Postfix–Cyrus–Web–cyradm–HOWTO

Luc de Louw

<[luc at delouw.ch](mailto:luc_at_delouw.ch)>

Revision History

Revision 1.2.3	2003–03–24	Revised by: ldl
Some minor correction and enhancements from user–input, updated software mentioned in the HOWTO		
Revision 1.2.2	2003–02–14	Revised by: ldl
Lots of grammar and typos fixed. Some corrections to the pam_mysql Makefile		
Revision 1.2.1	2003–02–12	Revised by: ldl
Nonofficial testrelease: Added lots of fixes and updates. Added OpenSSL and more pam related stuff.		
Revision 1.2.0	2002–10–16	Revised by: ldl
Added lot of user requests, updated the software mentioned in the HOWTO		
Revision 1.1.7	2002–10–15	Revised by: ldl
Added Michael Muenz' hints for SMTP AUTH, corrected ca–cert related mistake, improved SGML code (more metadata), updated the software mentioned in the document.		
Revision 1.1.6	2002–06–14	Revised by: ldl
Added sasl_mech_list: PLAIN to imapd.conf, added web–cyradm Mailinglist, added more to web–cyradm		
Revision 1.1.5	2002–06–11	Revised by: ldl
Added new SQL query to initialize web–cyradm to have full data integrity in the MySQL Database, mysql–mydestination.cf reported to be operational as expected.		
Revision 1.1.4	2002–05–15	Revised by: ldl
Added description what is needed in /etc/services Another fix for pam_mysql compile, updated software versions.		
Revision 1.1.3	2002–05–08	Revised by: ldl
Added more description for web–cyradm, fix for wrong path of the saslauthdb–socket, Fix for wrong place of com_err.h, protection of the TLS/SSL private key.		
Revision 1.1.2	2002–04–29	Revised by: ldl
Added description for Redhat users how to install the init scripts.		
Revision 1.1.1	2002–04–29	Revised by: ldl
Fixed bug in configuring cyrus–IMAP (disabled unused kerberos authentication)		
Revision 1.1.0	2002–04–28	Revised by: ldl
Initial support for building cyrus from source, dropped binary installation for Cyrus, because configuration has changed with Release 2.1.x		
Revision 1.0.2	2002–04–25	Revised by: ldl

Added basic description for sieve and correct sender handling, minor fixes to db related stuff, Added mysql–lookup for »mydestination« , fixed bug for building postfix with mysql support.

Revision 1.0.1   2002–04–07   Revised by: ldl

Added an important fix for compiling pam_mysql

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

Table of Contents

1. Introduction

The cyrus part is only valid for Cyrus−IMAP 2.1.x and Cyrus−SASL 2.1.x. If you plan to use Cyrus−IMAP 2.0.x then please consult the deprecated version 1.0.x of this HOWTO.

I recommend strongly to update to the Cyrus Version 2.1.x. If you do so, you will have chances to get valuable support by the community

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 <<u>luc at delouw.ch</u>>

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

This document is copyrighted (c) 2002, 2003 Luc de Louw and is distributed under the terms of the Linux Documentation Project (LDP) license, stated below.

Unless otherwise stated, Linux HOWTO documents are copyrighted by their respective authors. Linux HOWTO documents may be reproduced and distributed in whole or in part, in any medium physical or electronic, as long as this copyright notice is retained on all copies. Commercial redistribution is allowed and encouraged; however, the author would like to be notified of any such distributions.

All translations, derivative works, or aggregate works incorporating any Linux HOWTO documents must be covered under this copyright notice. That is, you may not produce a derivative work from a HOWTO and impose additional restrictions on its distribution. Exceptions to these rules may be granted under certain conditions; please contact the Linux HOWTO coordinator at the address given below.

In short, we wish to promote dissemination of this information through as many channels as possible. However, we do wish to retain copyright on the HOWTO documents, and would like to be notified of any plans to redistribute the HOWTOs.

If you have any questions, please contact <<u>linux−howto at metalab.unc.edu</u>>

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

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

- Michael Muenz <<u>m.muenz at maxonline.de</u>> for his help with SMTP Authentication
- The nice people at <<u>discuss at linuxdoc.org</u>> for supporting me in writing the 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 : <<u>luc at delouw.ch</u>>.

Please understand, that I don't want to add Cyrus−IMAP 2.0.x related stuff in this Document anymore

1.8. Translations

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

Translations to other languages are always welcome. If you translated this document, please translate the SGML source. Please let me know if you begin to translate, so I can set a link here.

2. Technologies

2.1. The Postfix MTA

> 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.
>
> ––www.postfix.org

Figure 1. Postfix – the big picture
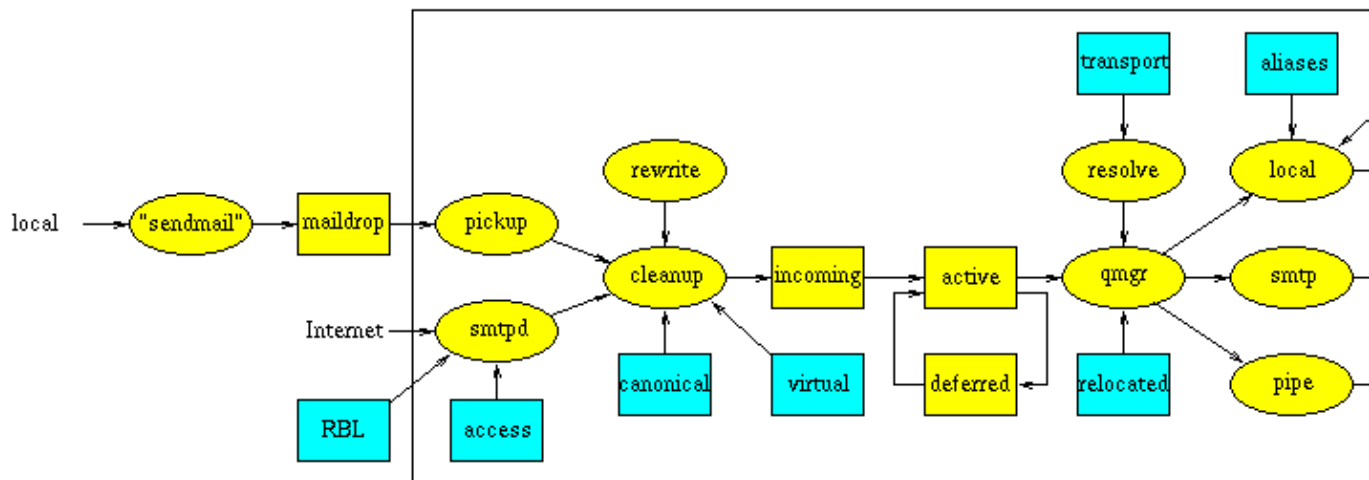
Doesn't it look impressive? – It looks much more complicated as it is. Postfix is indeed nice to configure and handle.

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 needed to get the system running.

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 own method. Each message is stored in its own file. The benefit of separate file is also the reliability, on filesystem errors, only one message is lost. Metadata like statuts of a message (seen etc) is stored in a database. Additionally the messages are indexed. This makes Cyrus very performant. Especially with lots of users and/or lot of big emails, there is nothing else 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 either use the commandline interface, or use one of the available Webinterfaces. This Method is much more secure than a Webinterface to `/etc/passwd`.

Starting from Cyrus 2.1, the SASL−lib version 2 is used for authentication. For the setup described in this HOWTO, there is a tree−layer authentication implemented. Cyrus authenticates with saslauthdaemon which forwards the request to pam_mysql which finally looks up the MySQL−table.

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

2.3. Cyrus SASL

SASL means »Simple Authentication and Security Layer«. It is standardized by the IETF (Internet Engineering Taskforce). SASL is used by network servers (Here for Cyrus−IMAP) to handle authentication requests from clients.

Cyrus SASL is a extensive software, and sometimes not easy to understand. Even I just have a minimum knowledge needed to write this HOWTO.

2.4. OpenSSL

OpenSSL is a library needed by SASL for encrytion of the data−stream. It is used by by almost all opensource software which needs encryption methods. Most or all distributions comes with a preinstalled OpenSSL. Be sure to install also the appropriate devel−package. If you like, you also can compile OpenSSL by your self. This is especially recommended, if you need to fix a security hole.

2.5. 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.

2.6. 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 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 postmaster.

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.

2.7. Web−cyradm Webinterface

Figure 2. Web−cyradm Domain administration
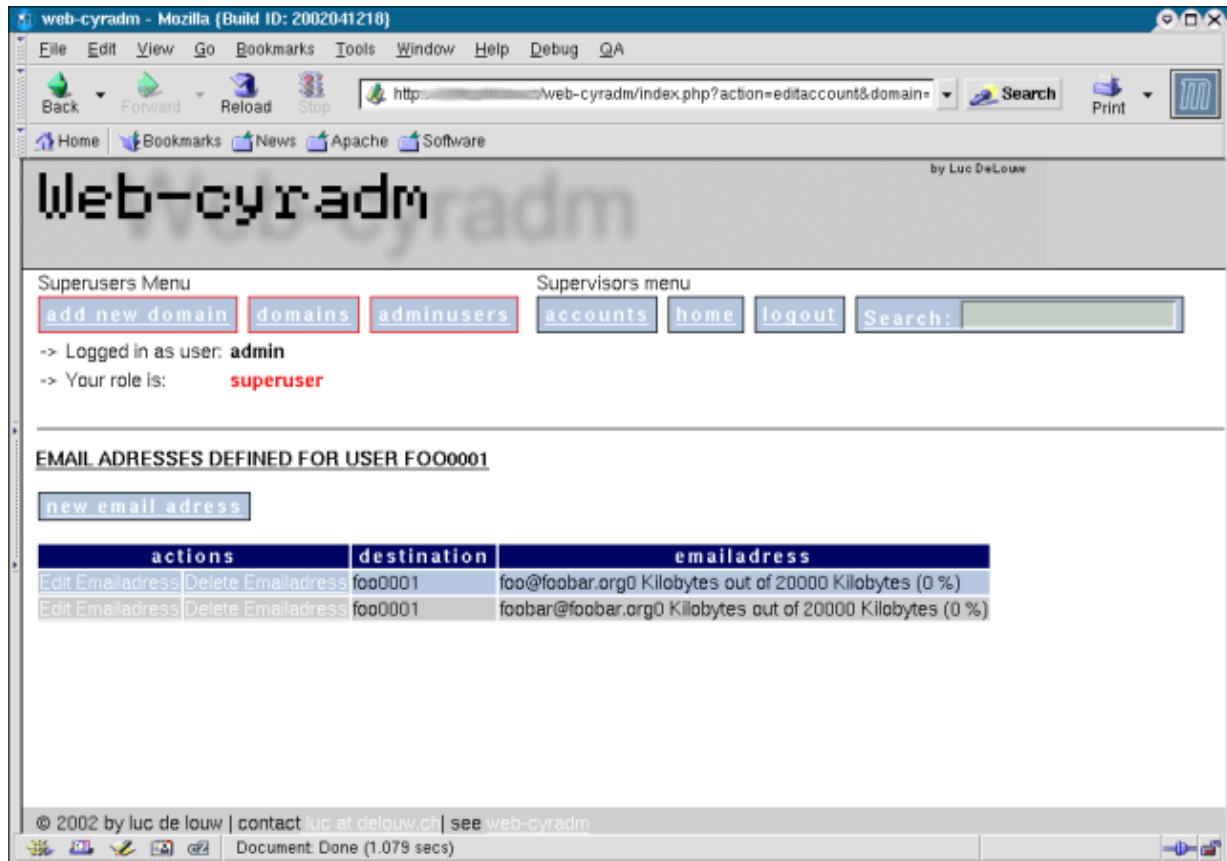
Web−cyradm is the webinterface that allows you to perform the administrative tasks to your mailsystem. This screenshot shows the domain administration part of Web−cyradm.

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

Web−cyradm is under active development from people around the globe. The list of features grows with each release. If you like to contribute to web−cyradm, or you have a nice idea, feel free to contact the mailinglist on http://www.web−cyradm.org

Here a choice of features:

- Administration of multiple virtual domains
- Setting of quotas
- Automatically create username, either with a defined prefix, or the domainname as postfix
- Delegate tasks like creating new users to »Domain Masters«
- Map user−accounts to emailadresses
- Forwarding of accounts or single aliases
- Vacation function for single aliases

- Support for SMTP Transport Tables
- Support for MySQL and PostgreSQL
- i18n (internationalization) support (including different charsets)
- Translated into 14 Languages and growing

Web–cyradm has support for different roles of its users. If you plan to use is as a frontend for your powerusers, please notice, that security may be a problem, the role based stuff needs a security review.

3. Getting and installing the software

Most of the software is included in your Linux distribution. I. e. SuSE is shipping Cyrus as far as I know since 7.1. Since SuSE 8.1, cyrus–imap 2.1 and sasl2 is included, and works. It is still recommended to compile Cyrus by yourself. SuSE does not ship a MySQL enabled Postifx.

Please let me know about other distributions, especially Debian.

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-3.23.56.tar.gz
cd mysql-3.23.56

./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

ln -s /usr/local/mysql/include/mysql /usr/include/mysql
ln -s /usr/local/mysql/lib/mysql /usr/lib/mysql
```

For security–improvement add a mysql–user on your system i.e. »mysql«, then

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

You may wish to start MySQL automatically at boottime, copy `/usr/local/mysql/share/mysql/mysql.server` to `/etc/init.d/` for SuSE, for Redhat it is `/etc/rc.d/init.d` instead of `/etc/init.d/`. Further you need to add symbolic links to `/etc/init.d/rc3.d` for SuSE and `/etc/rc.d/rc3.d` for Redhat.

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 Berkeley DB

The Berkeley DB is a requirement for building Cyrus−SASL and Cyrus−IMAP. Some Systems comes with recent versions but without the header files installed. Please see your distributors CD/DVD to check if you can install the header files from a package. Usually this package is called bdb−devel.

The version that comes with GNU/Debian Linux is out of Date, you will need to compile most recent version instead. If you already installed Berkely DB on your Debian Box, please fist uninstall the software to prevent conflicts.

It is also very important, that Cyrus−SASL and Cyrus−IMAP is compiled with the same version of Berkely DB of else you can run into problems

3.2.1. Download Berkely DB

Origin−Site: http://www.sleepycat.com/update/snapshot/db−4.0.14.tar.gz

3.2.2. Building and installing Berkeley DB

```
cd dist

./configure −−prefix=/usr/local/bdb

make
make install

echo /usr/local/bdb/lib >> /etc/ld.so.conf
ldconfig
```

3.3. Getting and installing OpenSSL

3.3.1. Download OpenSSL

Origin−Site http://www.openssl.org

3.3.2. Building and installing

```
cd /usr/local
tar −xvzf openssl−0.9.7a.tar.gz

cd openssl−0.9.7a

./config shared

make
make test
make install

echo "/usr/local/ssl/lib" >> /etc/ld.so.conf
ldconfig
```

(i) **Select your CPU to improve speed**

By default the Makefile generates code for the i486 CPU. You can change this by editing the Makefile after running **config** shared. Search for −m486 and replace it i.e with −march=athlon

3.4. Getting and installing Cyrus SASL and IMAP

Building Cyrus SASL and IMAP from source is not a easy task. There are some prerequisites to be fulfilled, and lots of difficult authentication related stuff to be considered.

3.4.1. Download Cyrus SASL and Cyrus IMAP

Origin−Site: ftp://ftp.andrew.cmu.edu/pub/cyrus−mail/cyrus−sasl−2.1.12.tar.gz

Origin−Site: ftp://ftp.andrew.cmu.edu/pub/cyrus−mail/cyrus−imapd−2.1.12.tar.gz

3.4.2. Create the cyrus user

On most systems there is no cyrus user and mailgroup per default. Check for a free UID, usually daemons are running with UID less that 100. As example I'm using UID 96 like SuSE has in the default /etc/passwd.

```
groupadd mail
useradd −u 96 −d /usr/cyrus −g mail cyrus
passwd cyrus
```

3.4.3. Building and installing Cyrus SASL

```
tar −xvzf cyrus-sasl−2.1.12.tar.gz
cd cyrus-sasl−2.1.12

./configure \
--enable-anon \
--enable-plain \
--enable-login \
--disable-krb4 \
--with-saslauthd=/var/run/saslauthd \
--with-pam \
--with-dblib=berkeley \
--with-bdb-libdir=/usr/local/bdb/lib \
--with-bdb-incdir=/usr/local/bdb/include \
--with-openssl=/usr/local/ssl \
--with-plugindir=/usr/local/lib/sasl2


make
make install

mkdir −p /var/run/saslauthd

cd saslauthd
make testsaslauthd
cp testsaslauthd /usr/local/bin

echo /usr/local/lib/sasl2 >> /etc/ld.so.conf
```

```
ldconfig
```

The SASL library is installed in `/usr/local/lib/sasl2` but some programs are expecting SASL in `/usr/lib/sasl2`. So it is a good idea to create a symbolic link: **ln −s /usr/local/lib/sasl2 /usr/lib/sasl2**.

3.4.4. Building Cyrus–IMAP

```
tar -xvzf cyrus-imapd-2.1.12.tar.gz
cd cyrus-imapd-2.1.12

export CPPFLAGS="-I/usr/include/et"

./configure \
--with-sasl=/usr/local/lib \
--with-perl \
--with-auth=unix \
--with-dbdir=/usr/local/bdb \
--with-bdb-libdir=/usr/local/bdb/lib \
--with-bdb-incdir=/usr/local/bdb/include \
--with-openssl=/usr/local/ssl \
--without-ucdsnmp \

make depend
make
make install
```

3.4.5. Automatic startup script

If you wish to start the Cyrus IMAP daemon automatically after booting, you need a startupscript. Place the following script in `/etc/init.d/` for Redhat it is `/etc/rc.d/init.d` instead of `/etc/init.d/`.

```
#!/bin/bash
#
# Cyrus startup script

case "$1" in
    start)
        # Starting SASL saslauthdaemon
        /usr/local/sbin/saslauthd -a pam&

        # Starting Cyrus IMAP Server
        /usr/cyrus/bin/master &
        ;;

    stop)

        # Stopping SASL saslauthdaemon
        killall saslauthd

        # Stopping Cyrus IMAP Server
        killall /usr/cyrus/bin/master

        ;;

    *)
        echo "Usage: $0 {start|stop}"
        exit 1
        ;;
```

```
esac
```

If I get the time, I'll provide a more sophisticated script, but this script works

Now create the Symlinks in the runlevel directory (SuSE):

```
ln −s /etc/init.d/cyrus /etc/init.d/rc3.d/S20
ln −s /etc/init.d/cyrus /etc/init.d/rc3.d/K10
```

For Redhat:

```
ln −s /etc/rc.d/init.d/cyrus /etc/rc.d/rc3.d/S20cyrus
ln −s /etc/rc.d/init.d/cyrus /etc/rc.d/rc3.d/K10cyrus
```

3.5. Getting and installing Postfix

3.5.1. Download

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

3.5.2. 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 postdrop

useradd −u 33333 −g 33333 −d /dev/null −s /bin/false postfix
```

3.5.3. 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.

⚠️ **Old MTA needs to be uninstalled**

It is important, that you are uninstalling any sendmail version from RPM based Systems. I suggest to remove sendmail, and install Postfix instead. At least SuSE RPMs need a MTA. After installing the Postfix−RPM, just over−install Postfix by further following the HOWTO

```
tar −xvzf postfix-2.0.7.tar.gz

cd postfix-2.0.7
```

```
make makefiles 'CCARGS=-DHAS_MYSQL \
-I/usr/local/mysql/include/mysql -DUSE_SASL_AUTH \
-I/usr/local/include/sasl -I/usr/local/bdb/include' \
'AUXLIBS=-L/usr/local/mysql/lib/mysql \
-lmysqlclient -lz -lm -L/usr/local/lib -lsasl2 -L/usr/local/bdb/lib'
make
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

Now you need to create some sybolic links to start Postfix automatically on system startup. The sample is for SuSE Linux, please consult your vendors manual for other distributions.

```
ln -s /usr/sbin/postfix /etc/init.d/rc3.d/S14postfix
ln -s /usr/sbin/postfix /etc/init.d/rc3.d/K07postfix
```

3.6. Getting and installing PAM

PAM is on almost all ditributions installed by default. I'm not descibing here how compile PAM by yourself, because it could break your system. I'll describe instead, how install the RPM. the version could be vary.

```
rpm -i pam-devel.rpm
```

Experianced Debian users: Please provide me information how to install pam−devel, thanks

3.7. Getting and installing pam_mysql

3.7.1. Download

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

3.7.2. Installing

```
tar -xvzf pam_mysql-0.5.tar.gz

cd pam_mysql
```

Depending if you compiled mysql by yourself or not, check the Makefile and enter the correct path to your mysql libs and add the compiler flag CFLAGS -I/path/to/mysql/include.

```
ifndef FULL_LINUX_PAM_SOURCE_TREE
export DYNAMIC=-DPAM_DYNAMIC
export CC=gcc
export CFLAGS=-O2 -Dlinux -DLINUX_PAM \
       -ansi -D_POSIX_SOURCE -Wall -Wwrite-strings \
       -Wpointer-arith -Wcast-qual -Wcast-align -Wtraditional \
       -Wstrict-prototypes -Wmissing-prototypes -Wnested-externs -Winline \
       -Wshadow -pedantic -fPIC -I/usr/local/mysql/include
export MKDIR=mkdir -p
export LD_D=gcc -shared -Xlinker -x -L/usr/local/mysql/lib/mysql -lz
endif
```

After customizing that file go ahead with compiling pam_mysql

```
make

cp pam_mysql.so /lib/security

[[ ! -d /var/lib/mysql ]] && mkdir /var/lib/mysql
ln -s /tmp/mysql.sock /var/lib/mysql/mysql.sock
```

3.8. Getting and installing Web−cyradm

3.8.1. Download

Origin−Site: http://www.web−cyradm.org

3.8.2. Installing

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

tar -xvzf web-cyradm-0.5.3.tar.gz

touch /var/log/web-cyradm.log
chown nobody /var/log/web-cyradm.log
```

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

Thats all. Now you need to configure the whole bunch of software.

Web−cyradm 0.5.3 is considered stable, and was released on 2003−03−24

Since web−cyradm uses PEAR for its database abstraction layer, you also need a recent copy of PEAR. This is included in recent PHP Versions. I strongly suggest to update PHP to 4.3.1, because a lot of important bugs have been fixed.

An often mistake is to forget to touch the logfile and change the owner to the UID that Apache use. This is usually »nobody« or »wwwrun«.

3.8.3. 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 three MySQL scripts: `insertuser_mysql.sql` and `create_mysql.sql`. The first inserts the Database user to the database »mysql« and creates the database »mail«. The second creates the needed tables and populates the database with an initial admin−user and the cyrus user.

The third script is used for upgrading from Web−cyradm 0.5.2 to 0.5.3.

The password for the database user »mail« in this example is »secret«. Please insert whatever user and password you like.

The username for the initial superuser is »admin« with the password »test«.

⚠️ **Change the default password!**

> If a malicious user wants to gain unauthorized access to a system, the first try is always the default username and password supplied by the vendor. It is IMPORTANT that you are changing them in the scripts before applying them.

After customizing the username and password, apply the scripts:

```
/usr/local/mysql/bin/mysql −u root −p < \
/usr/local/apache/htdocs/web-cyradm/scripts/insertuser_mysql.sql

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

3.8.4. Upgrading from 0.5.2 to 0.5.3

In version 0.5.3 there us a small Database enhancement done. You can upgrade your Database by issuing the MySQL script that commes with the distribution.

```
mysql mail −u mail −p < \
scripts/upgrade-0.5.2-to-0.5.3_mysql.sql
```

Since Version 0.5.3 web−cyradm does have full support for DES crypted passwords. You can use the php−script `migrate.php` to convert the users passwords from plain to unix compatible crypt (DES).

⚠️ **Migration from plain to crypt cannot be undone**

> Be sure to have a recent backup of your database before doing anything with the migration script.

4. Configuring MySQL

4.1. 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 only 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 change 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
```

4.2. Setting up rinetd

This step is only necessary if you run the mysql sever on another host than the mailserver. It allows you to securely connect from another host by allowing only defined IP adresses.

The example used is from the view of the host serving the MySQL database. Lets assume your mailserver has the IP 192.168.0.100 and the MySQL host has 192.168.0.200

Edit /etc/rinetd.conf and add:

```
192.168.0.200 3306 127.0.0.1 3306
allow 192.168.0.100
```

This means: The MySQL host is listening on 192.168.0.200 port 3306. If 192.168.0.100 is attempting a connection, it is forwarded to 127.0.0.1:3306. All other hosts are rejected.

5. 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=mail table=accountuser use

auth sufficient pam_unix_auth.so

account required pam_mysql.so user=mail passwd=secret host=localhost db=mail table=accountuser us

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 allows you to authenticate with its old unix−password AND its new mysql−based password.

To use the other services provided by cyrus and smtp−authtication you need to copy the file so that they match the service−ID

```
cp /etc/pam.d/imap /etc/pam.d/pop
cp /etc/pam.d/imap /etc/pam.d/sieve
cp /etc/pam.d/imap /etc/pam.d/smtp
```

6. Configuring Postfix

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

6.1. master.cf

You need to change just one line:

old:

```
flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
```

new:

```
flags= user=cyrus argv=/usr/cyrus/bin/deliver -r ${sender} -m ${extension} ${user}
```

What affect that changes?

A look to the cyrus man–pages **man deliver** clears that issue:

The Postfix default setup uses a wrong path to cyrus deliver, this is the first change. The parameter »−r« Inserts a proper return path, without that mail rejected/retured by sieve will be sent to the cyrus user at yourdomain.

6.2. 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, mysql:/etc/postfix/mysql-mydestination.cf
```

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 your 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
```

If you dont want to have a overriding /etc/postfix/virtual, skip the hash entry

Outgoing addresses should be rewritten from i.e test0002 at domain to user.name at 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 = mail

# the table name
table = virtual

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

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
```

6. Configuring Postfix   19

```
where_field = username
# Return the first match only
additional_conditions = and status = '1' limit 1
```

Finally the file `/etc/postfix/mysql-mydestination.cf`:

```
# mysql config file for local domain (like sendmail's sendmail.cw) 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 = domain
#
select_field = domain_name
where_field = domain_name
```

SMTP Authentication with SASL and PAM

Put the following in your `/etc/postfix/main.cf`

```
smtpd_sasl_auth_enable = yes
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destir
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = example.com
broken_sasl_auth_clients = yes
```

You also need to create the file `/usr/local/lib/sasl2/smtpd.conf` with the following content:

```
pwcheck_method: saslauthd
```

The next step is make the saslauthd socket being found by postfix:

```
mv /var/run/sasl2 /var/run/sasl2-old
ln -s /var/run/saslauthd /var/run/sasl2
```

7. Configuring Cyrus IMAP

7.1. Creating the config files

You have to create `/etc/imapd.conf` and `/etc/cyrus.conf`

7.1.1. `/etc/services`

If you like to use sieve (a mail filtering language), you must change an entry in `/etc/services`. With SuSE 8.0 take especially care about the port for sieve, they defined the wrong port. Add or change the following lines:

```
pop3            110/tcp
imap            143/tcp
imaps           993/tcp
pop3s           995/tcp
sieve           2000/tcp
```

7.1.2. `/etc/imapd.conf`

```
postmaster: postmaster
configdirectory: /var/imap
partition-default: /var/spool/imap
admins: cyrus
allowanonymouslogin: no
allowplaintext: yes
sasl_mech_list: PLAIN
servername: servername
autocreatequota: 10000
reject8bit: no
quotawarn: 90
timeout: 30
poptimeout: 10
dracinterval: 0
drachost: localhost
sasl_pwcheck_method: saslauthd
sievedir: /usr/sieve
sendmail: /usr/sbin/sendmail
sieve_maxscriptsize: 32
sieve_maxscripts: 5
#unixhierarchysep: yes
```

Be sure »servername« contains your FQHN (Fully Qualified Hostname)

The parameter »unixhierarchysep: yes« is only used if you like to have usernames like »hans.mueller.somedomain.tld« see Section 8 for more info.

7.1.3. Creating the TLS/SSL Certificate

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

mkdir /var/imap

cp new.key.pem /var/imap/server.pem
rm new.key.pem
cat ca-cert >> /var/imap/server.pem

chown cyrus:mail /var/imap/server.pem
chmod 600 /var/imap/server.pem # Your key should be protected

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

7.1.4. `/etc/cyrus.conf`

The other file you need to create is `/etc/cyrus.conf` It is the configuration file for the Cyrus master
process. It defines the startup procedures, services and events to be spawned by process »master«.

```
# standard standalone server implementation

START {
  # do not delete this entry!
  recover         cmd="ctl_cyrusdb -r"

  # this is only necessary if using idled for IMAP IDLE
#  idled                cmd="idled"
}

# UNIX sockets start with a slash and are put into /var/imap/socket
SERVICES {
  # add or remove based on preferences
  imap          cmd="imapd" listen="imap" prefork=0
  imaps         cmd="imapd -s" listen="imaps" prefork=0
  pop3          cmd="pop3d" listen="pop3" prefork=0
  pop3s         cmd="pop3d -s" listen="pop3s" prefork=0
  sieve         cmd="timsieved" listen="sieve" prefork=0

  # at least one LMTP is required for delivery
#  lmtp         cmd="lmtpd" listen="lmtp" prefork=0
  lmtpunix      cmd="lmtpd" listen="/var/imap/socket/lmtp" prefork=0

  # this is only necessary if using notifications
#  notify       cmd="notifyd" listen="/var/imap/socket/notify" proto="udp" prefork=1
}

EVENTS {
  # this is required
  checkpoint    cmd="ctl_cyrusdb -c" period=30

  # this is only necessary if using duplicate delivery suppression
  delprune      cmd="ctl_deliver -E 3" period=1440

  # this is only necessary if caching TLS sessions
  tlsprune      cmd="tls_prune" period=1440
}
```

7.2. Creating the directories

There must be created different directories. Additionally you should change some attributes of the filesystem

7.2.1. `/var/imap`

```
cd /var
mkdir imap
chown cyrus:mail imap
chmod 750 imap
```

7.2.2. `/var/spool/imap`

```
cd /var/spool
mkdir imap
chown cyrus:mail imap
chmod 750 imap
```

7.2.3. `/usr/sieve`

```
cd /usr
mkdir sieve
chown cyrus:mail sieve
chmod 750 sieve
```

7.2.4. The rest of the directories

The rest of the directories can be created by the tool **mkimap**

```
su − cyrus
/usr/local/cyrus-imapd-2.1.12/tools/mkimap
```

7.3. Changing the filesystem attributes

When using the ext2 filesystem, you must set an attribute, that defines, that all changes are immediately committed to the disk. With todays journaling filesystems there is no need. If you are still running ext2 filesystems, I strongly suggest to switch to ext3 filesystems. Ext2 and ext3 are fully compatible to each other.

To check what type of filesystem is used for `/var` issue the command **mount** or see your `/etc/fstab`. Please note that the `/var` could also be a part of the root or other filesystem.

```
cd /var/imap

chattr +S user quota user/* quota/*
chattr +S /var/spool/imap /var/spool/imap/*
```

8. Configuring Web−cyradm

First copy the distributions config file, and create to logfile. The logfile must be owned by user that runns the webserver. This is usually the user »nobody« or »wwwrun«.

```
cp config.inc.php-dist config.inc.php

touch /var/log/web-cyradm-login.log
chown nobody /var/log/web-cyradm-login.log
```

8.1. Cyrus setup

```
# The Cyrus login stuff

$CYRUS_HOST="localhost";
$CYRUS_PORT="143";
$CYRUS_USERNAME="cyrus";
$CYRUS_PASSWORD="secret";
```

This should be self−explanatory. Please note there is no support for SSL connections at the moment, this is especially important for users that what to like to have web−cyradm not on the same server where the cyrus−imapd resides.

8.2. Database setup

Since version 0.5.2 web−cyradm uses PEAR as a database abstraction layer. This adds more flexibility. Currently supported databases are MySQL and PostgreSQL. Please note that for PostgreSQL there is a patch needed, because Postfix does not support PostgreSQL natively. I strongly suggest to use MySQL. I know MySQL has some restrictions on transaction and stuff, but it is natively in the Postfix code.

The entries should be self explenatory

```
$DB_TYPE="mysql";

/* DB_TYPE

 Possible Values are:
 o mysql
 o pgsql

 To operate a mailsystem with PostgreSQL you will need a patch for
 Postfix.

 Other Databases needs to be supported by PAM and postfix

*/


$DB_HOST="localhost";
$DB_NAME="mail";
$DB_USER="mail";
$DB_PASSWD="secret";
$DB_PROTOCOL="unix"; // set to "tcp" for TCP/IP
$DSN="$DB_TYPE://$DB_USER:$DB_PASSWD@$DB_PROTOCOL+$DB_HOST/$DB_NAME";
```

8.3. Default Quota

The default quota to be used is set in the variable `DEFAULT_QUOTA=20000` and is used when creating a new domain

8.4. Crypted passwords

Web−cyradm supports the storage of encryted passwords. I strongly suggest, to use encryption. There are two methods supported at the moment: Unix−compatible (crypt) and MySQL. The Unix−compatible encryption allows you to take over encrytped passwords from an existing `/etc/shadow`. This should be preferred.

Unfortunately, MySQL uses a proprietary encryption method which is only available when using MySQL. I'm currently thinking about dropping support for MySQL crypt, because it would only work with MySQL and makes a migration to another database impossible. As soon as there is a method available to re−engineer the MySQL crypt on PHP there will be a solution (Help needed in programming, legal contraints?)

Check the variable `$CRYPT` in the file `config.inc.php`. Value »plain« means no encryption, »crypt« means Shadow compatible encryption, mysql means MySQL encryption.

Choose encryption method carefully

Since the supported crypto−methods are all one−way encryptions, there will be NO WAY to migrate from one to another. Note also, that this is a global variable, which means, it is used for all passwords, including the password of the admin users. I STRONGLY suggest to use Unix Shadow compatible encryption, because it makes you independant from any software vendor.

8.5. Usernames

There are two schemas of usernames supported which are defined in the variable »DOMAIN_AS_PREFIX«. The default is to have a defined prefix ($DOMAIN_AS_PREFIX=0), i.e. »test« for the domain »expample.com«. With this scheme, the first user gets the username test0001, the second test0002 and incrementing.

The other one is to have usernames like »hans.mueller.example.com«. If that case set $DOMAIN_AS_PREFIX=1

At the moment you can not mix both schemas, evaluate carefully with scheme matches your needs best

If you choose to have $DOMAIN_AS_PREFIX=1, be sure you uncomment the option `unixhierarchysep: yes` like described in

9. Testing the setup

9.1. (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. Note that this is assuming saslauthd is started in the cyrus startup script.

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

9.2. Testing Web−cyradm

Now you should be able to connect to http://localhost/web−cyradm/ 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)

Please be sure that you are providing a unique domain prefix when adding a new domain. I.e. test for the domain test.org. If you don't provide such a prefix you will get a error message.

9.3. 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 at delouw.ch
250 Ok
rcpt to: luc at 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 at localhost
451 <luc at localhost>: Temporary lookup failure
```

Then either MySQL is not running, DB permission are not set properly or you missconfigured `/etc/postfix/main.cf`

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

9.4. Testing the IMAP functionality

A lot of users like to test the cyrus−IMAPd with the Command Line Interface (CLI) »cyradm« and they are failing. To be successful with cyradm, you will need to add the cyrus user to `/etc/sasldb2` because »cyradm« always authenticates against SASL AND IMAP.

To add the Cyrus user to the sasldb use the command:

```
saslpasswd2 −c cyrus
Password: (enter your passwd)
Again (for verification): (enter your password)
```

To use the »cyradm« CLI please take care that the tool does not recognize standard CLI−options like −u and similar. Please follow the syntax like described in the man page »cyradm 1« like the following example:

```
bond:~ # cyradm --user cyrus --server localhost --auth plain
Password: # This is the SASL2 password
IMAP Password: # This is the IMAP password that you need to enter in the mysql-table »accountuser
localhost>
```

With the Cyrus command **help** you will see all possible commands and its abbreviations.

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'm using kmail.

Figure 3. Creating a new account
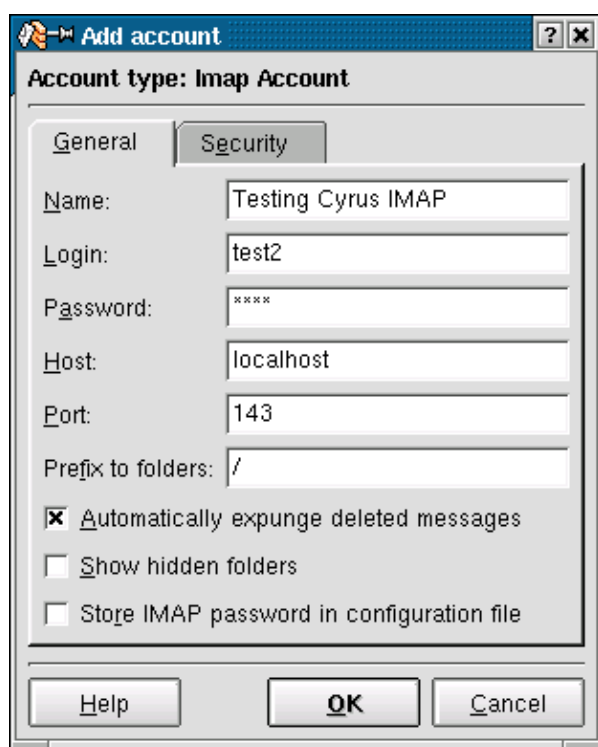
If you enabled TLS/SSL, you may wish to test also the following:

Figure 4. Testing TLS/SSL functionality
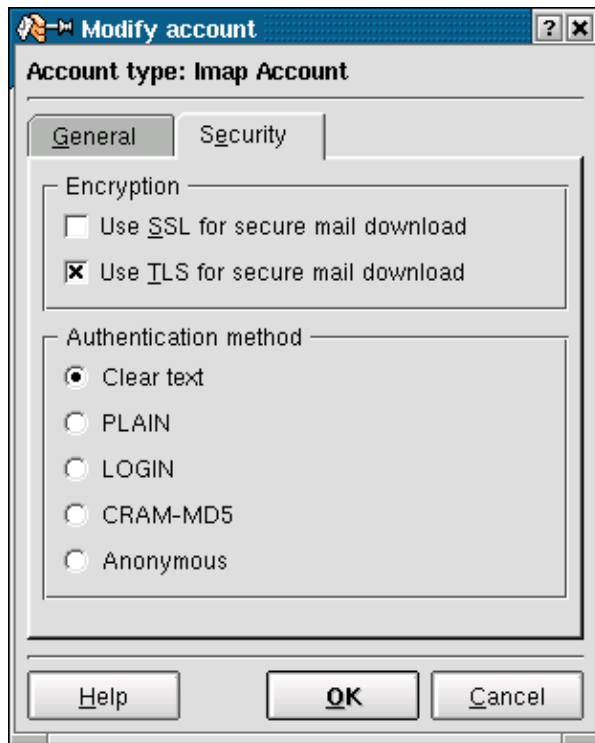
If login fails, and you are sure, you typed the right password, take care that MySQL is running.

---

10. Further Information

Here you will find some other resources available in the internet.

10.1. 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.

10.2. Mailing Lists

10.2.1. <postfix-users at postfix.org>

Send an mail to <majordomo at 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

10.2.2. <info-cyrus at lists.andrew.cmu.edu>

Send an mail to <majordomo at 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

10.2.3. <web-cyradm at web-cyradm.org>

Subscription can be done trought the webinterface
http://www.web–cyradm.org/mailman/listinfo/web–cyradm

Before writing to the list, check out the archive for similar incidents:
http://www.web–cyradm.org/pipermail/web–cyradm/

10.3. HOWTO

This 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.

10.4. 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-2.0.3/html`

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

The pam_mysql module has a readme with the incredible size of 1670 bytes.

10.5. 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.

11. 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

1. FAQ

11.1.1. Does web−cyradm only support users like »test0001« ? I'd like to have a more descriptive username

web−cyradm does also support usernames like »user.name.example.com« if you configure it. Your need to change config.inc.php and change the value of DOMAIN_AS_PREFIX to 1. then you need to add »unixhierarchysep: yes« to your `/etc/imapd.conf`

11.1.2. web−cyradm complains about »Fatal error: Call to undefined function: bindtextdomain() in /www/web−cyradm−0.5.3/index.php on line 46«, whats wrong?

Web−cyradm needs gettext enabled PHP. Please compile PHP with the configure−option −−with−gettext.

gettext is needed for NLS (Native Language Support) which means contributors can easily translate web−cyradm to there language. Fill in your Language in the file `/usr/local/apache/htdocs/web-cyradm/locale/templates/web-cyradm.pot` and send me the file, then your language will be supported in the next CVS snapshot

11.1.3. I got a error from Web−cyradm like this »Fatal error: Call to undefined function: query() in /usr/local/httpd/htdocs/web−cyradm/auth.inc.php on line 17«

Web−cyradm depends on PEAR for database abstraction. PEAR is included in recent PHP versions. Often PEAR is a separate package, check out the package base of your distribution. I strongly suggest to update to the most recent version of PHP anyway, because a lot of bugs have been fixed.

Another reason could be an authentication error with MySQL. Be sure the user »mail« has enought rights to acccess the database and tables.

11.1.4. Why MySQL and not LDAP?

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.

11.1.5. Why Postfix and not Qmail?

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)

11.1.6. I got a Error: "Temporary lookup failure"

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.

11.1.7. Does this HOWTO also work on other platforms?

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