Praktikum

LDAP

I. Tujuan

Praktikan mampu memahami apa yang dimaksud dengan LDAP, cara kerja LDAP dan melakukan instalasi serta setting LDAP server pada sistem operasi Linux.

II. Keperluan

a. Komputer dengan OS Linux Fedora core 5
b. Repository fedora core 5 atau paket RPM openldap-server dari Fedora Core 5
c. Praktikan sudah pernah menggunakan command line (CLI) dan Editor pada Linux Operating System

III. Dasar Teori

LDAP (Lightweight Directory Access Protocol) dapat diartikan sebagai direktory services dan object oriented database. Apa saja yang LDAP dapat lakukan? LDAP menyediakan berbagai layanan seperti menyediakan data untuk client contohnya data karyawan, addressbook, email, account login dan banyak data lainnya. Dengan LDAP kita juga dapat melakukan searching informasi dengan berbagai filtering atau melakukan akses terhadap informasi khusus sebuah object. Penggunaan LDAP umumnya :

a. Pusat management data
b. Otentikasi
c. Email
d. Address Book
e. Accounting
f. dll

Implementasi LDAP yang sudah banyak digunakan oleh perusahaan-perusahaan adalah sebagai berikut :

- Open Source Software (OSS) menggunakan OpenLDAP, tinyLDAP, Fedora Directory Services (FDS)
- Sun (Bagian dari SunOne)
- Netscape (NDS)
- Microsoft (Bagian dari Active Directory)
- Novell (Bagian dari eDirectory)
- dan masih banyak lagi

Pada praktikum kali ini, kita akan menggunakan LDAP sebagai server untuk Sharing AddressBook menggunakan OpenLDAP.

IV. Langkah Langkah Praktikum

Instalasi Aplikasi OpenLDAP Server

Sebelum melakukan instalasi OpenLDAP dari Repository lokal yang ada, kita harus memastikan terlebih dahulu bahwa konfigurasi yum pada komputer masing masing sudah mengarah pada server http://172.20.112.100/local-repo/

[root@fedora ~]#vi /etc/yum.repos.d/fedora-core.repo

```
[Local-Install]
name=Fedora Core $releasever - $basearch
baseurl=http://172.20.112.100/local-repo/
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora
file:///etc/pki/rpm-gpg/RPM-GPG-KEY
```

Perintah CLI untuk instalasi aplikasi openldap-server dengan yum.

```
[root@fedora ~]# yum install openldap-servers
Loading "installonlyn" plugin
Setting up Install Process
Setting up repositories
```

```
        Local-Install
[1/1]
        Reading repository metadata in from local files
        Parsing package install arguments
        Resolving Dependencies
        --> Populating transaction set with selected packages. Please wait.
        ---> Downloading header for openldap-servers to pack into transaction
set.
        openldap-servers-2.3.19-4 100% |=============|  48 kB    00:00
        ---> Package openldap-servers.i386 0:2.3.19-4 set to be updated
        --> Running transaction check

        Dependencies Resolved

        ================================================================
         Package     Arch       Version          Repository        Size
        ================================================================
        Installing:
         openldap-servers   i386  2.3.19-4     Local-Install     2.2 M

        Transaction Summary
        ============================================================
        Install      1 Package(s)
        Update       0 Package(s)
        Remove       0 Package(s)
        Total download size: 2.2 M
        Is this ok [y/N]: y
        Downloading Packages:
        Running Transaction Test
        Finished Transaction Test
        Transaction Test Succeeded
        Running Transaction
          Installing: openldap-servers             ##########################
[1/1]
        bdb_db_open: unclean shutdown detected; attempting recovery.
        bdb_db_open: Warning - No DB_CONFIG file found in directory
/var/lib/ldap: (2)
        Expect poor performance for suffix dc=my-domain,dc=com.
```

```
Installed: openldap-servers.i386 0:2.3.19-4
Complete!
```

Setelah instalasi selesai, berikutnya kita akan konfigurasi ldap client, terlebih dahulu melakukan backup file konfigurasi default dengan cara :

```
[root@fedora~]#cp /etc/openldap/ldap.conf
/etc/openldap/ldap.conf.default
[root@fedora~]#vi /etc/openldap/ldap.conf
#
# LDAP Defaults
BASE    dc=domainku, dc=com
URI     ldap://localhost:389
TLS_REQCERT allow
#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
```

Kemudian membuat password user admin sebagai administrator dengan cara :

```
[root@fedora ~]# slappasswd
New password:
Re-enter new password:
{SSHA}h94LbFbnTEkLoP4MlerYKxV6iZxAobFe
```

Konfigurasi LDAP Server

Edit file konfigurasi LDAP server yang berada di /etc/openldap/slapd.conf , sebelumnya kita backup dulu dengan cara :

```
[root@fedora ~]# cp /etc/openldap/slapd.conf
/etc/openldap/slapd.conf.default
[root@fedora ~]# vi /etc/openldap/slapd.conf

# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /etc/openldap/schema/core.schema
```

```
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
########################################################################
# ldbm and/or bdb database definitions
########################################################################

database        bdb
suffix          "dc=domainku,dc=com"
rootdn          "cn=Manager,dc=domainku,dc=com"
rootpw          {SSHA}h94LbFbnTEkLoP4MlerYKxV6iZxAobFe

# Mode 700 recommended.
directory       /var/lib/ldap
# Indices to maintain for this 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

# DB_CONFIG Settings - For SleepyCat Berkeley DB
dbconfig set_cachesize 0 10485760 0
dbconfig set_lg_regionmax 262144
dbconfig set_lg_bsize 2097152
```

Setelah konfigurasi selesai, sebaiknya di test dahulu siapa tahu ada kesalahan sintaks atau setting dengan cara :

```
[root@fedora ~]# /etc/init.d/ldap configtest
Checking configuration files for slapd:  bdb_db_open: DB_CONFIG for
suffix dc=domainku,dc=com has changed.
Performing database recovery to activate new settings.
bdb_db_open: Recovery skipped in read-only mode. Run manual recovery
if errors are encountered.
config file testing succeeded
                                                        [  OK  ]
```

Langkah selanjutnya, memastikan services ldap bisa aktif setelah komputer di restart (run level 3 4 5). Caranya :

```
[root@fedora ~]# chkconfig --level 345 ldap on
[root@fedora ~]# chkconfig --list ldap
ldap      0:off   1:off   2:off   3:on    4:on    5:on    6:off
[root@fedora ~]#
```

Mengaktifkan/menjalankan6 LDAP server

```
[root@fedora ~]# /etc/init.d/ldap start
Checking configuration files for slapd:  config file testing
succeeded
                                                        [  OK  ]
Starting slapd:                                         [  OK  ]
```

MEMBUAT ADDRESS BOOK

Informasi dapat di import atau export ke direktory services LDAP menggunakan LDIF yakni LDAP Data Interchange Format yang sudah di definisikan pada RFC 2849.

Sekarang Server LDAP sudah selesai di konfigurasi dan sudah dijalankan, sesuai penggunaannya, kita dapat mulai mencoba mencari informasi yang ada pada direktory LDAP saat ini sebelum kita memulai mengentri data address book yang kita inginkan. Coba masukkan perintah search untuk menampilkan “namingContexts” berikut:

```
[root@fedora ~]# ldapsearch -x -b '' -s base '(objectclass=*)'
namingContexts
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=domainku,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
[root@fedora ~]#
```

Selanjutnya kita akan membuat file LDIF Organisasi untuk Address book yang akan di import kedalam Direktory LDAP. Pada Addressbook struktur Hirarki direktory services yang akan dibuat, pada bagian pertama adalah base directory, sedang pada entry yang kedua untuk Account Manager's (administrator). Kedua bagian selanjutnya merupakan komponen unit organisasional yang digunakan nantinya untuk mengotorisasi user dan mengentri address book

```
[root@fedora ~]# vi /etc/openldap/addressbook.ldif
dn: dc=domainku,dc=com
objectclass: dcObject
objectclass: organization
o: Home LDAP Server
dc: domainku

dn: cn=Manager,dc=domainku,dc=com
objectclass: organizationalRole
cn: Manager

dn: ou=users,dc=domainku,dc=com
ou: users
```

```
objectClass: top
objectClass: organizationalUnit

dn: ou=addressbook,dc=domainku,dc=com
ou: addressbook
objectClass: top
objectClass: organizationalUnit
```

Gunakan command “ldapadd” untuk memasukkan atau isi file LDIF diatas kedalam direktory LDAP sebagai scheme direktory.

```
[root@fedora ~]# ldapadd -x -D 'cn=Manager,dc=domainku,dc=com' -W -f
/etc/openldap/addressbook.ldif
Enter LDAP Password:
adding new entry "dc=domainku,dc=com"
adding new entry "cn=Manager,dc=domainku,dc=com"
adding new entry "ou=users,dc=domainku,dc=com"
adding new entry "ou=addressbook,dc=domainku,dc=com"
[root@fedora ~]#
```

Setelah sukses memasukkan isi data LDIF, kita bisa melakukan request listing isi semua entri yang sudah ada pada LDAP direktory dengan base “dc=domainku, dc=com”. Command ini akan menampilkan semua entri yang baru saja dimasukkan :

```
[root@fedora ~]# ldapsearch -x -b 'dc=domainku,dc=com'
'(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=domainku,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# domainku.com
dn: dc=domainku,dc=com
objectClass: dcObject
```

```
objectClass: organization
o: Home LDAP Server
dc:: ZG9tYWlua3Ug

# Manager, domainku.com
dn: cn=Manager,dc=domainku,dc=com
objectClass: organizationalRole
cn: Manager

# users, domainku.com
dn: ou=users,dc=domainku,dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

# addressbook, domainku.com
dn: ou=addressbook,dc=domainku,dc=com
ou: addressbook
objectClass: top
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@fedora ~]#
```

Sekarang kita sudah mendefinisikan dan melakukan import skema direktory kita. Kita bisa mulai menambah user user untuk digunakan sebagai address book pada direktory LDAP. Dibawah ini adalah contoh sederhana untuk file LDIF sebuah alamat (contact). Buat file ldif berikut (sesuaikan dengan nama Anda sebagai peserta praktikum ini)

```
root@fedora ~]# vi daftaralamat.ldif
dn:cn=Josua Sinambela,ou=addressbook,dc=domainku,dc=com
```

```
cn: Josua Sinambela
gn: Josua
sn: Sinambela
o: Home
l: Wirobrajan
street: WB3/64 Sindurejan
st: DIY
postalCode: 55251
pager: 1234 5678
homePhone: 7810307
telephoneNumber: 0274547506
facsimileTelephoneNumber: 0274547506
mobile: 085643552741
mail: josh@ugm.ac.id
objectClass: top
objectClass: inetOrgPerson
```

Kemudian isi file LDIF diatas dapat di masukkan kedalam Direktory LDAP dengan command “ldapadd”.

Akses kontrol secara umum pada server LDAP, mendefinisikan bahwa setiap orang dapat membaca entri direktory, tetapi hanya user manager (administrator) yang dapat menulisi direktory tersebut.

Untuk menambah data dari file LDIF, user manager akan melakukan otentikasi dengan menambahkan command line "-D 'cn=Manager,dc=domainku,dc=com' -W"

Jadi perintah untuk menambahkan content dari file ldif diatas adalah :

```
[root@fedora ~]# ldapadd -x -D 'cn=Manager,dc=domainku,dc=com' -W -f daftaralamat.ldif
Enter LDAP Password:
adding new entry "cn=Josua Sinambela,ou=addressbook,dc=domainku,dc=com"
```

Keamanan LDAP server dengan TLS

Secara default security setting pada server LDAP memperbolehkan setiap orang melihat atau melakukan pencarian pada setiap entri yang ada di Directory LDAP, tetapi yang bisa merubah atau menambah data tersebut hanyalah user Manager atau administrator.

Beberapa tipe security setting yang dapat kita lakukan pada LDAP server adalah menggunakan teknologi SSL/TLS, sehingga data yang diambil maupun dikirimkan dari server ke client atau dari client ke server sudah dalam data yang aman. Yang kedua adalah, dapat membuat access control kepada user yang sudah memiliki otentikasi (user/password) dan user yang belum dikenali (anonymous).

Dibawah ini merupakan sistem keamanan dan access kontrol yang mendefinisikan untuk menolak akses dari semua orang, kecuali orang orang yang sudah di otentikasi atau memiliki user account. Semua user yang sudah terauthentikasi (memiliki account) dapat mengganti informasi detil mereka masing masing, dan semua entry yang ada di "ou=addressbook,dc=domainku,dc=com" .

```
[root@fedora ~]# vi /etc/openldap/slapd.conf
## Tambahkan baris dibawah ini
TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
TLSCertificateFile /etc/pki/tls/certs/slapd.pem
TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem
security ssf=1 update_ssf=112 simple_bind=64

disallow bind_anon
access to *
       by self write
       by anonymous auth
       by users read
access to dn.subtree="ou=addressbook,dc=domainku,dc=com"
       by users write
```

Setelah konfigurasi diatas di masukkan dan di save. Maka sebelum menggunakan konfigurasi yang baru (dengan cara merestart ldap services), terlebih dahulu kita membuat certificate yang akan digunakan oleh server LDAP untuk keperluan TLS/SSL.

Caranya :

```
[root@fedora ~]# cd /etc/pki/tls/certs
[root@fedora certs]# make slapd.pem
Country Name (2 letter code) [GB]:ID
State or Province Name (full name) [Berkshire]:D.I.Yogyakarta
Locality Name (eg, city) [Newbury]:Yogyakarta
Organization Name (eg, company) [My Company     Ltd]:LearningWithExpert
Organizational Unit Name (eg, section) []:Konsultan Teknologi
Informasi Independen
Common Name (eg, your name or your server's hostname)
[]:Retooling Praktikum
Email Address []:josh@ugm.ac.id
[root@fedora certs]#
```

Kemudian mengganti group owner dan permission sertifikat yang baru kita buat agar dapat digunakan server LDAP dengan cara :

```
[root@fedora certs]# chown root.ldap /etc/pki/tls/certs/slapd.pem
[root@fedora certs]# chmod 640 /etc/pki/tls/certs/slapd.pem
```

Kemudian konfigurasi setting ldap.conf agar support penggunaan TLS.
Penggunaan TLS ditandai degan URI dengan protokol "ldaps"

```
[root@fedora ~]# vi /etc/openldap/ldap.conf
URI ldaps://127.0.0.1:636
BASE dc=domainku,dc=com
TLS_REQCERT demand
TLS_CACERTDIR /etc/pki/tls/certs/
TLS_CACERT /etc/pki/tls/certs/ca-bundle.crt
TLS_CRLCHECK peer
```

Kembali melakukan checking configurasi, mana tahu ada kesalahan ketik atau sintaks pada file file konfigurasi yang sudah diubah.

```
[root@fedora ~]# /etc/init.d/ldap configtest
Checking configuration files for slapd:  config file testing succeeded
                                                           [  OK  ]
```

Setelah tidak ada pesan error, kita bisa menggunakan konfigurasi yang baru degan cara merestart services LDAP.

```
root@fedora ~]# /etc/init.d/ldap restart
Stopping slapd:                                            [  OK  ]
Checking configuration files for slapd:  config file testing
succeeded                                                  [  OK  ]
Starting slapd:                                            [  OK  ]
[root@fedora ~]#
```

Sekarang konfigurasi dan skema direktory yang tersedia sudah support keamanan berbasis TLS dan user otentikasi. Sekarang kita bisa mencoba membuat user baru pada file LDIF yang akan di masukkan ke direktory LDAP. Sebelumnya user baru harus menggenerate passwordnya dengan comman "slappasswd"

```
root@fedora ~]# slappasswd
New password: <masukkan password user baru>
Re-enter new password: <masukkan password user baru>
{SSHA}KyFcZ07GVsoPf0bXmq4TMEFZIMh6qbMi
```

```
[root@fedora ~]# vi userbaru.ldif
dn:uid=josh,ou=users,dc=domainku,dc=com
uid: josh
userPassword: {SSHA}KyFcZ07GVsoPf0bXmq4TMEFZIMh6qbMi
objectClass: top
objectClass: account
objectClass: simpleSecurityObject
```

Untuk mengentri user baru pada Direktory LDAP, gunakan command berikut :

```
[root@fedora ~]# ldapadd -x -D 'cn=Manager,dc=domainku,dc=com' -W -f
userbaru.ldif
Enter LDAP Password:
adding new entry "uid=josh,ou=users,dc=domainku,dc=com"
```