

OpenLDAP And OpenFire

Dashamir Hoxha <dashohoxha@gmail.com>

Copyright (C) 2008 Dashamir Hoxha. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License."

Abstract: This article describes the installation, configuration and usage of OpenFire as an internal Jabber (Instant Messenger) server. User authentication is done through a centralized OpenLDAP server, so we are going to describe first how to install and configure OpenLDAP.

1. OpenLDAP

Lightweight Directory Access Protocol (LDAP) is a means of serving data on individuals, system users, network devices and systems over the network for e-mail clients, applications requiring authentication or information. We are going to use it as a central authentication system for the staff of our company.

In our company we have different applications and different systems, some of them integrated somehow with each-other, some not. The employees of the company have to login to these systems in order to perform their tasks and duties. They are authenticated with a username and password. If they use a different username and password for each system, then the situation is a bit complicated. The problems with this scenario are this:

- The employees have to remember many usernames and passwords, and this is difficult.
- If they use the same password for all of their accounts, then when they have to change it, they should change it for each application.
- It is difficult for the application managers to create and maintain all these username/passwords in all the applications.

However, if a central authentication system (like OpenLDAP, ActiveDirectory, etc.) is used, the situation becomes simple. The managers maintain all the data of the staff in a single site, and all the applications refer to it in order to check that a username and password are correct. The employees use the same username and password to access all the applications (this is called single sign-on).

1.1. Installation and Configuration

- OpenLDAP can be installed easily with this command:

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

- Modify the configuration file `/etc/openldap/slapd.conf` and comment `nis.schema` and `misc.schema` :

```
include /etc/openldap/schema/core.schema
```

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

- Modify the access control policy, so that everybody can read, but only the administrator and the person himself can modify the attributes. Also, the username and password cannot be seen by everybody. The configuration lines that are added are these:

```
### access control policy
access to dn.subtree="dc=myCompany,dc=net" attrs=uid,userPassword
    by self write
    by dn="uid=dashohoxha,ou=people,dc=myCompany,dc=net" write
    by anonymous auth
    by * none

access to dn.children="ou=people,dc=myCompany,dc=net" attrs=cn,givenName,sn,
    displayName,mail,mobile,homePhone,homePostalAddress,telephoneNumber
    by self write
    by dn="uid=dashohoxha,ou=people,dc=myCompany,dc=net" write
    by * read

access to dn.subtree="ou=people,dc=myCompany,dc=net"
    by dn="uid=dashohoxha,ou=people,dc=myCompany,dc=net" write
    by * read

access to * by * read
```

- Set also some other settings like this:

```
database bdb
suffix "dc=myCompany,dc=net"
rootdn "cn=ldapAdmin,dc=myCompany,dc=net"
rootpw {crypt}ijFYncSNctBYg

directory /var/lib/ldap

index uid,cn,surname,givenName,displayName,mail eq,pres,sub
```

rootdn is the superuser that can modify everything in the database. Indexing some attributes is used in order to make searching faster.

- Enable the service and start it:

```
chkconfig ldap on
chkconfig --list ldap
service ldap start
service ldap status
```

- Create a LDIF data file `people.ldif` with a content like this:

```
dn: dc=myCompany,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
```

dc: myCompany
organizationName: myCompany
telephoneNumber: +355 4 251212
facsimileTelephoneNumber: +355 4 251313
postalAddress: Rr. Donika Kastrioti, Nr.44
Tirana/Albania
street: Rr. Donika Kastrioti
localityName: Tirana
description: My wonderful company as much text as you want to place
in this line up to 32K

dn: cn=ldapAdmin,dc=myCompany,dc=net
objectClass: organizationalRole
cn: ldapAdmin
description: LDAP Directory Administrator

dn: ou=teams,dc=myCompany,dc=net
objectClass: organizationalUnit
ou: teams

dn: ou=people,dc=myCompany,dc=net
objectClass: organizationalUnit
ou: people

dn: ou=software,ou=teams,dc=myCompany,dc=net
objectClass: organizationalUnit
ou: software
description: The group of people that takes care about installing,
configuring, modifying and maintaining the software that is needed
for the everyday work of the company.

dn: ou=marketing,ou=teams,dc=myCompany,dc=net
objectClass: organizationalUnit
ou: marketing
description: Marketing Team

dn: ou=sales,ou=teams,dc=myCompany,dc=net
objectClass: organizationalUnit
ou: sales
description: Sales Team

.

dn: uid=dashohoxha,ou=people,dc=myCompany,dc=net
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: dashohoxha
userPassword: dashopassw
givenName: Dashamir
surname: Hoxha
cn: Dashamir Hoxha
displayName: Dasho
mail: dhoxha@myCompany.net
mail: dashohoxha@gmail.com
homePhone: 555-111-2222
mobile: 0692501878
o: myCompany
ou: software
title: Computer Engineer
telephoneNumber: 345

```
description: Leader of the software team.
```

```
. . . . .
```

- Load the LDIF file into the database:

```
ldapadd -f people.ldif -xv -D "cn=ldapAdmin,dc=myCompany,dc=net" -W
```

1.2. Install and Configure phpLDAPAdmin

phpLDAPAdmin is a web interface for managing OpenLDAP. We are going to install it on the same server that we have installed OpenLDAP. Installation and configuration of phpLDAPAdmin can be done as described in the following steps.

- Install the package *phpldapadmin* :

```
yum install phpldapadmin
```

- Add this line at `/etc/httpd/conf.d/phpldapadmin.conf` and restart apache:

```
Allow from 192.168.25.0/24
```

- Modify the configuration file `/etc/phpldapadmin/config.php` like this:

```
$ldapservers->SetValue($i, 'server', 'name', 'People');  
  
//$ldapservers->SetValue($i, 'server', 'base', array());  
$ldapservers->SetValue($i, 'server', 'base', array('ou=people,dc=myCompany,dc=net'));  
  
$ldapservers->SetValue($i, 'server', 'auth_type', 'session');  
  
$ldapservers->SetValue($i, 'login', 'attr', 'string');  
$ldapservers->SetValue($i, 'login', 'string', 'uid=<username>,ou=people,dc=myCompany,dc=net');  
  
$ldapservers->SetValue($i, 'appearance', 'show_create', false);  
  
$ldapservers->SetValue($i, 'custom', 'pages_prefix', 'prefix_');
```

- I created another connection to the LDAP server of the localhost for the teams:

```
$i++;  
$ldapservers->SetValue($i, 'server', 'name', 'Teams');  
$ldapservers->SetValue($i, 'server', 'host', '127.0.0.1');  
$ldapservers->SetValue($i, 'server', 'port', '389');  
$ldapservers->SetValue($i, 'server', 'base', array('ou=teams,dc=myCompany,dc=net'));  
#$ldapservers->SetValue($i, 'server', 'auth_type', 'cookie');  
$ldapservers->SetValue($i, 'server', 'auth_type', 'session');  
$ldapservers->SetValue($i, 'login', 'dn', '');  
$ldapservers->SetValue($i, 'login', 'pass', '');
```

```

$ldapservers->SetValue($i, 'server', 'tls', false);
$ldapservers->SetValue($i, 'server', 'low_bandwidth', false);
$ldapservers->SetValue($i, 'appearance', 'password_hash', 'md5');
# $ldapservers->SetValue($i, 'login', 'attr', 'dn');
$ldapservers->SetValue($i, 'login', 'attr', 'string');
# $ldapservers->SetValue($i, 'login', 'string', '');
$ldapservers-
>SetValue($i, 'login', 'string', 'uid=<username>,ou=people,dc=myCompany,dc=net');
$ldapservers->SetValue($i, 'login', 'class', '');
$ldapservers->SetValue($i, 'server', 'read_only', false);
$ldapservers->SetValue($i, 'appearance', 'show_create', true);
$ldapservers->SetValue($i, 'auto_number', 'enable', true);
$ldapservers->SetValue($i, 'auto_number', 'mechanism', 'search');
$ldapservers->SetValue($i, 'auto_number', 'search_base', '');
$ldapservers->SetValue($i, 'auto_number', 'min', '1000');
$ldapservers->SetValue($i, 'auto_number', 'dn', '');
$ldapservers->SetValue($i, 'auto_number', 'pass', '');
$ldapservers->SetValue($i, 'login', 'anon_bind', true);
$ldapservers->SetValue($i, 'custom', 'pages_prefix', 'prefix_');
$ldapservers->SetValue($i, 'unique_attrs', 'dn', '');
$ldapservers->SetValue($i, 'unique_attrs', 'pass', '');

```

- I created another connection to the LDAP server of the localhost (which uses the full *dn* to login, instead of *uid*, and the server base is at the root of the domain, instead of at 'ou=people,...'):

```

$i++;
$ldapservers->SetValue($i, 'server', 'name', 'LDAP Server');
$ldapservers->SetValue($i, 'server', 'host', '127.0.0.1');
$ldapservers->SetValue($i, 'server', 'port', '389');
$ldapservers->SetValue($i, 'server', 'base', array('dc=myCompany,dc=net'));
# $ldapservers->SetValue($i, 'server', 'auth_type', 'cookie');
$ldapservers->SetValue($i, 'server', 'auth_type', 'session');
$ldapservers->SetValue($i, 'login', 'dn', '');
$ldapservers->SetValue($i, 'login', 'pass', '');
$ldapservers->SetValue($i, 'server', 'tls', false);
$ldapservers->SetValue($i, 'server', 'low_bandwidth', false);
$ldapservers->SetValue($i, 'appearance', 'password_hash', 'md5');
$ldapservers->SetValue($i, 'login', 'attr', 'dn');
$ldapservers->SetValue($i, 'login', 'string', '');
$ldapservers->SetValue($i, 'login', 'class', '');
$ldapservers->SetValue($i, 'server', 'read_only', false);
$ldapservers->SetValue($i, 'appearance', 'show_create', true);
$ldapservers->SetValue($i, 'auto_number', 'enable', true);
$ldapservers->SetValue($i, 'auto_number', 'mechanism', 'search');
$ldapservers->SetValue($i, 'auto_number', 'search_base', '');
$ldapservers->SetValue($i, 'auto_number', 'min', '1000');
$ldapservers->SetValue($i, 'auto_number', 'dn', '');
$ldapservers->SetValue($i, 'auto_number', 'pass', '');
$ldapservers->SetValue($i, 'login', 'anon_bind', true);
$ldapservers->SetValue($i, 'custom', 'pages_prefix', 'custom_');
$ldapservers->SetValue($i, 'unique_attrs', 'dn', '');
$ldapservers->SetValue($i, 'unique_attrs', 'pass', '');

```

- Set some user friendly names for the attributes:

```

$friendly_attrs = array(
    'uid'                => 'Username',
    'userPassword'      => 'Password',
    'givenName'         => 'Firstname',

```

```

'sn'           => 'Lastname',
'cn'           => 'Fullname',
'displayName' => 'Nickname',
'jpegPhoto'   => 'Photo (jpg)',
'photo'       => 'Photo',
'mail'        => 'Email',
'mobile'      => 'Mobile',
'homePhone'   => 'Home Phone',
'homePostalAddress' => 'Home Address',
'description' => 'Description',
'o'           => 'Organization',
'ou'          => 'Team',
'title'       => 'Title',
'telephoneNumber' => 'Phone',
'facsimileTelephoneNumber' => 'Fax',
'postalAddress' => 'Address',
'street'      => 'Street',
'l'           => 'City',
'st'          => 'State/Province',
'c'           => 'Country',
'owner'       => 'Leader',
'member'      => 'Member'

```

```
);
```

- Set the order that the attributes are displayed:

```

$attrs_display_order = array(
    'uid',
    'userPassword',
    'givenName',
    'sn',
    'cn',
    'displayName',
    'jpegPhoto',
    'photo',
    'mail',
    'mobile',
    'homePhone',
    'homePostalAddress',
    'description',
    'o',
    'ou',
    'title',
    'telephoneNumber',
    'facsimileTelephoneNumber',
    'postalAddress',
    'street',
    'l',
    'st',
    'c',
    'owner',
    'member'

```

```
);
```

- Set some hidden and read-only attributes, etc.:

```
$hidden_attrs = array( 'jpegPhoto', 'objectClass' );
```

```
$read_only_attrs = array('objectClass', 'o', 'ou', 'title');
$unique_attrs = array('uid', 'mail');
```

- Configure predefined queries:

```
/* To make searching easier, you may setup predefined queries below: */
$q=0;
$queries = array();

/* The name that will appear in the simple search form */
$queries[$q]['name'] = 'People List';

/* The base to search on */
$queries[$q]['base'] = 'ou=people,dc=myCompany,dc=net';

/* The search scope (sub, base, one) */
$queries[$q]['scope'] = 'sub';

/* The LDAP filter to use */
$queries[$q]['filter'] = '(&(objectClass=inetOrgPerson)(uid=*))';

/* The attributes to return */
$queries[$q]['attributes'] = 'uid, cn, mail, mobile, homePhone,
telephoneNumber';

$q++;
$queries[$q]['name'] = 'Teams';
$queries[$q]['base'] = 'ou=teams,dc=myCompany,dc=net';
$queries[$q]['scope'] = 'sub';
$queries[$q]['filter'] = '(&(objectClass=organizationalUnit)(ou=*))';
$queries[$q]['attributes'] = 'ou, description';
```

1.3. Custom phpLDAPAdmin Templates

In the directory `/usr/share/phpldapadmin/templates` I created a subdirectory and moved there all `*.xml` files. Then I created the files

- `prefix_team.xml`

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE template SYSTEM "template.dtd">
<template>
<title>Team</title>
<regexp>^ou=teams</regexp>
<icon>images/uniquegroup.png</icon>
<description>Create a New Team</description>
<askcontainer>0</askcontainer>
<rdn>cn</rdn>
<visible>1</visible>

<objectClasses>
  <objectClass id="groupOfNames"></objectClass>
</objectClasses>

<attributes>
<attribute id="cn">
```

```

        <display>Name</display>
        <order>1</order>
    </attribute>
    <attribute id="description">
        <display>Description</display>
        <order>2</order>
    </attribute>
    <attribute id="owner">
        <display>Leader</display>
        <value>uid=</value>
        <icon>images/uid.png</icon>
        <onchange>autoFill:member,%owner%</onchange>
        <order>3</order>
    </attribute>
    <attribute id="member">
        <display>Member</display>
        <value>uid=</value>
        <hidden>1</hidden>
    </attribute>
</attributes>
</template>

```

● prefix_person.xml

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE template SYSTEM "template.dtd">
<template>
<title> User Account</title>
<regexp>^ou=people</regexp>
<icon>images/user.png</icon>
<description>Create a New User Account</description>
<askcontainer>0</askcontainer>
<rdn>uid</rdn>
<visible>1</visible>

<objectClasses>
<objectClass id="top"></objectClass>
<objectClass id="person"></objectClass>
<objectClass id="organizationalPerson"></objectClass>
<objectClass id="inetOrgPerson"></objectClass>
</objectClasses>

<attributes>
<attribute id="uid">
    <display>User ID</display>
    <onchange>autoFill:displayName,%uid%</onchange>
    <onchange>autoFill:mail,%uid%@myCompany.net</onchange>
    <order>1</order>
</attribute>
<attribute id="userPassword">
    <display>Password</display>
    <helper>
        <default>md5</default>
        <display>Encryption</display>
        <id>enc</id>
        <location>side</location>
        <value>blowfish</value>
        <value>clear</value>
        <value>crypt</value>
        <value>ext_des</value>
    </helper>

```

```
        <value>md5</value>
        <value>md5crypt</value>
        <value>sha</value>
        <value>smd5</value>
        <value>ssha</value>
    </helper>
    <icon>images/lock.png</icon>
    <post>=php.Password(%enc%,%userPassword%)</post>
    <spacer>1</spacer>
    <type>password</type>
    <verify>1</verify>
    <order>2</order>
</attribute>
<attribute id="givenName">
    <display>First name</display>
    <icon>images/uid.png</icon>
    <onchange>autoFill:cn,%givenName% %sn%</onchange>
    <order>3</order>
</attribute>
<attribute id="sn">
    <display>Last name</display>
    <onchange>autoFill:cn,%givenName% %sn%</onchange>
    <order>4</order>
</attribute>
<attribute id="cn">
    <display>Common Name</display>
    <order>5</order>
</attribute>
<attribute id="displayName">
    <display>Display Name</display>
    <spacer>1</spacer>
    <order>6</order>
</attribute>
<attribute id="mail">
    <display>Email</display>
    <order>7</order>
</attribute>
<attribute id="homePhone">
    <display>Home Phone</display>
    <value>0123</value>
    <order>8</order>
</attribute>
<attribute id="mobile">
    <display>Mobile</display>
    <value>0123</value>
    <spacer>1</spacer>
    <order>9</order>
</attribute>
<attribute id="o">
    <display>Organization</display>
    <value>myCompany</value>
    <hidden>1</hidden>
    <order>10</order>
</attribute>
<attribute id="ou">
    <display>Team</display>
    <value>...</value>
    <order>11</order>
</attribute>
<attribute id="title">
    <display>Title</display>
    <value>...</value>
```

```
        <order>12</order>
    </attribute>
    <attribute id="telephoneNumber">
        <display>Phone</display>
        <value>0123</value>
        <order>13</order>
    </attribute>
    <attribute id="description">
        <display>Description</display>
        <value>...</value>
        <order>14</order>
    </attribute>
</attributes>
</template>
```

These customized templates allow to create easily new users and teams.

1.4. Configure E-Mail Clients

Configuring the e-mail client to utilize an LDAP server will allow the address book of the client to access the searchable LDAP database. The results of the search are then directly admitted into the address book for use by the e-mail client. The e-mail client configuration includes:

- Specifying the name of the LDAP server: *prog.myCompany.net*
- Specifying the base identifier from which all searches are to take place:
ou=people,dc=myCompany,dc=net .

For more detailed instructions about the configuration of different email clients see:

- <http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP.html>
- <http://www.uab.edu/it/question-answer/ldap/outlook/index.html>
- <http://www.megawebhost.com/LDAP/LdapClientConfiguration.html>

1.5. Referencies

- [OpenLDAP Software 2.4 Administrator's Guide](#)
- [YoLinux LDAP Tutorial: Deploying OpenLDAP](#)
- [YoLinux LDAP Tutorial: OpenLDAP Password Protection, security and Authentication](#)
- [LDAP for Rocket Scientists](#)
- [How to allow a logged in user to modify only his attributes](#)
- [Creating Templates](#)

- <http://phpldapadmin.sourceforge.net/>
- [How do I configure LDAP Directory Services in Outlook XP?](#)
- [LDAP E-Mail Client Configuration](#)

2. OpenFire

OpenFire is an IM server (a server for communication by Instant Messages, called also Jabber server). It does the same thing that is done by MSN messenger, Yahoo Messenger, Google Messenger, etc. The advantages of using it instead of using any public messengers are these:

- The traffic of messages is only on the local network, so it is faster and does not overload the Internet connection.
- Since the traffic is local, it is more secure! The messages of our staff do not have to go up to the satellite, fly to the US and come back again to the office in the next door, with the possibility of being sniffed by everybody!
- Since we install and manage the server ourselves, we can customize its settings so that they fit best our needs.
- After all it is fun doing it ourselves, and it turns out to be not so difficult.

Some configurations that we would like to customize so that they fit our requirements are these:

- For each team (department) there is going to be a chat room, which is managed by the leaders of the team.
- Usually only the members of the team are allowed to enter the team's chat room, however the managers can register other people if needed.
- The managers can enter any chat room.
- All the conversation in chat rooms and pear-to-pear is logged.
- When a user is offline for a while, once he gets online, the server will send him any missed messages and also all the conversation in the chat rooms that he has missed.

2.1. Installation

- Download `openfire-3.4.5-1.i386.rpm` from <http://www.igniterealtime.org/downloads/index.jsp> and install it with:

```
yum --nogpgcheck install openfire-3.4.5-1.i386.rpm
```

- Create the MySQL database for openfire:

```
mysql -u root -p
```

```
mysql> create database openfire;  
mysql> grant all on openfire.* to 'openfireuser'@'localhost' identified by  
'openfirepassw';  
mysql> quit
```

```
mysql -u root -p -D openfire <  
/opt/openfire/resources/database/openfire_mysql.sql
```

- Open in firewall the ports that are needed for the messenger service. Edit `/etc/sysconfig/iptables` and add these lines:

```
# client port  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5222 -j ACCEPT  
# (old) ssl client port  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5223 -j ACCEPT  
# server to server  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5269 -j ACCEPT  
# external component  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5275 -j ACCEPT  
# connection manager  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5262 -j ACCEPT  
# http client connection  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT  
# https client connection  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8483 -j ACCEPT  
# admin console  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 9090 -j ACCEPT  
# https admin console  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 9091 -j ACCEPT  
# file transfer proxy  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 7777 -j ACCEPT  
# real time media proxy  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000:20000 -j  
ACCEPT  
# STUN service  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3478 -j ACCEPT  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3479 -j ACCEPT  
# flash cross domain  
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 5229 -j ACCEPT
```

Then restart the firewall:

```
service iptables restart
```

- Start the service *openfire* :

```
chkconfig openfire on  
chkconfig --list openfire  
  
service openfire start  
service openfire status
```

2.2. Setup

- Open in browser the web-based setup wizard at `http://prog.myCompany.net:9090/` .
- Select a *Standard Database Connection* , then select MySQL and set the database URL to `jdbc:mysql://localhost:3306/openfire` . Set username and password of the database as `openfireuser` and `openfirepassw` .
- At *Profile Settings* select *Directory Server (LDAP)* and then:

- Fill the connection settings like this:

```
Server Type      : OpenLDAP
Host             : prog.myCompany.net
Port            : 389
Base DN         : ou=people,dc=myCompany,dc=net
Administrator DN : cn=ldapAdmin,dc=myCompany,dc=net
Password        :
```

- Set *User Mapping* and *User Profiles (vCard)* like this:

```
Username Field : uid
```

```
(check) Store avatar in database if not provided by LDAP
```

```
Name           : {cn}
Email          : {mail}
Full Name      : {cn}
Nickname       : {uid}
Photo/Avatar   : {jpegPhoto}
Street Address : {homePostalAddress}
Phone Number   : {homePhone}
Job Title      : {title}
Department     : {ou}
Phone Number   : {telephoneNumber}
Mobile Number  : {mobile}
Pager         : {pager}
```

- Set *Group Mapping* options like this:

```
Group Mapping
Group Field      : cn
Member Field     : member
Description Field : description
```

```
Advanced Setting
Posix Mode      : Yes
Group Filter    : (member=*)
```

Note: If openfire was configured without LDAP integration, setup can be started again like this: first edit `/opt/openfire/conf/openfire.xml` and modify the content of `<setup>` to be false, then restart openfire (**service openfire restart**) and

start again the setup wizard at <http://prog.myCompany.net:9090/> .

- After adding also one or more admin users, the setup is finished. Now we can open <http://prog.myCompany.net:9090/> or <https://prog.myCompany.net:9091/> and login as admin.

2.3. Configuration

Open <https://prog.myCompany.net:9091/> and login with an admin username and password. Then do the following configurations:

- Go to *Plugins / Available Plugins* and install all the open source plugins that are available.
- Go to *Server / Server Settings / Resource Policy* . Set *Assign kick value*: 2.
- *Server / Server Settings / Offline Messages* : Store, Store or Bounce. 1000.00KB
- *Server / Server Settings / Message Audit Policy* : Disable
- *Server / Server Settings / Private Data Storage* : Enable
- *Server / Server Settings / File Transfer Settings* : Enabled, port: 7777
- *Server / Server Settings / Content Filter* : Disabled
- *Server / Server Settings / Presence Service* : Anyone
- *Server / Server Settings / Search Service Properties*: Enabled (Username, Name, Email)
- *Server / Server Settings / Subscription Properties*: Accept / Local
- *Server / Server Settings / User Service* : Disabled
- *Server / Gateways / Settings* : Check IRC, MSN Messenger and Yahoo! Messenger ; at Permissions check 'All users can register'.
- *Group Chat / Group Chat Setting / Service Properties* : set the service name as 'chat'. Then restart the server: **service openfire restart** .
- *Group Chat / Group Chat Setting / History Settings* : select Show Entire Chat History .
- *Group Chat / Group Chat Setting / Administrators* : add some users as administrators of the group chats, like dhoxha@prog.myCompany.net, ekonomi@prog.myCompany.net, anurja@prog.myCompany.net, etc.
- *Group Chat / Group Chat Setting / Room Creation Permissions* : select 'Only specific users can create a chat room', then add some users that are allowed to create chatrooms: dhoxha@prog.myCompany.net, anurja@prog.myCompany.net, ekonomi@prog.myCompany.net, etc.

- *Group Chat / Group Chat Setting / Other Settings* : select Never kick idle users.
- *Group Chat / Room Administration / Create New Room* : check the room options List Room in Directory, Make Room Moderated, Make Room Members-only, Allow Users to register with the room, Log Room Conversations .

2.4. Creating ChatRooms from Clients

Chatrooms can also be created from the clients. I will describe how to do this from Pidgin and Gajim:

● Pidgin

- Choose *Menu Boddies* → + *Add Chat...* In the dialog window that is opened set:
 - Room: test-01 (name of the chatroom)
 - Server: chat.prog.myCompany.net
 - Check *Autojoin when account becomes online* .
 - Check *Hide chat when the window is closed* .

Up to now we have just registered a chatroom in our contact list. Using the button Room List we could have seen the list of the existing rooms in server. This chatroom is now in our contact list.

- Double-click the chatroom at the contact list. Since this is a new chatroom that didn't exist before, it is created (in the server) at the moment that we open it. Of course, this works only for the users that have the right to create chatrooms. At the moment that it is created, it also offers the possibility to configure it, or we can accept the default configuration values.
- We choose to configure it, and let's make the configuration more or less like this:
 - Check the options: *List Room in Directory* , *Room is Persistent* , *Room is Moderated* , *Room is Members-only*
 - Check also these options: *Log Room Conversations* , *Only login with registered nickname* , and uncheck the option: *Allow Ocupants to change nickname* .
 - Add also any Admin or Owner, and leave the rest to their default values.
- After the chatroom window is opened, we can register other people in it by opening: *Conversation* → *Invite...* .

● Gajim

- Select the menu *Actions* → *Group Chat* → *Join New Group Chat* in the window that is opened set Room: test-02@chat.prog.myCompany.net and check *Join this room automatically*

when I connect .

- Actually, such a chatroom does not exist, so it is created in the server at the moment that Gajim opens its configuration window. Creating a chatroom like this works only for those users that have the right to create new chatrooms.
- In the configuration window, set the options more or less the same as for Pidgin. In addition, we can also enter here the bodies who are allowed to enter the chatroom (the Member List).
- In the chatroom window, we can also open the room configuration window at *Actions* → *Configure Room*, where we can also add new members, etc.

2.5. Chat Clients

Any jabber clients can be used. Most of them are free and most of them work both in windows and in linux. A list of such clients can be found at <http://www.jabber.org/clients> and http://en.wikipedia.org/wiki/List_of_Jabber_client_software .

I have used two of them, [Pidgin](#) and [Gajim](#) . Connecting to the server and entering chatrooms can be done like this:

● Pidgin

- To add a new account, open *Accounts* → *Manage* and then press the button + Add
- At the dialog window that is opened, fill the values like this:

```
Protocol      : XMPP
Screen Name   : username (your username at LDAP)
Domain        : prog.myCompany.net
Password      : (your password at LDAP)
Remember password (check if you like)
Create this new account on the server (don't check, because accounts
are retrieved from LDAP and it is not possible to create new accounts).
```

At Advanced can be also filled (optionally) *File transfer proxies: prog.myCompany.net:7777*

- As soon as you are online, you will get an invitation for chat, if you are registered in a chatroom.
- If you don't get such an invitation, then try to join yourself a chatroom. Select the menu *Buddies* → *+ Add Chat...* In the dialog window that is opened set:

```
Room      : tech-support (name of the chatroom)
Server    : chat.prog.myCompany.net
Check Autojoin when account becomes online.
Check Hide chat when the window is closed.
```

So, we just registered a chatroom in our contact list. Now can double-click and open it. At Room List we could have seen also a list of the existing chatrooms in the server.

- In case that you are not allowed to enter the chatroom, then you should contact its administrator, so that he can add you as a member.

- Gajim

- To add a new account in the program, select the menu *Edit* → *Accounts* then press the button *New*
- Choose *I already have an account I want to use* and in the following window give the username, server and password. Username and password are the ones that are registered in LDAP, and the server is 'prog.myCompany.net' .
- After the account is created, change its status to *Available* , in order to be online. As soon as you are online, you may get an invitation for joining the chatroom *tech-support@prog.myCompany.net* . Accept it and check also 'Join this room automatically when I connect'. You will enter the chatroom, where you will be able to communicate with the other members.
- In case that you don't get any invitation, then try to join the chatroom yourself. Select the menu *Actions* → *Group Chat* → *Join New Group Chat* . In the dialog window set *Room: tech-support@chat.prog.myCompany.net* and check *Join this room automatically when I connect*. In case that you are not allowed to join it, then contact the chatroom administrator, so that he can add you as a member.

2.6. Connecting to MSN and Yahoo Messengers

Both of the clients, Pidgin and Gajim can be used to communicate with the messenger networks of MSN and Yahoo!, using our messenger server as a gateway. For example, to connect to Yahoo! they can be configured like this (it is the same for MSN):

- Pidgin: Select the menu *Accounts* → *Manage* and click the button + *Add*. In the following window set as protocol *Yahoo!*, then put your Yahoo! username and password. We can also check *Remember password* and *New mail notification* . Then, from the menu *Accounts* → *Enable Account* we can activate/disactivate one or the other, or both of them.
- Gajim: Select the menu *Actions* → *Discover Services*. Then select *Yahoo! Transport yahoo.prog.myCompany.net* and then click the button *Register*. Then give the username and password that you use at Yahoo!, etc.

3. GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

1. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

2. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs

or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ascii without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

3. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

4. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all

words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

5. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

7. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

8. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

9. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided

that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

10. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

11. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

3.1. ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C) year your name.  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License, Version 1.2  
or any later version published by the Free Software Foundation;  
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover  
Texts. A copy of the license is included in the section entitled ``GNU  
Free Documentation License''.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being list their titles, with  
the Front-Cover Texts being list, and with the Back-Cover Texts  
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two

alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.