Postfix−Cyrus−Web−cyradm−HOWTO

Luc de Louw

luc@delouw.ch

Revision History

Revision 1.0.0	2002−04−07	Revised by: ldl
Initial Release		

This document guides you through the installation of the Postfix mail transportation agent (MTA), the Cyrus IMAP server. The goal is a fully functional high−performance mailsystem with user−administration with Web−cyradm, a webinterface. Data like virtualusers, aliases etc. are stored in a mysql database.

Table of Contents

Table of Contents

1. Introduction

1.1. Contributors and Contacts

First I would thank all those people who send questions and suggestions that made a further development of this document possible. It shows me, sharing knowledge is the right way. I would encourage you to send me more suggestion, just write me an email `<luc at delouw.ch>`

1.2. Why I wrote this document

There are different approaches howto set up different mailsystems. Most documents available are related to Sendmail, procmail, WU−IMAPd and friends. These fine−running software is unfortunately very un−flexible concerning user administration.

For longer time I was testing alternative MTA's like qmail, postfix and exim, IMAP/POP−servers like Cyrus, vpopmail, Courier IMAP and others.

At the end of the day, from my point of view the couple Postfix/Cyrus seems to be the most flexible and performant solution.

All these combinations of software had one in common: there was only little documentation available concerning how this software is working together with each other. For installing the software, lot of effort must be spent to get all information needed to get all software running.

1.3. Copyright Information

1.4. Disclaimer

No liability for the contents of this documents can be accepted. Use the concepts, examples and other content at your own risk. As this is a new edition of this document, there may be errors and inaccuracies, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that.

All copyrights are held by their by their respective owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.5. New Versions

This is the initial release.

New version of this document are announced on freshmeat

The latest version of this document you can get from http://www.delouw.ch/linux

- HTML.
- Postscript (ISO A4 format).
- Acrobat PDF.
- SGML Source.
- HTML gzipped tarball.

1.6. Credits

I would thank to the nice people at < `discuss at linuxdoc.org`> for supporting me in writing HOWTOs

1.7. Feedback

Feedback is most certainly welcome for this document. Without your submissions and input, this document wouldn't exist. Please send your additions, comments and criticisms to the following email address : <`luc at delouw.ch`>.

1.8. Translations

At the moment no translations are available. A german translation is planned and would be written by myself as soon as the document is valid

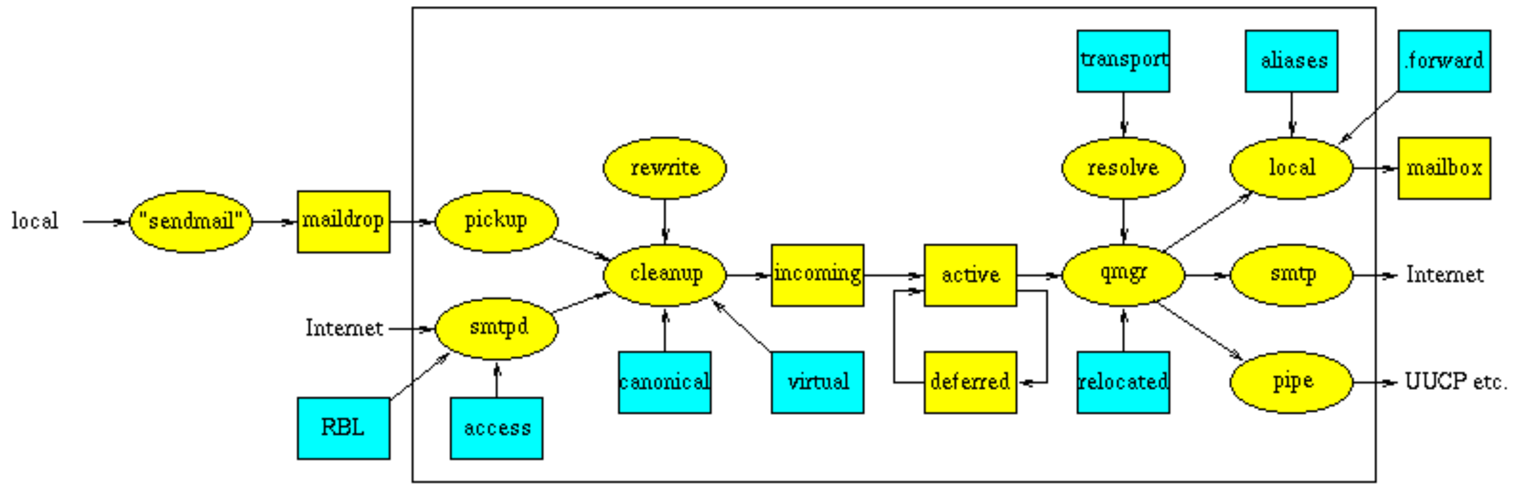
Translations to other languages are always welcome. If you translated this document, please let me know, so I can set a link here

2. Technologies

2.1. The Postfix MTA

Quoting www.postfix.org »Postfix attempts to be fast, easy to administer, and secure, while at the same time being sendmail compatible enough to not upset existing users. Thus, the outside has a sendmail−ish flavor, but the inside is completely different.«

Figure 1. Postfix − the big picture



Doesn't it look impressive? − It looks much more complicated as it is. Postfix is indeed nice to configure and handle

Unlike sendmail, postfix is not one monolithic program, it is a compilation of small programs, each of it has a specialized function. At this place I don't what to go into details with program does what. If you are interested how Postfix is working, please see the documentation at http://www.postfix.org/docs.html

In this document you will find the information what to put in the config files

---

2.2. Cyrus IMAP

The Cyrus IMAP is developed and maintained by Carnegie Mellon University.

Unlike the WU−IMAPd Cyrus is using its own method to store the users mail. The data is stored in a database, this makes Cyrus so performant. Especially with lots of users and/or lot of big emails, there is nothing such fast as the Cyrus IMAP−server.

Another very important feature is, you don't need a local Un*x user for each account. All users are authenticated by the IMAP−Server. This makes it a great solution for really huge base of users.

User administration is done by special IMAP−commands. This allows you to eighter use the commandline interface, or use one of the available Webinterfaces. This Method is much more secure than a Webinterface to `/etc/passwd`!

Since CMU changed the license policy for Cyrus, this software is going to be used by much more users

2.3. MySQL Database

MySQL is a very fast, powerful and very nice to handle Database.

Since Cyrus can authenticate its users with pam, you can use pam_mysql as a connector to the Userdatebase stored in MySQL. This allows you to create a nice Webinterface for your users for changing passwords, define and delete aliases and more.

2.4. pam_mysql

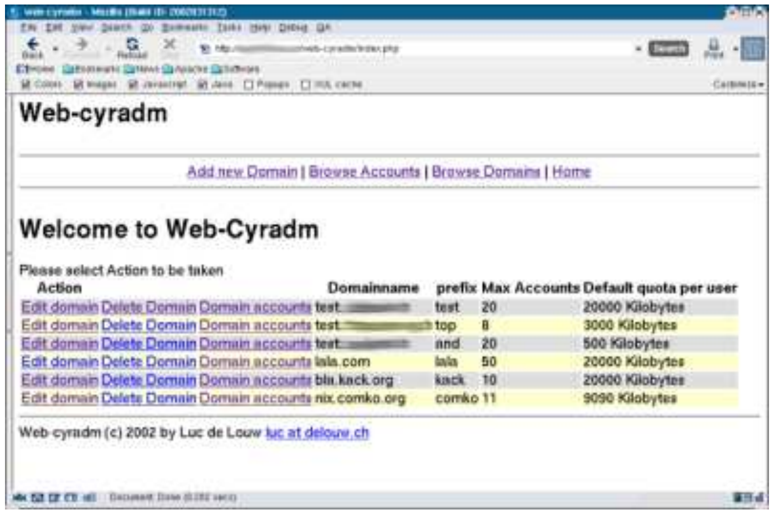
pam means "Pluggable authentication module" and was originally proposed by some people at Sun. In meantime a lot of modules have been developed. One of them is an interface to MySQL

With pam_mysql you to store the users password in a mysql database. Further, Postfix is able to lookup aliases from a MySQL−table. At the end of the day, you have a base for all administrative tasks to be done by the Sysadmin.

Further you will be able to delegate some tasks to Powerusers, e.g. creating Accounts for a particular Domain. Changing passwords and creating new aliases can be delegated to the user. At the end of the day you as a Sysadmin have the time to do some more productive tasks, or write a HOWTO for the Linux Documentation Project :−)

2.5. Web−cyradm Webinterface

Figure 2. Web−cyradm Domain administration



Web−cyradm is the Webinterface that allows you to perform the administrative tasks to your mailsystem This Screenshot shows the domain−administration part of Web−cyradm.

Web−cyradm is written in PHP, which is often installed on webservers. Time to set up Web−cyradm takes just a few minutes.

At the time being, Web−cyradm does not support different roles for its users. So you cannot use it as a frontend for your Powerusers (Domainadmins) or endusers. This Part of Web−cyradm is being developed, and should be ready for distribution in a few weeks (approx. end of may 2002.

3. Getting and installing the software

Most of the software is included in your Linux distribution. SuSE is shipping Cyrus as far as I know since 7.1 and Redhat at least since recent time.

I suggest you to install Cyrus and SASL as binary from rpm. Postfix is needed to compile by yourself because the lack of MySQL support by the rpm's from the distributors.

3.1. Getting and installing MySQL

3.1.1. Download

Origin−Site: http://www.mysql.com/downloads/

3.1.2. Building and installing

```
cd /usr/local
tar -xvzf mysql-3.23.49a.tar.gz
cd mysql-3.23.49a

./configure \
--prefix=/usr/local/mysql \
--enable-assembler \
--with-innodb

make
make install

/usr/local/mysql/bin/mysql_install_db
echo /usr/local/mysql/lib/mysql >> /etc/ld.so.conf
ldconfig
```

For security−improvement add a mysql−user on your system i.e. "mysql", then

```
chown -R mysql /usr/local/mysql/var
```

and change the line user=root to user=mysql in the file `/usr/local/mysql/bin/safe_mysqld`

you may wish to start mysql automatically at boottime, copy `/usr/local/mysql/share/mysql/mysql.server` to `/etc/init.d/` for SuSE and Redhat. Further you need to add Symlinks to `/etc/init.d/rc3.d` for SuSE and `/etc/rc.d/rc3.d`

The following example is for SuSE Linux and should be easily changed for Redhat and other Linux distributions and commercial Unixes.

```
cp /usr/local/mysql/share/mysql/mysql.server /etc/init.d/
ln -s /etc/init.d/mysql.server /etc/init.d/rc3.d/S20mysql
ln -s /etc/init.d/mysql.server /etc/init.d/rc3.d/k08mysql
```

3.2. Getting and installing Postfix

3.2.1. Download

Origin−Site: http://www.postfix.org/ftp−sites.html

3.2.2. Creating a User−ID (UID) and Group−ID (GID) for postfix

Before you can build and install postfix you have to be sure a »postfix« and a »postdrop« groups and users exists on the System. First check for the groups. You can check this by **grep postfix /etc/group** and **grep maildrop /etc/group**

If there are no such groups and users, you just create them. Search for a free nummeric UID and GID. In the following example I will use UID and GID 33333 for Postfix and 33335 for the maildrop UID and GID. This ID's are corresponding to other documents.

```
groupadd -g 33333 postfix
groupadd -g 33335 maildrop

useradd -u 33333 -g 33333 -d /dev/null -s /bin/false postfix
useradd -u 33335 -g 33335 -d /dev/null -s /bin/false maildrop
```

3.2.3. Building and installing

The following screen shows what you have to do, if you installed MySQL from source as described above. If you installed MySQL from a binary package such as rpm or deb, then you have to change the include and library−flags to −I/usr/include/mysql and −L/usr/lib/mysql.

```
tar -xvzf postfix-1.1.7.tar.gz

cd postfix-1.1.7

make -f Makefile.init makefiles \
'CCARGS=-DHAS_MYSQL -I/usr/local/mysql/include' \
'AUXLIBS=-L/usr/local/mysql/lib -lmysqlclient -lz -lm'

make install
```

During **make install** a few question are asked. Just pressing **Enter** should match your needs. For Redhat users it could be useful to enter `/usr/local/share/man`

3.3. Getting and installing Cyrus IMAP

3.3.1. Download and installing

Like mentioned above, SuSE and Redhat are shipping Cyrus in their distributions. Just use yast or the corresponding tool in Redhat.

- cyrus−imapd−devel−2.0.16−115
- cyrus−sasl−1.5.24−157
- cyrus−sasl−gssapi−1.5.24−157
- cyrus−sasl−devel−1.5.24−157
- perl−Cyrus−IMAP−2.0.16−115
- perl−Cyrus−SIEVE−acap−2.0.16−115
- perl−Cyrus−SIEVE−managesieve−2.0.16−115
- cyrus−imapd−2.0.16−115

If you like, you can install it also on the commandline using:

```
rpm -ihv (package-name).rpm
```

Be sure to use only the lastest available version, so check out the downloads−site of your distribution

3.4. Getting and installing pam_mysql

3.4.1. Download

Origin−Site: http://sourceforge.net/projects/pam−mysql/

3.4.2. Installing

```
tar -xvzf pam_mysql-0.4.7.tar.gz

cd pam_mysql

make

cp pam_mysql.so /lib/security
```

3.5. Getting and installing Web−cyradm

3.5.1. Download

Origin−Site: http://www.delouw.ch/linux/web−cyradm

3.5.2. Installing

Web−cyradm is written in PHP. If you don't have a webserver with php installed, I like to refer to my Apache−Compile−HOWTO. That document describes how to set up Apache with PHP and other modules

```
cd /usr/local/apache/htdocs

tar -xvzf web-cyradm-latest.tar.gz
```

After unpacking web−cyradm move it to a place in your webservers DocumentRoot

This is all, now we need to configure the whole bunch of software

4. Configuration

4.1. Configuring MySQL

4.1.1. Securing MySQL

Because you are using MySQL to authenticate users, you need to restrict network access to Port 3306.

I suggest to just bind mysql to the loopback−interface 127.0.0.1. This makes sure nobody can connect to your MySQL−Daemon via the network.

edit `/etc/init.d/mysql.server` and edit line 107 as following:

Original line:

```
$bindir/safe_mysqld --datadir=$datadir --pid-file=$pid_file&
```

Changed line:

```
$bindir/safe_mysqld --datadir=$datadir --pid-file=$pid_file \
--bind-address=127.0.0.1&
```

(Re−)start your MySQL−Daemon by issuing **/etc/init.d/mysql.server start**

To ensure the configuration−change was successful issue: **netstat −an|grep LISTEN**. The Output should be looking similar to this:

```
bond:~ # netstat -an|grep LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
```

4.1.2. Create the databases and tables

Now we need to create the database and tables for postfix and web−cyradm and add a user to the database

Web−cyradm comes with two SQL−files: `insertuser.sql` and `create.sql` The first inserts the Database user to the database »mysql«, the second creates the database »mail« and the needed tables.

The password for the user "mail" in this example is "secret" please insert whatever user and password you like

First you must add the user by executing **/usr/local/mysql/bin/mysql < insertuser.sql** After the new DB−user is successfully added, you need to reload mysql with **mysqladmin reload**

To create the needed tables in the database:

```
/usr/local/mysql/bin/mysql mail -u mail -p < \
/usr/local/apache/htdocs/web-cyradm/create.sql
```

Now lets populate our tables, and insert the first admin−user. This user is needed to login to Web−cyradm

Execute **/usr/local/mysql/bin/mysql mail −p** And type the following SQL query:

```
insert into adminuser (username, password) values ('admin', 'test');
```

Please note, this setup for web−cyradm is fully compatible with replex, another project. Please see http://www.replex.org for more details.

4.2. Configuring PAM

Now we need to get sure that PAM knows how to authenticate the Cyrus users

You have to create the file `/etc/pam.d/imap` with the following entries:

```
auth sufficient pam_mysql.so user=mail passwd=secret host=localhost db=mailadmin table=accountuser usercolumn=username   passwdcolumn=password crypt=0

auth sufficient pam_unix_auth.so

account required pam_mysql.so user=mail passwd=secret host=localhost db=mail table=accountuser usercolumn=username passwdcolumn=password   crypt=0

account  sufficient       pam_unix_acct.so
```

The lines containing pam_unix_auth.so and pam_unix_acct.so are only needed if you are migrating from wu−IMAP to cyrus. This way the users can be authenticate with its old unix−password and its new mysql−based password

If you will use Cyrus also for POP−Service just **cp /etc/pam.d/imap /etc/pam.d/pop**

4.3. Configuring Postfix

Postfix needs two major config files: `main.cf` and `master.cf`. Both needs now our attention.

4.3.1. master.cf

You need to change just one line:

old:

```
argv=/cyrus/bin/deliver
```

new:

```
argv=/usr/cyrus/bin/deliver
```

4.3.2. main.cf

Here you need to change some more things like hostname, relaying, alias−lookups etc.

First change hostname:

```
myhostname = foo.bar.org
```

mydestination

Here you have to put all domainnames that are local (corresponding to sendmail's /etc/mail/sendmail.cw) If you have multiple domains separate them with comma

```
mydestination = foo.bar.org, example.com, furchbar-grausam.ch, whatever.domain.tld
```

relayhost

Here you define where to deliver outgoing mails. If you do not provide any host. mails are delivered directly to the destination smtp host. Usually your relayhosts are your providers smtp−server

```
relayhost = relay01.foobar.net relay02.foobar.net relay03.foobar.net
```

mailtransport

Here you define how the mails accepted for local delivery should be handled. In our situation mails should be delivered by the cyrus delivery−program

```
mailbox_transport = cyrus
```

At the end of file you need to add:

```
virtual_maps = hash:/etc/postfix/virtual, mysql:/etc/postfix/mysql-virtual.cf
```

Outgoing addresses should be rewritten from i.e test0002@domain to user.name@virtualhost.com. This is important if you like to use a webmail interface.

```
sender_canonical_maps = mysql:/etc/postfix/mysql-canonical.cf
```

Now you need to create the file `/etc/postfix/mysql-virtual.cf`:

```
#
# mysql config file for alias lookups on postfix
# comments are ok.
#

# the user name and password to log into the mysql server
hosts = localhost
user = mail
password = secret

# the database name on the servers
```

```
dbname = mailadmin

# the table name
table = virtual

#
select_field = dest
where_field = alias
additional_conditions = and status = '1'
```

And the file `/etc/postfix/mysql−canonical.cf`:

```
# mysql config file for canonical lookups on postfix
# comments are ok.
#

# the user name and password to log into the mysql server
hosts = localhost
user = mail
password = secret

# the database name on the servers
dbname = mail

# the table name
table = virtual
#
select_field = alias
where_field = username
# Return the first match only
additional_conditions = and status = '1' limit 1
```

4.4. Configuring Cyrus IMAP

There is only little changes needed. Edit `/etc/imapd.conf` and take care that the following entry is done

```
    sasl_pwcheck_method: pam
```

This tells the Cyrus IMAP to authenticate using PAM

If you want to enable Cyrus' TLS/SSL facilities you have to create a certificate first. This requires an OpenSSL installation

```
openssl req -new -nodes -out req.pem -keyout key.pem
openssl rsa -in key.pem -out new.key.pem
openssl x509 -in req.pem -out ca-cert -req \
-signkey new.key.pem -days 999

cp new.key.pem /var/imap/server.pem

echo tls_cert_file: /var/imap/server.pem >> /etc/imapd.conf
echo tls_key_file: /var/imap/server.pem >> /etc/imapd.conf
```

If you like to use sieve (A Mail Filtering Language), you must change an entry in `/etc/services`. Add or change the following line:

```
sieve           2000/tcp
```

4.5. Configuring Web−cyradm

You just need to do some changes in
`/usr/local/apache/htdocs/web−cyradm/config.inc.php`

```
cp   config.inc.php−dist config.inc.php
```

Edit the file and change the password and databasename to the appropriate values

5. Testing the setup

5.1. (Re−)Starting the daemons

Now all the software has been installed and configured, lets do some testings now. First you have to (re−)start all the daemons affected

- **postfix start**
- **/etc/init.d/cyrus start**
- **/etc/init.d/mysql.server start**
- **/usr/local/apache/bin/apachectl startssl**

Hopefully all daemons started without any complaints...

Now you can verify if the daemons are running properly by issuing **netstat −an|grep LISTEN**

The output should look similar like that:

```
bond:~ # netstat -an|grep LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
```

The port are assigned like this:

- 993 imap−ssl
- 995 pop3−ssl
- 3306 mysql
- 110 pop3
- 143 imap
- 2000 sieve
- 80 http
- 25 smtp
- 443 https

5.2. Testing Web−cyradm

Now you should be able to connect to http://localhost/mailadmin/ Login with the credentials defined before.

Define a Domainname and some accounts. Be sure the domainname belongs to your server. If not you have to fake it by enter the domain in `/etc/hosts`. The Domain must also be defined as local in `/etc/postfix/main.cf` (mydestination = domain)

5.3. Testing postfix

Now we are going to write a mail:

```
telnet localhost 25
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail ESMTP Postfix

helo localhost
250 mail
mail from: luc@delouw.ch
250 Ok
rcpt to: rcpt to: luc@localhost
250 Ok

data
354 End data with <CR><LF>.<CR><LF>
some text
.
250 Ok: queued as B58E141D33

quit
```

If you see such a message, then all seems to work fine. Be sure to specify a recipients address you previously defined in the web−cyradm database

If you get an error like this:

```
rcpt to: luc@localhost
451 <luc@localhost>: Temporary lookup failure
```

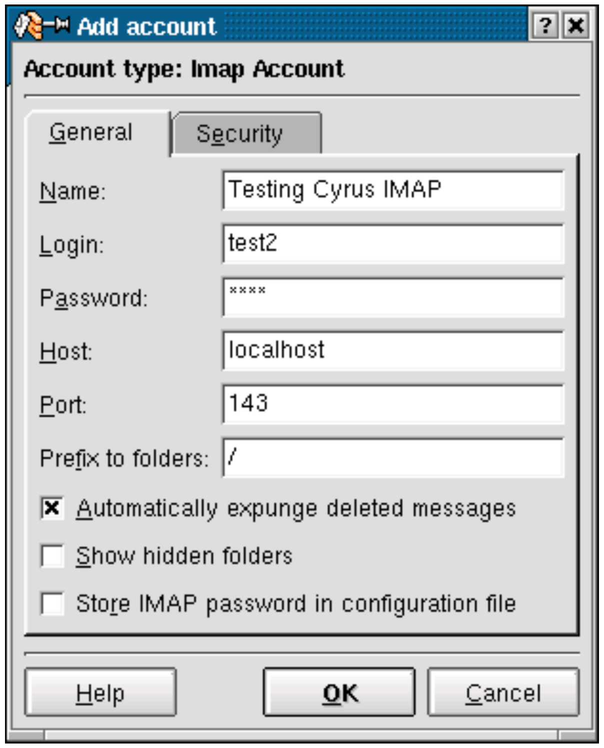
Then eighter MySQL is not running, DB permission are not set properly or you miss−configured `/etc/postfix/main.cf`

On any errors, I suggest to examine `/var/log/mail`. Often you will find some hints whats went wrong.

5.4. Testing the IMAP and POP functionality

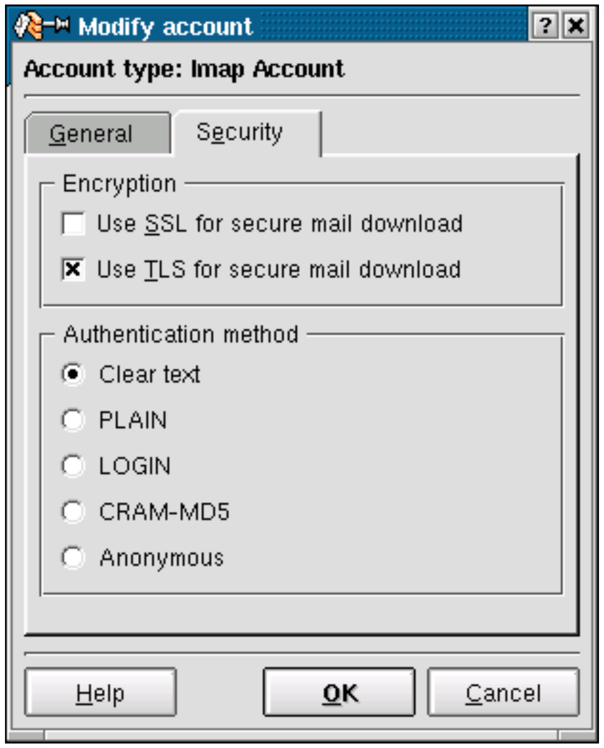
To make that kind of tests. you just need a mailclient like kmail or netscape (Yes of course M$−Products are working as well) but in this example I'll using kmail

Figure 3. Creating a new account



If you enabled TLS/SSL, you may wish to test also the following:

Figure 4. Testing TLS/SSL functionality



If login fails, and you are sure, you typed the right password, take care that MySQL is running

6. Further Information

Here you will find some other resources available in the internet

6.1. News groups

Some of the most interesting news groups are:

- alt.comp.mail.postfix

  This is low traffic−group

- comp.mail.imap

Maybe you also check out your country newsgroups e.g ch.comp.os.linux

Most newsgroups have their own FAQ that are designed to answer most of your questions, as the name Frequently Asked Questions indicate. Fresh versions should be posted regularly to the relevant newsgroups. If you cannot find it in your news spool you could go directly to the FAQ main archive FTP site. The WWW versions can be browsed at the FAQ main archive WWW site.

6.2. Mailing Lists

6.2.1. `<postfix−users@postfix.org>`

Send an mail to `<majordomo@postfix.org>` with the content (not subject):

```
subscribe postfix−users
```

Before writing to the list, check out the archive: http://www.deja.com/group/mailing.postfix.users

6.2.2. `<info−cyrus@lists.andrew.cmu.edu>`

Send an mail to `<majordomo@lists.andrew.cmu.edu>` with the content (not subject):

```
subscribe info−cyrus
```

Before writing to the list, check out the archive:
http://asg.web.cmu.edu/archive/index.php?mailbox=archive.info−cyrus

6.3. HOWTO

These are intended as the primary starting points to get the background information as well as show you how to solve a specific problem. Some relevant HOWTOs are `Cyrus−IMAP` and `Apache−Compile−HOWTO`. The main site for these is the LDP archive

---

6.4. Local Resources

Usually distributions installs some documentation to your system. As a standard they are located in `/usr/share/doc/packages`

The SuSE rpms of Cyrus contains a lot a such documentation.

Postfix has some html−files in the source directory `/usr/local/postfix−20010228−pl08/html`

PAM comes also with lots of documentation in `/usr/share/doc/packages/pam`

The pam_mysql module has a readme with the size of 1670 bytes :−(

6.5. Web Sites

There are a huge number of informative web sites available. By their very nature they change quickly so do not be surprised if these links become quickly outdated.

A good starting point is of course the Linux Documentation Project home page, an information central for documentation, project pages and much more.

To get more deepened information about Postfix, then www.postfix.org would be the starting point.

Please let me know if you have any other leads that can be of interest.

---

7. Questions and Answers

Here I answer the questions which I got from users. If you don't find an answer feel free to contact me

- Q: Why MySQL and not LDAP?

  A: Good question. LDAP is role–based and it would be indeed a better solution for such applications. Unfortunately LDAP is very hard to set up. You have to make proper schemes etc. MySQL is the way strait ahead, it is very easy to handle and versatile. There is a PAM module available for LDAP, feel free to use it.
- Q: Why Postfix and not Qmail?

  A: Lots of people like to see such a setup with Qmail. The reason why is, Mysql–support is a hack and not in the included in the main source–tree. This could end up in a bad situation. Think if a security–hole is found in qmail and the patch does not work with the corrected version. Postfix is supporting MySQL natively. Another (personal) reason is that I find Postfix more sympatic (I don't know why)
- Q: I got a Error: "Temporary lookup failure"

  A: Postfix cannot look up the alias table. Must common failure is that MySQL is not running, or there is a authentication Error. Check `/var/log/mail` and `/usr/local/mysql/var/<hostname>.err` to track the error
- Q: Does this HOWTO also work on other platforms?

  A: Unsure. I personally compiled MySQL and Apache on AIX 4.3 and 5.1L (php does not run properly on AIX), Solaris 6/7/8 and HP–UX. Cyrus, pam_mysql and cyrus I never tried. On Solaris there is maybe a chance to get pam_mysql running. On AIX there is no PAM, but a similar mechanism. In short: Try it, and let me know if were successful