.

Instalasi OpenLdap

Untuk latihan instalasi OpenLDAP ini penulis menggunakan Fedora Core 4 Linux, sedangkan instalasi OpenLDAP baik client maupun server membutuhkan beberapa paket-paket pendukung tambahan, diantaranya :

- *OpenSSL*
- *Nss-LDAP*
- *Kerberos Authentication Services*
- *Cyrus's Simple Authentication and Security Layer Libraries*
- *Database Software (Ldbm)*
- *TCP Wrappers*

Saya asumsikan semua paket di atas telah terinstall dengan baik berserta semua dependensinya pada mesin Fedora anda. Lalu lakukan langkah-langkah berikut :

1. Cek dan install paket LDAP

Pastikan paket *openldap-server* telah terinstall pada mesin Fedora Anda, apabila belum Anda dapat menggunakan *cd* ke-3 Fedora Core 4

```
[root@ldap ~]# rpm -qa |grep ldap
```

```
openldap-2.2.23-5
```

```
openldap-clients-2.2.23-5
```

```
nss_ldap-234-4
```

```
php-ldap-5.0.4-10
```

```
python-ldap-2.0.6-4
```

```
openldap-devel-2.2.23-5
```

```
[root@ldap ~]# mount /dev/cdrom /media/cdrom/
```

```
mount: block device /dev/cdrom is write-protected, mounting read-only
```

```
[root@ldap ~]# rpm -ivh /media/cdrom/Fedora/RPMS/openldap-servers-2.2.23-5.i386.rpm
```

warning: /media/cdrom/Fedora/RPMS/openldap-servers-2.2.23-5.i386.rpm: Header V3 DSA signature:
NOKEY, key ID 4f2a6fd2

Preparing... ##### [100%]
openldap-servers ##### [100%]

2. Konfigurasi file slapd.conf

[root@ldap ~]# vim /etc/openldap/slapd.conf

```
-----isi slapd.conf-----

# Sekema yang di gunakan
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/nis.schema

# Dukungan koneksi LDAPv2
allow bind_v2
pidfile      /var/run/slapd.pid
argsfile     /var/run/slapd.args

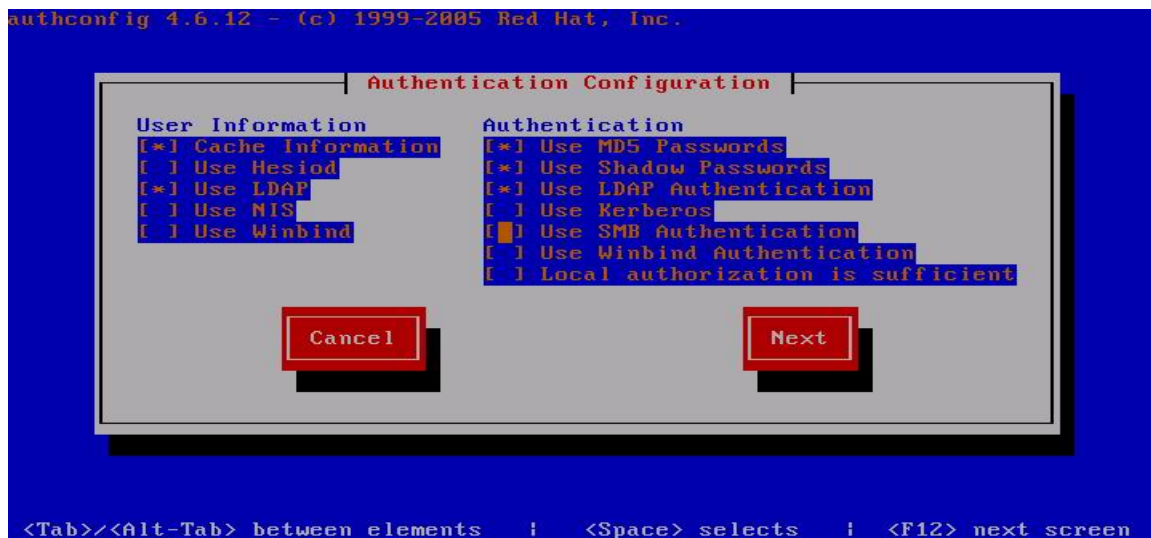
# Definisi Database yang di gunakan
database      ldbm
suffix        "dc=smartbee,dc=com"
rootdn        "cn=Manager,dc=smartbee,dc=com"
rootpw        rahasia
directory     /var/lib/ldap

# Index yang di gunakan untuk maintain database
index objectClass eq,pres
index ou,cn,mail,surname,givenname eq,pres,sub
index uidNumber,gidNumber,loginShell eq,pres
index uid,memberUid eq,pres,sub
index nisMapName,nisMapEntry eq,pres,sub

----- end -----
```

3. Edit file ldap.conf

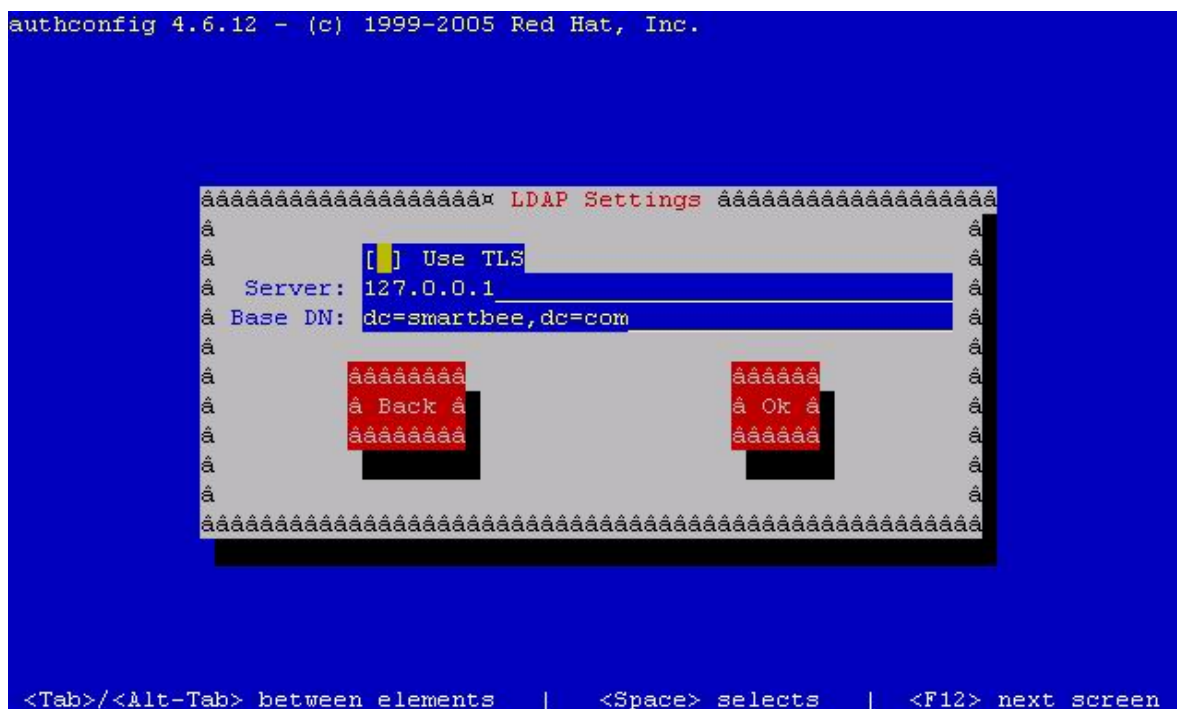
[root@ldap openldap]# authconfig



Pilih option :

- Cache Information
- Use LDAP
- Use MD5 Passwords
- Use Shadow Password
- Use LDAP Autentification

Lalu tekan Next



Arahkan LDAP Setting ke LDAP server anda

Server : 127.0.0.1

Base DN : dc=smartbee,dc=com

Untuk LDAP Client maka Anda dapat mengarahkan ke ip LDAP Server Anda

4. **Buat file LDIF**

```
[root@ldap ~]# cd /etc/openldap/
```

```
[root@ldap openldap]# vim basic.ldif
```

```
-----basic.ldif-----
```

```
dn: dc=smartbee,dc=com
objectClass: dcObject
objectClass: organization
o: smartbee
dc: smartbee
```

```
dn: ou=people,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: people
description: User List
```

```
dn: ou=groups,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: groups
description: Group List
```

```
dn: ou=hosts,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: hosts
description: Computer List
```

```
dn: uid=rsukmana,ou=people,dc=smartbee,dc=com
uid: rsukmana
givenname: ratdhian
sn: sukmana
cn: ratdhian sukmana
mail: ratdhian.sukmana@smartbee.com
userPassword: bonjovi
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
dn: uid=htrisnadi,ou=people,dc=smartbee,dc=com
uid: htrisnadi
givenname: harri
sn: trisnadi
cn: harri trisnadi
```

```
mail: harri.trisnadi@smartbee.com
userPassword: skidrow
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
dn: uid=irohimi,ou=people,dc=smartbee,dc=com
uid: irohimni
givenname: imi
sn: rohimi
cn: imi rohimi
mail: imi.rohimi@smartbee.com
userPassword: whitelion
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
dn: uid=emaryani,ou=people,dc=smartbee,dc=com
uid: emaryani
givenname: eni
sn: maryani
cn: eni maryani
mail: eni.maryani@smartbee.com
userPassword: mrbig
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

----- end -----

5. Jalankan service ldap dan masukkan data basic.ldif ke database ldap

```
[root@ldap openldap]# /etc/init.d/ldap start
```

```
Checking configuration files for slapd:
```

```
config file testing succeeded      [ OK ]
```

```
Starting slapd:                   [ OK ]
```

```
[root@ldap openldap]#
```

```
[root@ldap openldap]# ldapadd -x -D "cn=Manager,dc=smartbee,dc=com" -w rahasia -f basic.ldif
```

```
adding new entry "dc=smartbee,dc=com"
```

```
adding new entry "ou=people,dc=smartbee,dc=com"
```

```
adding new entry "ou=groups,dc=smartbee,dc=com"
```

```
adding new entry "ou=hosts,dc=smartbee,dc=com"
```

```
adding new entry "uid=rsukmana,ou=people,dc=smartbee,dc=com"
```

adding new entry "uid=htrisnadi,ou=people,dc=smartbee,dc=com"

adding new entry "uid=irohimi,ou=people,dc=smartbee,dc=com"

adding new entry "uid=emaryani,ou=people,dc=smartbee,dc=com"

Data yang baru di input akan terlihat pada databse LDAP sebagai berikut

```
[root@ldap openldap]# ll /var/lib/ldap/
total 80
-rw----- 1 ldap ldap 8192 Dec 19 21:50 cn.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 dn2id.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 givenName.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 id2entry.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 mail.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 nextid.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 objectClass.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 ou.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 sn.dbb
-rw----- 1 ldap ldap 8192 Dec 19 21:50 uid.dbb
```

6. Lakukan test untuk meng-queri user ID rsukmana

```
[root@ldap openldap]# ldapsearch -x uid=rsukmana
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: uid=rsukmana
# requesting: ALL
#
# rsukmana, people, smartbee.com
dn: uid=rsukmana,ou=people,dc=smartbee,dc=com
uid: rsukmana
givenName: ratdhian
sn: sukmana
cn: ratdhian sukmana
mail: ratdhian.sukmana@smartbee.com
userPassword:: Ym9uam92aQ==
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```



```
[root@ldap openldap]#
```

7. Lihat ini dari database LDAP anda

```
[root@ldap openldap]# ldapsearch -x
```

Ok, Selamat Server Ldap Anda telah berjalan dengan baik.

Referensi

- Rizcallah, Marcel. *LDAP DIRECTORIES*. Paris: Wiley, 2003
- Jackiewicz, Tom. *Deploying OpenLDAP*. United States: Apress, 2005
- Marshall, Brad *Introduction To LDAP*
- Susanto, Budi *Contoh Pengaturan OpenLDAP*
- <http://en.wikipedia.org> *Directory Service*
- <http://tuma.vlsm.org> *PAM LDAP*
- <http://www.openldap.org> *OpenLDAP-Administrator's Guide*

Biografi Penulis



Ratdhian Cipta Sukmana.

Mempelajari Ilmu Komputer berawal dari hobi, sejak SMU telah mengikuti pelatihan-pelatihan komputer hingga akhirnya dapat menyelesaikan S1 pada jurusan System Komputer Universitas Gunadarma Jakarta di akhir tahun 2001. Memulai karirnya sebagai Technical Support di beberapa perusahaan dan hingga kini masih aktif sebagai staff IT salah satu perusahaan Media di Jakarta. Sangat tertarik dengan Open Source dan Networking. Kopetensi inti pada bidang IT Support, Network Security, Administrator dan System Developer. Aktif di berbagai milis, dan selalu berusaha menggemakan konsep keterbukaan akan ilmu pengetahuan dengan semangat “Open Content”. Berbagai artikel komputasi menarik lain yang di tuliskan berdasarkan pengalaman tersedia di situs blog <http://ratdix.wordpress.com>