Linux Single Sign On Server

Disusun Oleh:
Kurusetra Computer
www.kurusetra.web.id
Budi Santosa

Daftar Isi

OpenLDAP

OpenLDAP merupakan server Lightweight Directory Access Protocol (LDAP) yang biasa digunakan sebagai buku alamat atau media penyimpanan informasi user dan password. Server OpenLDAP mampu diintegrasikan dengan Samba, OpenVPN, ProFTPD, Postfix dll, untuk mengelola pengguna. Pada tutorial kali ini kita bahas konfigurasi OpenLDAP pada ubuntu 12.04 precise pangolin. Konfigurasinya cukup mudah, kita edit file slapd.conf, kemudian dikonversi menjadi file konfigurasi di direktori slapd.d dengan slaptest. Langkah konfigurasinya sebagai berikut.

Instalasi OpenLDAP

```
apt-get install slapd ldap-utils migrationtools phpldapadmin
apt-get install samba smbldap-tools smbclient samba-doc smbfs
cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
gzip -d /etc/ldap/schema/samba.schema.gz
```

Konfigurasi File slapd.conf

```
vim /usr/share/slapd/slapd.conf
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema
include         /etc/ldap/schema/misc.schema
include         /etc/ldap/schema/openldap.schema

pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args
loglevel        none
modulepath      /usr/lib/ldap
moduleload      back_hdb.la
sizelimit 500
tool-threads 1
backend         hdb
database        hdb
suffix          "dc=kurusetra,dc=web,dc=id"
rootdn "cn=admin,dc=kurusetra,dc=web,dc=id"
rootpw 1111
directory       "/var/lib/ldap"
dbconfig set_lk_max_objects 1500
dbconfig set_lk_max_locks 1500
dbconfig set_lk_max_lockers 1500
index           objectClass eq
lastmod         on
checkpoint      512 30
```

```
access to
attrs=userPassword,shadowLastChange,sambaNTPassword,sambaLMPassword,top,per
son,organizationalPerson,inetOrgPerson,posixAccount
        by self write
        by * read

access to
attrs=userPassword,shadowLastChange,sambaNTPassword,sambaLMPassword
        by dn="cn=admin,dc=kurusetra,dc=web,dc=id" write
        by anonymous auth
        by self write
        by * none


#access to attrs=userPassword,shadowLastChange
#        by dn="cn=admin,dc=kurusetra,dc=web,dc=id" write
#        by anonymous auth
#        by self write
#        by * none
access to dn.base="" by * read
access to *
        by dn="cn=admin,dc=kurusetra,dc=web,dc=id" write
        by * read
```

Konversi Direktori Konfigurasi

```
/etc/init.d/slapd stop
rm -fr /etc/ldap/slapd.d/*
slaptest -f /usr/share/slapd/slapd.conf -F /etc/ldap/slapd.d/
chown -R openldap.openldap /etc/ldap/slapd.d/
/etc/init.d/slapd restart
```

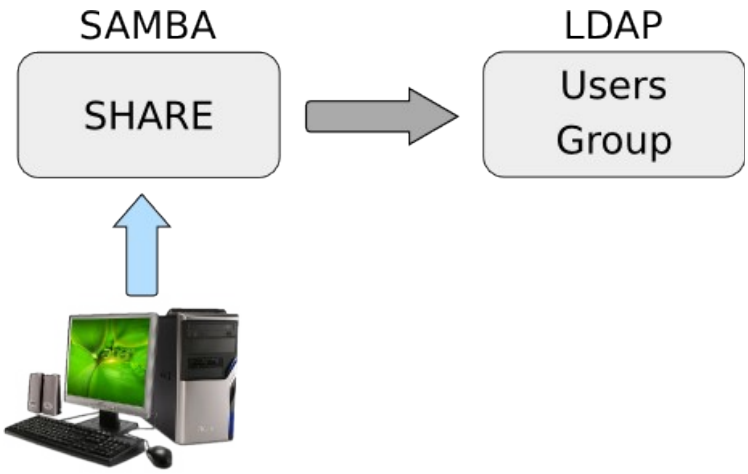
Konfigurasi Top Level Domain

```
vim kurusetra.ldif
dn: dc=kurusetra,dc=web,dc=id
objectClass: top
objectClass: dcObject
objectclass: organization
o: kurusetra
dc: kurusetra
description: Kurusetra Computer
```

Penambahan Top Level Domain

```
ldapadd -x -D cn=admin,dc=kurusetra,dc=web,dc=id -f kurusetra.ldif -W
Passwordnya 1111
```

Integrasi Samba LDAP



Konfigurasi Samba

```
workgroup = KURUSETRA
security = user
passdb backend = ldapsam:ldap://localhost/
ldap ssl = off
obey pam restrictions = no
#######################################################################
#COPY AND PASTE THE FOLLOWING UNDERNEATH "OBEY PAM RESTRICTIONS = NO"
#######################################################################
#
#       Begin: Custom LDAP Entries
#
ldap admin dn = cn=admin,dc=kurusetra,dc=web,dc=id
ldap suffix = dc=kurusetra,dc=web,dc=id
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers
ldap idmap suffix = ou=Users
; Do ldap passwd sync
ldap passwd sync = Yes
passwd program = /usr/sbin/smbldap-passwd %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n
*all*authentication*tokens*updated*
add user script = /usr/sbin/smbldap-useradd -m "%u"
ldap delete dn = Yes
delete user script = /usr/sbin/smbldap-userdel "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
domain logons = yes
#invalid users = root
```

Restart SAMBA.

```
/etc/init.d/samba restart
/etc/init.d/smbd restart
/etc/init.d/nmbd restart
```

#Tambahkan password LDAP pada samba

```
smbpasswd -w 1111
```

Konfigurasi SMBLDAP-TOOLS

```
cd /usr/share/doc/smbldap-tools/examples/
cp smbldap_bind.conf /etc/smbldap-tools/
cp smbldap.conf.gz /etc/smbldap-tools/
gzip -d /etc/smbldap-tools/smbldap.conf.gz
cd /etc/smbldap-tools/
net getlocalsid
vim smbldap.conf
```

Edit the file so that the following information is correct (according to your individual setup):

```
SID="S-1-5-21-949328747-3404738746-3052206637" ## This line must have the
same SID as when you ran "net getlocalsid"
sambaDomain="KURUSETRA"
slaveLDAP="127.0.0.1"
masterLDAP="127.0.0.1"
ldapTLS="0"
suffix="dc=kurusetra,dc=web,dc=id"
defaultMaxPasswordAge="99999"
sambaUnixIdPooldn="sambaDomainName=EXAMPLE,${suffix}"
userSmbHome=
userProfile=
userHomeDrive=
userScript=
mailDomain="kurusetra.web.id"
```

vim smbldap_bind.conf

Edit the file so that the following information is correct (according to your individual setup):

```
slaveDN="cn=admin,dc=kurusetra,dc=web,dc=id"
slavePw="1111"
masterDN="cn=admin,dc=kurusetra,dc=web,dc=id"
masterPw="1111"
```

Set the correct permissions on the above files:

```
chmod 0644 /etc/smbldap-tools/smbldap.conf
chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
```

Populate LDAP using smbldap-tools

Execute the command to populate the directory.

```
smbldap-populate -u 30000 -g 30000
```

At the password prompt assign your root password:

```
smbpasswd -w
1111
```

Verify that the directory has information in it by running the command:

```
ldapsearch -x -b dc=kurusetra,dc=web,dc=id | less
```

Integrasi LDAP ke Sistem Linux

Step 8: Add an LDAP user to the system

Add the user to LDAP

```
smbldap-useradd -a -m -M ricky -c "Richard M" ricky
smbldap-useradd -w client-winxp
# Here is an explanation of the command switches that we used.
-a allows Windows as well as Linux login
-m makes a home directory, leave this off if you do not need local access
-M sets up the username part of their email address
-c specifies their full name
```

Set the password the new account.

```
smbldap-passwd ricky
```

Step 9: Configure the server to use LDAP authentication.

Install the necessary software for this to work.

```
apt-get install auth-client-config libpam-ldap libnss-ldap
```

Answer the prompts on your screen with the following:

```
Should debconf manage LDAP configuration?: Yes
LDAP server Uniform Resource Identifier: ldapi://127.0.0.1
Distinguished name of the search base: dc=kurusetra,dc=web,dc=id
LDAP version to use: 3
Make local root Database admin: Yes
Does the LDAP database require login? No
LDAP account for root: cn=admin,dc=kurusetra,dc=web,dc=id
LDAP root account password: 1111
```

#untuk mengulang konfigurasi

```
#dpkg-reconfigure ldap-auth-client
#dpkg-reconfigure ldap-auth-config
#dpkg-reconfigure libnss-ldap
```

Open the /etc/ldap.conf file for editing.

```
vim /etc/ldap.conf
```

Configure the following according to your setup:

```
host 127.0.0.1
base dc=kurusetra,dc=web,dc=id
uri ldap://127.0.0.1/
rootbinddn cn=admin,dc=kurusetra,dc=web,dc=id
bind_policy soft
```

Copy the /etc/ldap.conf file to /etc/ldap/ldap.conf

```
cp /etc/ldap.conf /etc/ldap/ldap.conf
```

Create a new file /etc/auth-client-config/profile.d/open_ldap:

vim /etc/auth-client-config/profile.d/open_ldap

Insert the following into that new file:

```
[open_ldap]
nss_passwd=passwd: compat ldap
nss_group=group: compat ldap
nss_shadow=shadow: compat ldap
nss_netgroup=netgroup: compat ldap
pam_auth=auth       required     pam_env.so
 auth       sufficient   pam_unix.so likeauth nullok
 auth       sufficient   pam_ldap.so use_first_pass
 auth       required     pam_deny.so
pam_account=account    sufficient   pam_unix.so
 account    sufficient   pam_ldap.so
 account    required     pam_deny.so
pam_password=password   sufficient   pam_unix.so nullok md5 shadow
use_authtok
 password   sufficient   pam_ldap.so use_first_pass
 password   required     pam_deny.so
pam_session=session    required     pam_limits.so
 session    required     pam_mkhomedir.so skel=/etc/skel/
 session    required     pam_unix.so
 session    optional     pam_ldap.so
```

Backup the /etc/nsswitch.conf file:

```
cp /etc/nsswitch.conf /etc/nsswitch.conf.original
```

Backup the /etc/pam.d/ files:

```
cd /etc/pam.d/
mkdir bkup
cp * bkup/
```

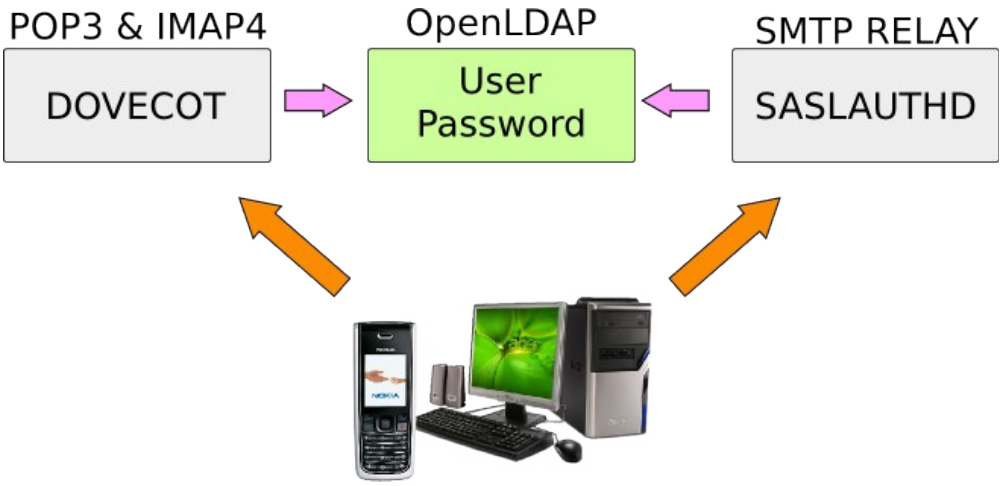
Enable the new LDAP Authentication Profile by executing the following

```
auth-client-config -a -p open_ldap
```

Reboot the server and test to ensure that you can still log in using SSH and LDAP.

```
ldconfig
id ricky
reboot
```

Integrasi Dovecot POP3 & IMAP4



Konfigurasi Dovecot

```
apt-get install dovecot-pop3d dovecot-imapd dovecot-ldap
```

vim /etc/dovecot/dovecot.conf

```
listen = *, ::
```

vim /etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }

service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}
```

vim /etc/dovecot/conf.d/10-mail.conf
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_privileged_group = mail

vim /etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
auth_mechanisms = plain
!include auth-ldap.conf.ext
```

vim /etc/dovecot/dovecot-ldap.conf.ext

```
hosts = 127.0.0.1
dn = cn=admin,dc=kurusetra,dc=web,dc=id
dnpass = 1111
ldap_version = 3
base = dc=kurusetra,dc=web,dc=id
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_filter = (&(objectClass=posixAccount)(uid=%u))
```

Integrasi Postfix SASL Auth

Konfigurasi SASL Auth

apt-get install libsasl2-modules-ldap sasl2-bin libsasl2-modules
vim /etc/saslauthd.conf

```
ldap_servers: ldap://localhost
ldap_password_attr: userPassword
ldap_filter: uid=%u
ldap_search_base: ou=Users,dc=kurusetra,dc=web,dc=id
```

```
mkdir /var/spool/postfix/var/
mkdir /var/spool/postfix/var/run/
mkdir /var/spool/postfix/var/run/saslauthd
chown -R root:sasl /var/spool/postfix/var/
chmod 710 /var/spool/postfix/var/run/saslauthd
adduser postfix sasl
ln -s /var/spool/postfix/var/run/saslauthd /var/run/saslauthd
```

vim /etc/default/saslauthd

```
MECHANISMS="ldap"
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

vim /etc/postfix/sasl/smtpd.conf

```
pwcheck_method: saslauthd
mech_list: LOGIN PLAIN
```

POSTFIX SASL AUTH

vim /etc/postfix/main.cf

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
smtpd_sasl_authenticated_header = yes
```

```
smtpd_recipient_restrictions = reject_unauth_pipelining, permit_mynetworks,
permit_sasl_authenticated, reject_non_fqdn_recipient,
reject_unauth_destination
```

Restart SASL

```
/etc/init.d/saslauthd restart
```

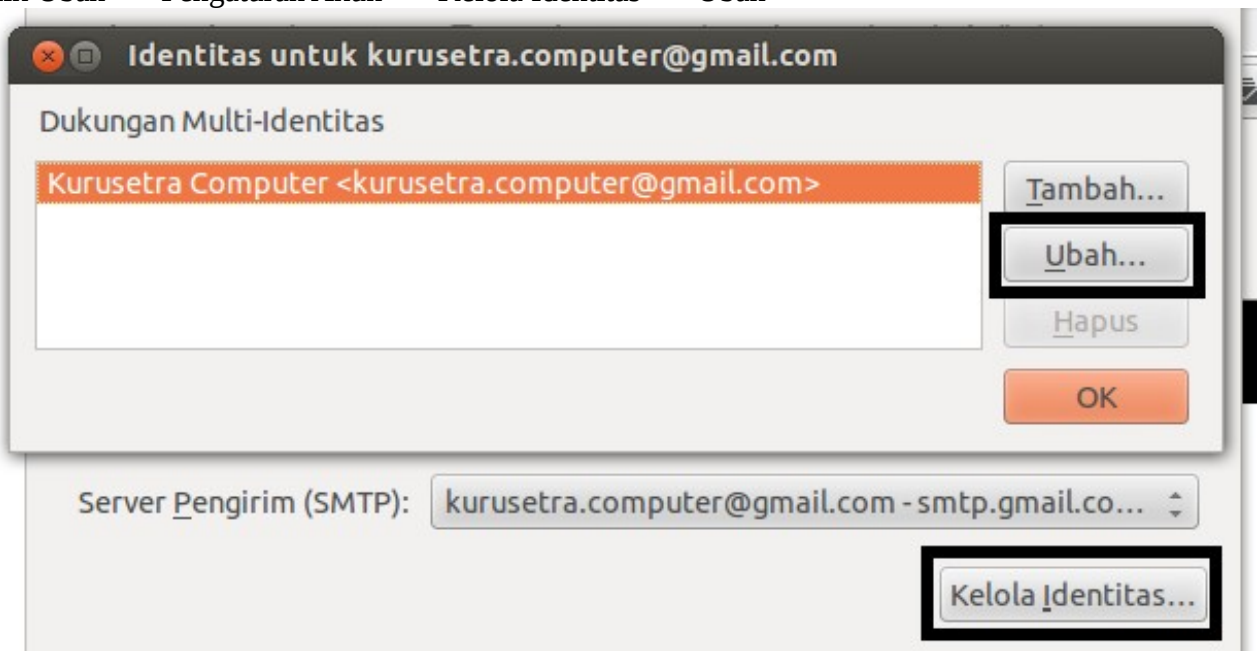
Pengujian SASL LDAP Auth

testsaslauthd -u nunik -p 261278
testsaslauthd -f /var/spool/postfix/var/run/saslauthd/mux -u nunik -p 261278

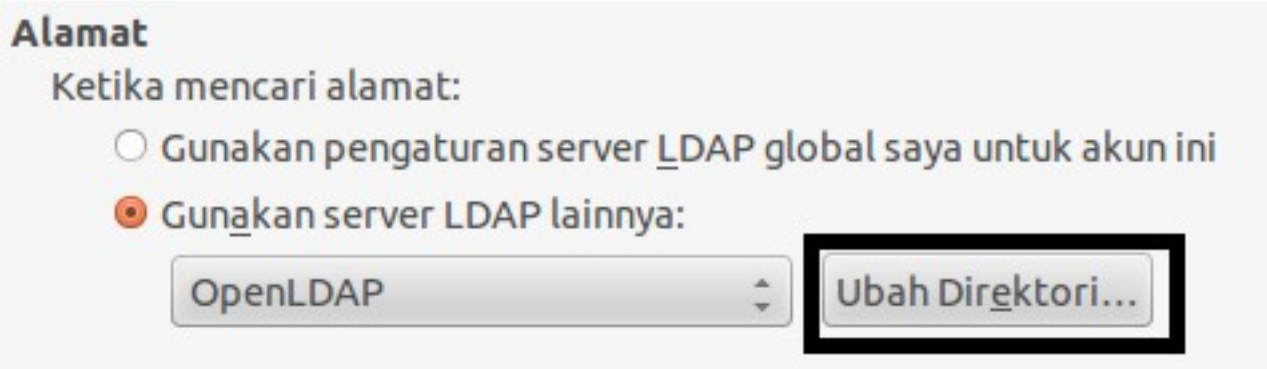
Integrasi Addressbook

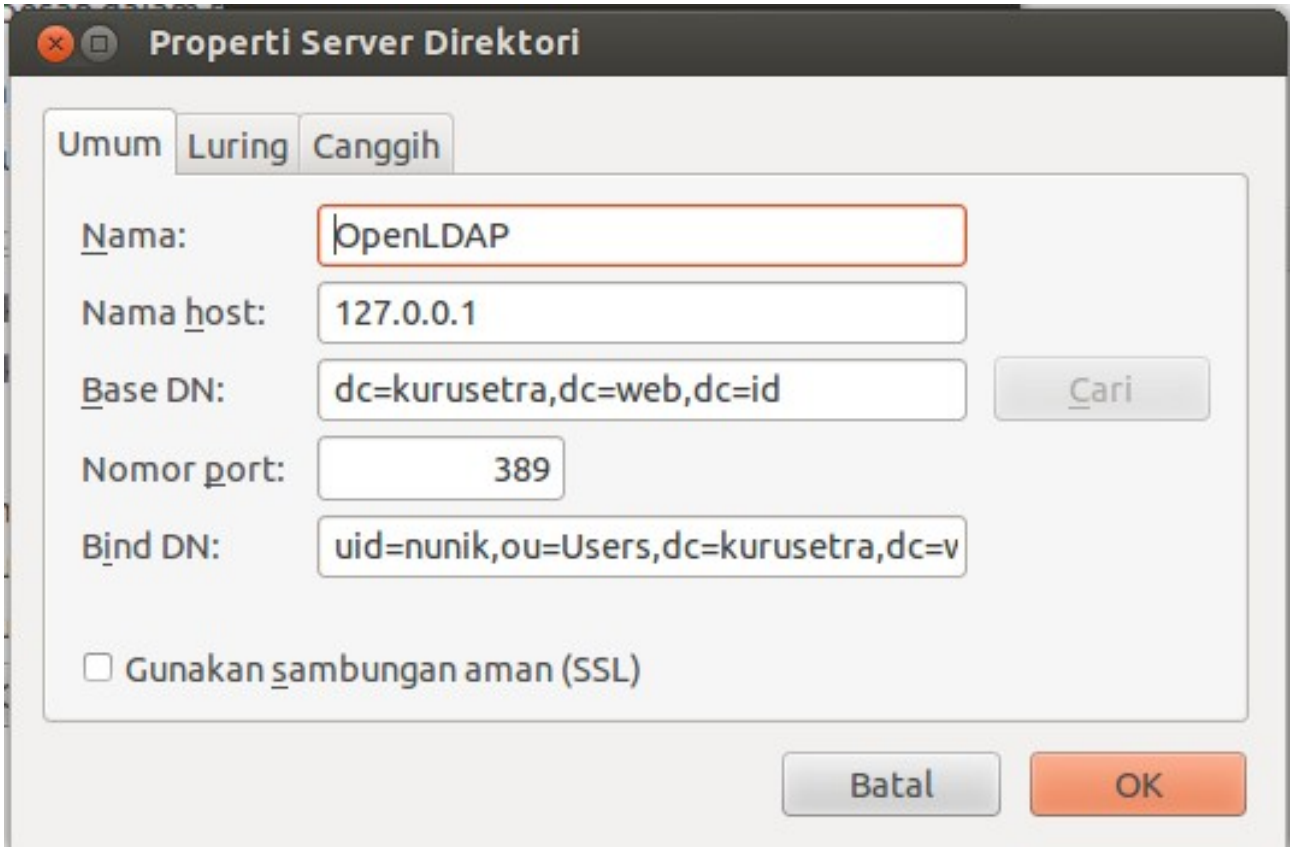
Konfigurasi Thunderbid Addressbook

Klik Ubah --> Pengaturan Akun --> Kelola Identitas --> Ubah



Klik Susunan & Alamat --> Pilih Gunakan Server LDAP Lain nya
--> Ubah Direktori --> Tambah





Nama : OpenLDAP
Nama Host : 127.0.0.1
Base DN : dc=kurusetra,dc=web,dc=id
Nomor Port : 389
Bind DN : uid=nunik,ou=Users,dc=kurusetra,dc=web,dc=id

Openfire Jabber Server

Instalasi Java Runtime

tar xzvf jre-7u7-linux-i586.tar.gz
mkdir /usr/java
mv jre1.7.0_07/ /usr/java/

Instalasi OpenFire

Download openfire di url http://www.igniterealtime.org/downloads/index.jsp
dpkg -i openfire_3.7.1_all.deb

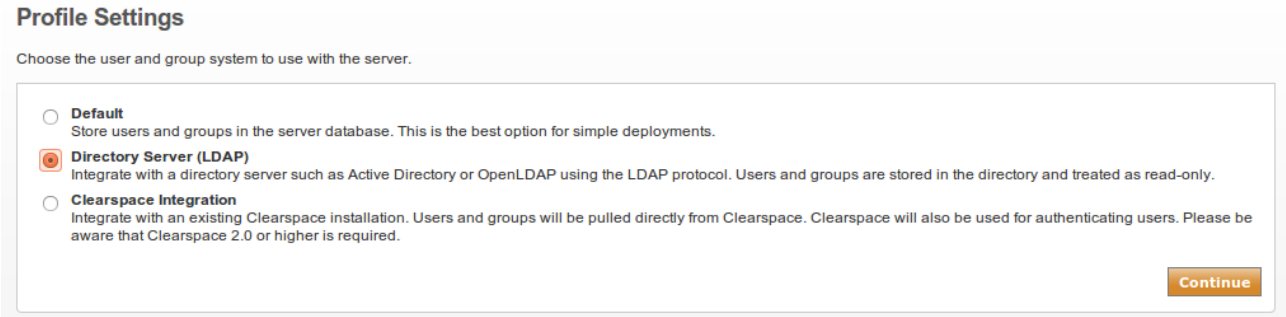
Startup Openfire

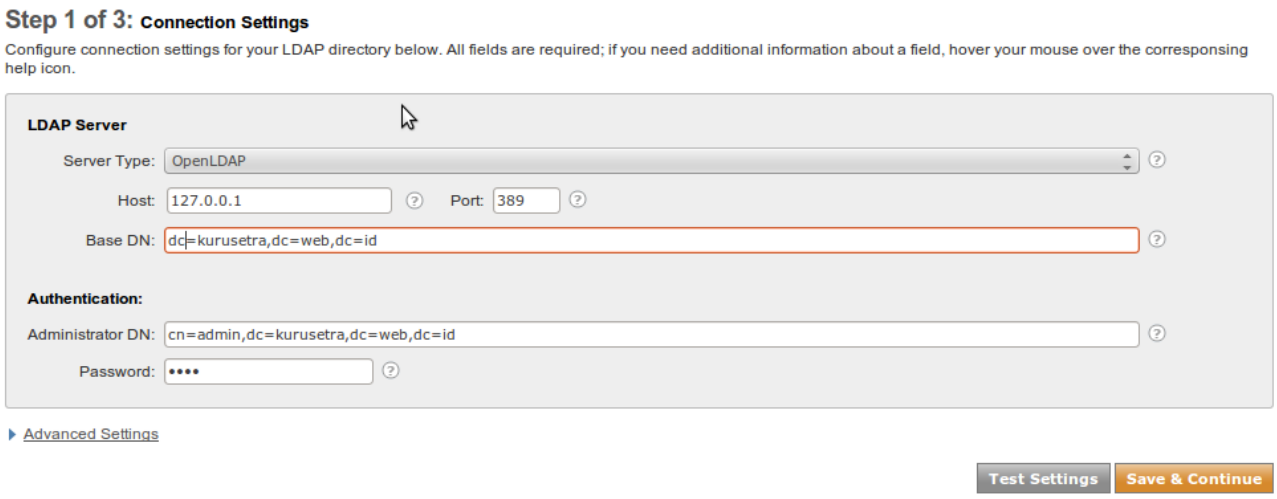
vim /etc/init.d/openfire
export JAVA_HOME=/usr/java/jre1.7.0_07/

Buka Web Browser

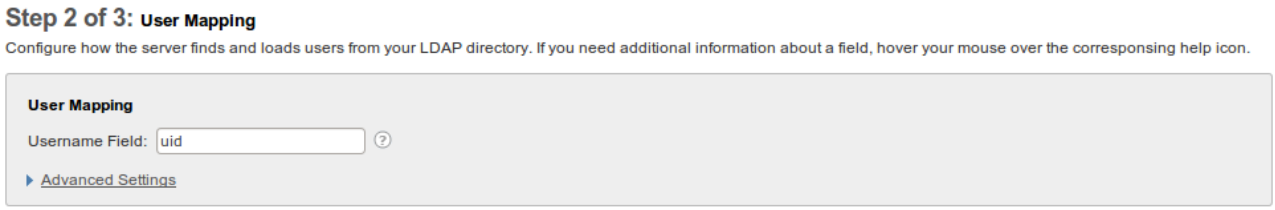
http://127.0.0.1:9090

Integrasi LDAP dengan OpenFire

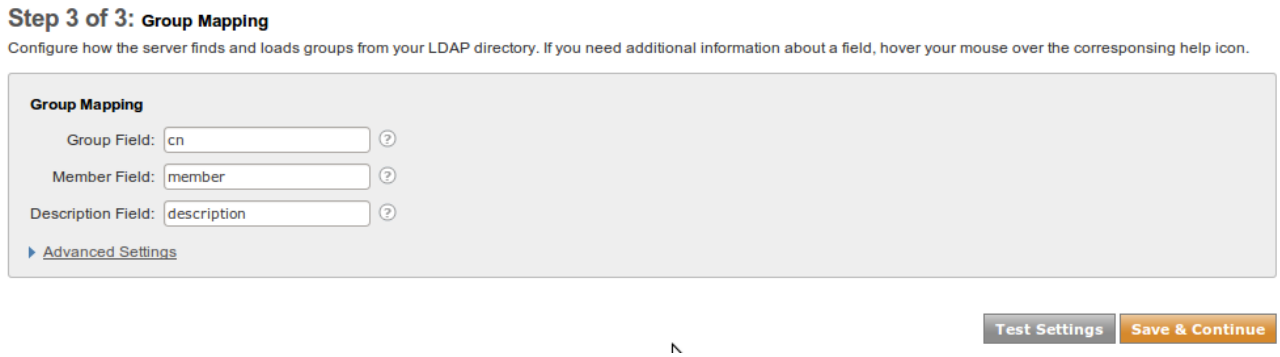




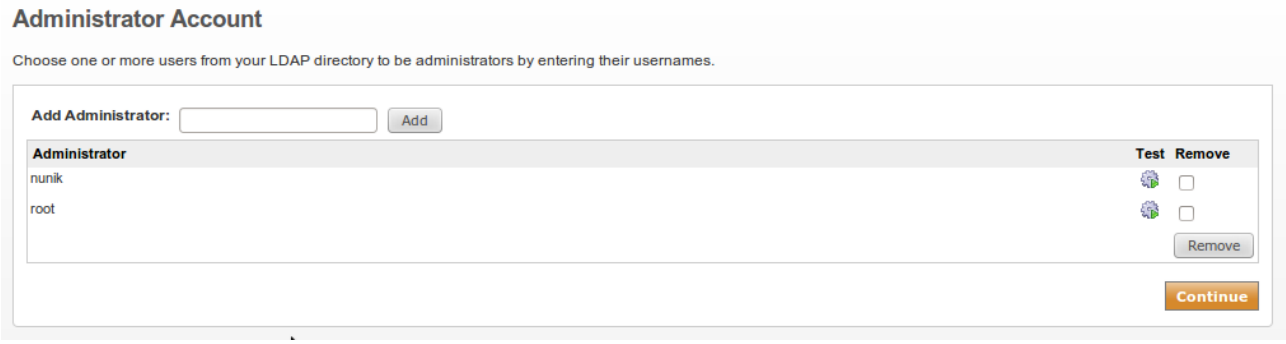
Server Type : OpenLDAP
Host : 127.0.0.1
Base DN : dc=kurusetra,dc=web,dc=id
Administrator DN : dc=admin,dc=kurusetra,dc=web,dc=id
Password : 1111

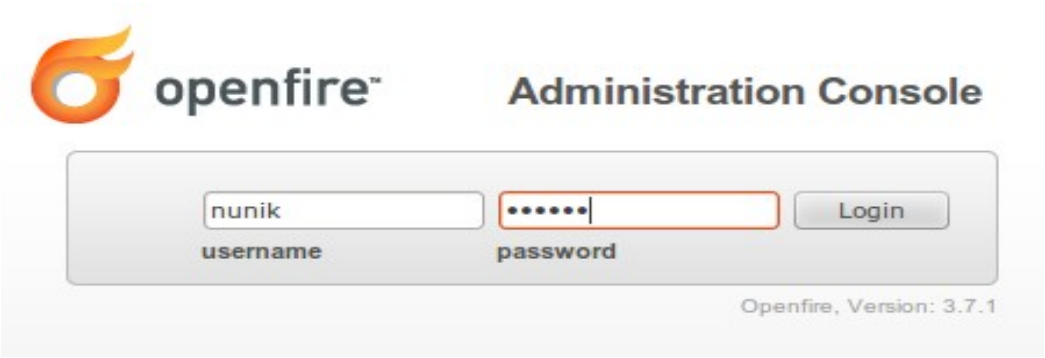


Username Field: uid [default]

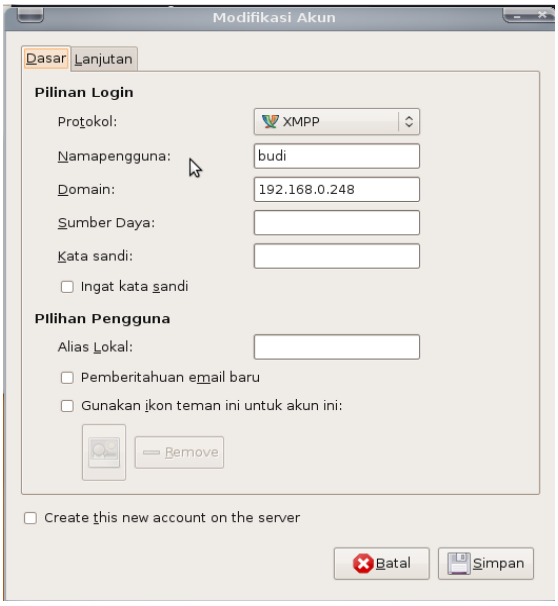


Group Field : cn
Member Field : memberUid
Description Field : description





Klien OpenFire Pidgin



Integrasi dengan Joomla CMS

Install Joomla

Instalasi Joomla seperti biasa

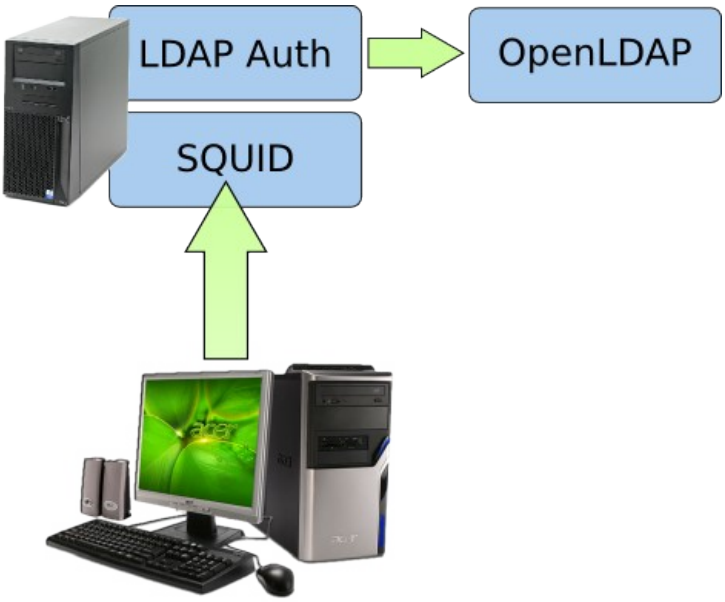
Konfigurasi Joomla

Extension -> Plugin Manager --> Authentication – LDAP

Konfigurasi Authentication LDAP

Host	: 127.0.0.1
Port	: 389
LDAP V3	: Yes
Negotiate TLS	: No
Follow Referrals	: No
Authorisation Method	: Bind Directly as User
Base DN	: dc=kurusetra,dc=web,dc=id
Search String	: uid=[search]
User's DN	: uid=[username],ou=Users,dc=kurusetra,dc=web,dc=id
Connect Username	: kosong [tidak disi]
Connect Password	: kosong [tidak disi]
Map: Fullname	: cn
Map: email	: mail
Map: User ID	: uid

Integrasi Squid Proxy Server



Pengujian openLDAP

/usr/lib/squid3/squid_ldap_auth -b 'dc=kurusetra,dc=web,dc=id' -v 3 -f 'uid=%s' 127.0.0.1
nunik 261278
OK

vim /etc/squid/squid.conf
#auth_param basic program /usr/lib/squid3/squid_ldap_auth -v 3 -b "dc=kurusetra,dc=web,dc=id" -v 3 -f "uid=%s" -h 127.0.0.1

```
auth_param basic program /usr/lib/squid3/squid_ldap_auth -b
"dc=kurusetra,dc=web,dc=id" -f "uid=%s" -h localhost
auth_param basic children 5
auth_param basic realm Masukan Username dan Password Anda!!!
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

#Recommended minimum configuration:

```
acl all src 0.0.0.0/0.0.0.0
acl password proxy_auth REQUIRED
http_access allow localhost password
```

And finally deny all other access to this proxy

```
http_access allow all password
```

OpenLDAP Self Service Password Changer

Linux Tool Box (LTB) menyediakan utilitas aplikasi untuk mengganti sendiri password OpenLDAP single sign on. Password yang dirubah unix password dan samba, secara otomatis semua server yang terintegrasi pada server OpenLDAP akan mengenali perubahan tersebut. Jadi administrator tidak perlu bingung lagi apabila pengguna ingin mengganti password sendiri. Apabila pengguna lupa ya terpaksa bermain command line interface sambaldap-passwd. Tools LTB ini cukup membantu dan konfigurasinya sangat mudah.

Self Service Password
http://ltb-project.org/wiki/download
http://tools.ltb-project.org/attachments/download/497/ltb-project-self-service-password-0.8.tar.gz

```
tar xzvf /home/budi/Unduhan/ltb-project-self-service-password-0.8.tar.gz
vim ltb-project-self-service-password-0.8/conf/config.inc.php

# LDAP
$ldap_url = "ldap://localhost";
$ldap_binddn = "cn=admin,dc=kurusetra,dc=web,dc=id";
$ldap_bindpw = "1111";
$ldap_base = "dc=kurusetra,dc=web,dc=id";
$ldap_login_attribute = "uid";
$ldap_fullname_attribute = "cn";
$ldap_filter = "(&(objectClass=person)($ldap_login_attribute={login}))";
$ad_mode = false;
$ad_options['force_unlock'] = false;
$ad_options['force_pwd_change'] = false;
$samba_mode = true;
$shadow_options['update_shadowLastChange'] = true;
$hash = "SSHA";
$who_change_password = "manager";
$use_questions = false;


ltb-project-self-service-password-0.8/ /var/www/self
chown -R www-data.www-data /var/www/self/
```

Buka Web Browser Firefox
http://127.0.0.1/self