Egroupware server with LDAP backend

*Posted by **sphaero** on Wed 17 Oct 2007 at 10:26*
*Tags: **egroupware**, **ldap**, **pam**, **php**, **samba***

Egroupware is a webbased groupware suite with an impressive list of features. Egroupware uses a Mysql backend to store all it's data but the latest release makes it easy to store useraccounts in an LDAP tree. This documents describes how to install the latest version while using an LDAP backend for useraccounts. Egroupware can then manage the unix loginaccounts as well as samba login accounts.

Before you start

You need to have a base install of Debian Etch running. I'm writing this document using a clean install of Debian Etch with no extra packages installed. You need to be familiar with Debian and working with the shell editing configuration files, etc. The following steps in this document should setup a working system. We need to think of a few passwords, let me list these:

- 'yoursecretldappassword' is used for the admin user who can edit the ldap tree
- 'yoursecretmysqlrootpassword' is used for the root user who manages mysql
- 'yoursecretegroupwaremysqlpassword' is for the egroupware mysql user who manages the egroupware database
- 'yoursecretheaderadminpassword' is used for the header admin user who configures the egroupware environment
- yoursecretconfigpassword' is used for egroupware configuration which manages the egroupware configuration

Installing packages

First setup an SSH server so you can work from a remote machine. It's probably easier.

```
apt-get install openssh-server
```

Install all needed packages:

```
apt-get install apache2 php5 php5-mysql php5-imap php5-ldap php5-mcrypt
```

You'll need to answer at least the following questions, perhaps even more:

- Configuring slapd: Admin password enter: 'yoursecretldappassword'. //This admin user is used to manage the ldap tree//
- Samba Server: Workgroup/Domain Name: enter you workgroup name.
- Configuring libnss-ldap: LDAP server Uniform Resource Identifier: **ldap://127.0.0.1**
- Configuring libnss-ldap: Distinguished name of the search base: dc=example,dc=net
- Configuring libnss-ldap: LDAP version to use: 3
- Configuring libnss-ldap: LDAP account for root: cn=admin,dc=example,dc=net
- Configuring libnss-ldap: LDAP root account password: enter 'yoursecretldappassword'
- Configuring libpam-ldap: Make local root Database admin. //This is up to you, for now say 'no'//

- Configuring libpam-ldap: Does the LDAP database require login?: no

Post-installation configuration

Ok, we've installed and done a little configuration of the required packages. We need to tune these in order for our setup to work.

Setup LDAP

First let's check if the ldap tree was build successfully. Run the following command and check if the output corresponds:

```
server:~# slapcat
dn: dc=example,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: example.net
dc: example
structuralObjectClass: organization
entryUUID: 7573ad44-df47-102b-9824-95946d13a46c
creatorsName:
modifiersName:
createTimestamp: 20070815064947Z
modifyTimestamp: 20070815064947Z
entryCSN: 20070815064947Z#000000#00#000000

dn: cn=admin,dc=example,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fTQ0Z1FIZ0VteTJGRk0=
structuralObjectClass: organizationalRole
entryUUID: 75748c96-df47-102b-9825-95946d13a46c
creatorsName:
modifiersName:
createTimestamp: 20070815064947Z
modifyTimestamp: 20070815064947Z
entryCSN: 20070815064947Z#000001#00#000000
```

As you can see from this output we have one domain called dc=example,dc=net and in this domain we have one special admin user 'cn=admin,dc=example,dc=net' which is there to manage the ldap tree. ((This is not a regular user)). There should be nothing else in the ldap tree.

Egroupware can manage your samba accounts as well but in order to support samba accounts in the ldap tree we need to add a schema to the ldap server. Run the following command to copy the schema to the right place.

```
zcat /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > /etc/ldap/
```

Then edit the /etc/ldap/slapd.conf file and make schema section look like this:

```
# Schema and objectClass definitions
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
```

Now restart the ldap server:

```
/etc/init.d/slapd restart
```

Egroupware will not setup our ldap tree for us so we need to prepare it before hand. We will create 3 'Organizational Units'. It's just a sub-tree of our main ldap tree basically. We'll create 'people', 'groups' and 'machines'. Open your text editor and enter the following text and safe the file as 'ous.ldif':

```
dn: ou=people,dc=example,dc=net
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=example,dc=net
objectClass: organizationalUnit
ou: groups

dn: ou=machines,dc=example,dc=net
objectClass: organizationalUnit
ou: machines
```

Now run the following command to create the OUs in the ldap tree. The command will ask you for your ldap admin password. Enter 'yoursecretldappassword' here:

```
ldapadd -W -x -v -D cn=admin,dc=example,dc=net < ous.ldif
```

The command should complete successfully. You can use the slapcat command again to see if the OUs really did get created. We've finished setting up the ldap tree. We can now focus on setting up the environment for Egroupware.

Egroupware Environment

PHP

Egroupware needs some php tweaking. First install PEAR::Auth_SASL by running:

```
pear install Auth_SASL
```

Find and change the following lines in /etc/php5/apache2/php.ini

```
mbstring.func_overload = 7
memory_limit = 24M
```

That's it. Reload apache:

```
/etc/init.d/apache2 force-reload
```

MySQL

As normal you should set a root password for the MySQL database:

```
mysqladmin -u root password 'yoursecretmysqlrootpassword'
```

You'll need to enter 'yoursecretmysqlrootpassword' for the next 2 mysql commands. Now create a database for Egroupware:

```
mysql -u root -p -e "CREATE DATABASE egroupware"
```

And set privileges for this database

```
mysql -u root -p -e "GRANT ALL ON egroupware.* TO egroupware@localhost I
```

Installing Egroupware

Since the egroupware package in Etch is already a bit outdated we'll install the latest release using Subversion. Just 'cd' to /var/www and run the following command:

```
cd /var/www
svn checkout http://svn.egroupware.org/egroupware/branches/1.4/aliases/d
```

This will download the latest stable release from the repository of the Egroupware project. It can take a while depending on your setup. The good thing about subversion is you can use the same command to update egroupware as well.

After the download completes fire up your browser to start the Egroupware setup:

```
http://your.ipaddress/egroupware/setup
```

Run the 'installation tests' and make sure no red crosses are shown. Although the setup tests show that 'magic_quotes_gpc = Off' it is actually on. So why this shows up as an error I don't know. Just ignore this. The other warnings you can safely ignore as well. Continue to the Header Admin.

Header Admin setup

This is where you setup your Egroupware environment. It is quite straightforward and explained very well. Leave the defaults as they are but fill in the password fields:

- Header Password: enter 'yoursecretheaderadminpassword'
- DB Password: enter 'yoursecretegroupwaremysqlpassword'
- Configuration Password: enter 'yoursecretconfigpassword'

Since the setup can't create the header.inc.php file we need to create it ourselves. Press the 'view' button at the end of the page and copy the contents into your texteditor. Save the file as: '/var/www/egroupware/header.inc.php' and set permissions on it because it contains some sensitive information.

```
chmod 640 /var/www/egroupware/header.inc.php
chown :www-data /var/www/egroupware/header.inc.php
```

When you continue you'll be presented with 2 login screens.

Egroupware config

Login in the Setup/Config Admin Login with username admin and password 'yoursecretconfigpassword' After login you are presented with the 'Setup - Domain: default(mysql)' with all red crosses. Just press the 'install' button to install all applications.

I got one error about 'sitemgr-link NOT installed, you need to copy it from egroupware/sitemgr/sitemgr-link to egroupware/sitemgr-link and install it manually !!!' but I ignore this. I suggest you do the same if you get this error. Now press 'Re-Check My installation'. Now you'll see a few less red crosses. The setup says we're missing some directories. Let's create them right away and set permissions.

```
mkdir -p /var/lib/egroupware/default/files /var/lib/egroupware/default/t
chown -R www-data /var/lib/egroupware/default/
```

Now press the 'Edit Current Configuration'. We'll need to answer a few more questions. Just leave all the defaults as they are but fill in the following:

- POP/IMAP mail server hostname or IP address: imap.your.provider or 127.0.0.1
- SMTP server hostname or IP address: 'smtp.your.provider' or '127.0.0.1'
- Select which type of authentication you are using: LDAP
- Select where you want to store/retrieve user accounts: LDAP
- Minimum account id (e.g. 500 or 100, etc.): 10000
- Maximum account id (e.g. 65535 or 1000000): 20000
- LDAP host: 127.0.0.1
- LDAP accounts context: ou=people,dc=example,dc=net
- LDAP groups context: ou=groups,dc=example,dc=net
- LDAP rootdn: cn=admin,dc=example,dc=net
- LDAP root password: 'yoursecretldappassword'
- LDAP encryption type: md5
- Do you want to manage homedirectory and loginshell attributes?: Yes
- LDAP Default homedirectory prefix: /home
- LDAP Default shell: /bin/bash

Now press save. If everything went well you'll be brought back to the Setup - Domain. Let's finish the installation by creating the admin account. Press 'Create admin account'. Fill in

some suitable settings. Don't leave any setting empty! Create the demo accounts as well. The demo accounts are handy for testing. You'll need to delete them later. Press 'Save' If everything went OK you'll be presented with no more red crosses. Press 'Back to user login' and login with one of the accounts. It should work. Login with the admin account to control Egroupware.

Setup shell accounts

We've setup the Egroupware application which created some demo accounts. In order to use these account for shell access as well we need to configure PAM. I'm not going to cover an in depth configuration of PAM and LDAP. Instead I present you with a script which will do this for you. Open your text editor and copy the following:

```
#!/bin/sh
# This script configures pam for ldap support.
#

cat < /etc/pam.d/common-account
#
# /etc/pam.d/common-account - authorization settings common to all servi
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system.  The default is to
# only deny service to users whose accounts are expired in /etc/shadow.
#
account [success=1 default=ignore] pam_unix.so
account required pam_ldap.so use_first_pass
account required pam_permit.so
EOF

cat < /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all service
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
auth [success=1 default=ignore] pam_unix.so nullok_secure
auth required pam_ldap.so use_first_pass
auth required pam_permit.so
EOF

cat < /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all se
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define  the services to be
# used to change user passwords.  The default is pam_unix

# The "nullok" option allows users to change an empty password, else
# empty passwords are treated as locked accounts.
#
# (Add md5 after the module name to enable MD5 passwords)
#
# The "obscure" option replaces the old OBSCURE_CHECKS_ENAB option in
# login.defs. Also the "min" and "max" options enforce the length of the
# new password.

password [success=1 default=ignore] pam_unix.so nullok obscure min=4 max
password required pam_ldap.so use_first_pass
password required pam_permit.so
EOF

cat < /etc/pam.d/common-session
#
# /etc/pam.d/common-session - session-related modules common to all serv
#
# This file is included from other service-specific PAM config files,
```

Save this file as pamldap-setup.sh and make it executable. Just run the file and you're setup:

```
chmod +x pamldap-setup.sh
./pamldap-setup.sh
```

Restart the nscd daemon before trying to login with the demo users, though:

```
/etc/init.d/nscd restart
```

If you want home directories created automatically for your users see the following document: **http://www.debian-administration.org/articles/403**

Setup Samba

Open /etc/samba/smb.conf with your text editor and add the following entries:

```
#Comment the original passdb backend = tdbsam!!!
passdb backend = ldapsam
ldap ssl = Off
ldap suffix = dc=example,dc=net
ldap machine suffix = ou=machines
ldap user suffix = ou=people
ldap group suffix = ou=groups
ldap admin dn = cn=admin,dc=example,dc=net
ldap passwd sync = Yes
```

This configuration is based on the default Etch configuration. If you have a different configuration for samba there might be more settings involved but that's beyond the scope of this document. Samba needs to know the password for the admin user to connect to the ldap server. Set it by running the following command:

```
smbpasswd -w 'yoursecretldappassword'
```

Egroupware needs to know the SID for your domain or workgroup. Run the following command and copy the output.

```
net getlocalsid
```

Login in as the admin user in Egroupware and go to Admin (most left icon) - Sambaadmin - site configuration. Enter the output of the previous command in 'Samba SID' field. Submit the configuration and create a test user to see if Samba is working. You can test samba by running:

```
smbclient -L \\127.0.0.1 -U 'yourtestuser'
```

The output should show a list of shares. (You need smbclient installed though).

Final thought

This is a basic setup of a server running Egroupware from which you can manage your

users. The problem I found so far is the fact the groups use gid starting from 1 which conflicts with the system groups. I've just fixed it by hand but perhaps I've overlooked something. You probably need to tweak some things or set things more secure. Hopefully comments to this article will give some usefull tips or extensions which I could add to this article.

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (128.95.xx.xx) on Wed 17 Oct 2007 at 21:10*

Isn't there anything like Red Hat's `authconfig` to make the pam changes for you? On RHEL I've done this with (all one line)

```
authconfig --enableshadow --enablemd5 --enableldap \
--enableldapauth --ldapserver=ldaps://ldap.example.com \
--ldapbasedn="dc=example,dc=com" --enableldaptls \
--enablecache --disablenis --kickstart
```

Sometimes you have to tweak /etc/ldap.conf but I've never had to edit pam files.

Re: Egroupware server with LDAP backend

*Posted by **flatfoot** (87.119.xx.xx) on Sat 20 Oct 2007 at 03:48*
*[**Send Message**]*

as there's no egroupware package for stable (Debian 4.0 Etch), one could try to port it from unstable.

1. download sources

wget **http://ftp.de.debian.org/debian/pool/main/e/egroupware/egroupware_1.4.002.dfsg.orig.tar.gz**
wget **http://ftp.de.debian.org/debian/pool/main/e/egroupware/egroupware_1.4.002.dfsg-1.diff.gz**
wget **http://ftp.de.debian.org/debian/pool/main/e/egroupware/egroupware_1.4.002.dfsg-1.dsc[/code]**

2. unpack

dpkg-source -x egroupware_1.4.002.dfsg-1.dsc

3. install build dependencies

apt-get install debhelper dpatch gawk po-debconf

4. build package

dpkg-buildpackage -us -uc

5. install

dpkg -i egroupware_1.4.002.dfsg-1_all.deb

and all it's dependencies

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (62.41.xx.xx) on Fri 2 Nov 2007 at 08:34*

or
if unstable is also in your apt list

apt-get build-dep egroupware
apt-get source -t unstable egroupware -B
dpkg -i egroupware_...deb

simple and very clean.

Louis

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (80.100.xx.xx) on Sat 20 Oct 2007 at 11:22*

I am running Ubuntu 7.10 desktop.
Can I use this document to install egroupware 1.4 to?
Furthermore I noticed that no additional mail server packages are installed, am I correct in assuming that debian-etch already has one installed?

Re: Egroupware server with LDAP backend

*Posted by **Steve** (82.32.xx.xx) on Sat 20 Oct 2007 at 19:59*
*[**Send Message** / **View Steve's Scratchpad** / **View Weblogs**]*

Debian Etch comes with Exim by default, as did Debian Sarge.

Steve

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (82.227.xx.xx) on Mon 22 Oct 2007 at 19:58*

A nice article ! Thanks !

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (99.253.xx.xx) on Sun 4 Nov 2007 at 13:49*

"The problem I found so far is the fact the groups use gid starting from 1 which conflicts with the

system groups. I've just fixed it by hand but perhaps I've overlooked something."

Hi, thanks for a nice step by step guide. A few questions, with regards to your statement above, can you detail how you "fixed" it by hand? So basically whenever egroupware adds a user and that user's group for a shell account, the gid has to be changed to the recommended debian users gid range by hand?

Also now that egroupware is taking care of shell account setups, how does one go about adding users from the command line outside of egroupware if so desired - would "adduser" be still a viable option?

Regards,

Re: Egroupware server with LDAP backend

*Posted by **sphaero** (80.100.xx.xx) on Sun 4 Nov 2007 at 15:02*
*[**Send Message** / **View Weblogs**]*

Actually I mentioned this wrong! It is fixed by setting the 'Minimum account id'.
This number will also be used for creating gid's. If you do net set this it will start from 0 which will conflict with the system users.

I don't know if you can add user from commandline. It could be you could just add users normally as you would with a ldap setup from there users should be able to login in egroupware. I don't know how you would manage unique uid's. I haven't tried this myself since I don't need it but I'm very interested in your findings.

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (212.117.xx.xx) on Fri 16 Nov 2007 at 08:26*

Nice job, but how do I use the LDAP for the addressbook ?
It works for the accounts, but I dont get it to work with the addressbook.

Thx Michel

Re: Egroupware server with LDAP backend

*Posted by **sphaero** (62.177.xx.xx) on Mon 17 Mar 2008 at 15:29*
*[**Send Message** / **View Weblogs**]*

I didn't get that to work so I switched back to Mysql for the addressbook. I'm not sure but I think for the addressbook it really needs the rfx2301bis schema.

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (80.100.xx.xx) on Wed 13 Feb 2008 at 01:49*

Sorry, I am kind of newbe.
I have Ubuntu Desktop 7.10 installed and can't get LDAP configured. I worked through this document untill creating the OUs in the LDAP tree, but when I try to ldapadd I get the errormessage:

ldap bind: invalid credentials (49)
I think that there is something wrong with the fqdn, because slapcat keeps telling me "dc=nodomain" but I just can't get it right. I checked /etc/hosts and /etc/resolv.conf but it still won't work.
Please HELP.

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (12.36.xx.xx) on Mon 17 Mar 2008 at 14:46*

I get the following errors in setup and therefore cannot setup the Admin Account:
Warning: ldap_search() [function.ldap-search]: Search: No such object in /var/www/egroupware /phpgwapi/inc/class.accounts_ldap.inc.php on line 679

Warning: ldap_get_entries(): supplied argument is not a valid ldap result resource in /var/www /egroupware/phpgwapi/inc/class.accounts_ldap.inc.php on line 681

Warning: Invalid argument supplied for foreach() in /var/www/egroupware/phpgwapi /inc/class.accounts_ldap.inc.php on line 681

Warning: ldap_search() [function.ldap-search]: Search: No such object in /var/www/egroupware /phpgwapi/inc/class.accounts_ldap.inc.php on line 706

Warning: ldap_get_entries(): supplied argument is not a valid ldap result resource in /var/www /egroupware/phpgwapi/inc/class.accounts_ldap.inc.php on line 708

Any help would be appreciated,

lyle@grovehillmemorial.org

Re: Egroupware server with LDAP backend

*Posted by **Anonymous** (84.85.xx.xx) on Mon 23 Jun 2008 at 16:22*

After i did this i get a : putty fatal error... server unexpectedly closed network connection. everything works fine ftp mysql apache2 only putty. if you telnet to the address the reply looks fine: SSH-2.0-OpenSSH_4.3p2 Debian-9. and before i going to make a 230KM trip to the hosting facility i will wait for an answer.

lemn8@motomonsters.nl

Email: **webmaster@debian-administration.org**

Article Feeds in Atom, RSS, & RDF formats