Postfix-Cyrus-Web-cyradm-HOWTO

Luc de Louw

luc at delouw.ch

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.

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 strongly recommend that you upgrade to Cyrus Version 2.1.x. If you do so, you will have a better ability to get valuable support from the user community

1.1. Contributors and Contacts

First I would thank all those people who sent questions and suggestions that made the further development of this document possible. It shows me that 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 on how to set up different mailsystems. Most documents that are available are related to Sendmail, procmail, WU-IMAPd and friends. These packages are very good but are unfortunately very inflexible in their user administration.

For a long time I was testing alternative MTA's like qmail, postfix and exim, in conjunction with 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 best performing solution.

All these combinations of software had one thing in common: their was very little documentation available describing how these packages work together with each other. To install the software, lot of effort has be spent to get all information needed to get all the software running.

1.3. Copyright Information

This document is copyrighted (c) 2002, 2003, 2004 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 <`linux-howto at metalab.unc.edu`>

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 can be obtained from http://www.delouw.ch/linux

- HTML (http://www.delouw.ch/linux/Postfix-Cyrus-Web-cyradm-HOWTO/html/index.html).
- Postscript (ISO A4 format) (http://www.delouw.ch/linux/Postfix-Cyrus-Web-cyradm-HOWTO/Postfix-Cyrus-Web-cyradm-HOWTO.ps).
- Acrobat PDF (http://www.delouw.ch/linux/Postfix-Cyrus-Web-cyradm-HOWTO/Postfix-Cyrus-Web-cyradm-HOWTO.pdf).
- SGML Source (http://www.delouw.ch/linux/Postfix-Cyrus-Web-cyradm-HOWTO/Postfix-Cyrus-Web-cyradm-HOWTO.sgml).
- HTML gzipped tarball (http://www.delouw.ch/linux/Postfix-Cyrus-Web-cyradm-HOWTO/Postfix-Cyrus-Web-cyradm-HOWTO.tar.gz).

1.6. Credits

- Martynas Bieliauskas <`martynas at inet.lt`> submitted a good idea how to restrict the cyrus admin to localhost only.
- Michael Muenz <`m.muenz at maxonline.de`> for his help with SMTP Authentication

- Ron Wheeler `<rwheeler at artifact-software.com>` for his help with editing for readability
- The nice people at `< discuss at tldp.org>` 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 : `<luc at delouw.ch>`.

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 me as soon as I get the time.

Translations to other languages are always welcome. If you translate 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 than 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 which has a specialized function. At this point I don't what to go into details about what each program does what. If you are interested how Postfix works, 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 in conjunction with the other components of a full e-mail setup.

2.2. Cyrus IMAP

Cyrus IMAP is developed and maintained by Carnegie Mellon University.

Unlike the WU-IMAPd package, Cyrus uses its own method to store the user's mail. Each message is stored in its own file. The benefit of using separate files is improved reliability since only one message is lost if there is a filesystem error. Metadata such as the status of a message (seen, etc) is stored in a database. Additionally, the messages are indexed to improve Cyrus performance, specially with lots of users and/or lots of big emails. There is nothing else as fast as the Cyrus IMAP-server.

Another very important feature is that 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 when you have a really huge number 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 Web interfaces. This method is much more secure than a Webinterface to `/etc/passwd`.

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

Since CMU changed the license policy for Cyrus, this software is going to be used by many 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 (in this case Cyrus-IMAP) to handle authentication requests from clients.

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

2.4. OpenSSL

OpenSSL is a library needed by SASL for encryption of the data-stream. It is used by almost all opensource software that need encryption. Most or all Un*x distributions come with a pre-installed OpenSSL. Be sure to also install the appropriate devel-package. If you like, you can compile OpenSSL by yourself. This will be required if you need to fix a security hole.

2.5. MySQL Database

MySQL is a very fast, powerful and very easy to use database.

Since Cyrus can authenticate its users with pam, you can use pam_mysql as a connector to the user database stored in MySQL. This allows you to create a nice Webinterface for your users for changing passwords, defining and deleting 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. For example, tasks such as creating accounts, changing passwords and creating new aliases can be delegated to an administrator for a particular domain. At the end of the day, you, as a sysadmin, will 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 required to maintain the mail system. 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 you to my Apache-Compile-HOWTO (http://www.delouw.ch/linux/apache.phtml). 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 would like to contribute to web-cyradm, or you have a nice idea, feel free to contact the mailinglist on http://www.web-cyradm.org

The following is a partial list of features:

- Administration of multiple virtual domains
- Setting of quotas
- Automatically creating usernames, either with a defined prefix, or the domainname
- Delegation of tasks such as creating new users to »Domain Masters«
- Mapping of user-accounts to email addresses
- Forwarding of accounts to single aliases

- Vacation functions for a single aliases
- Support for SMTP Transport Tables
- Support for MySQL and PostgreSQL
- i18n (internationalization) support (including different charsets)
- Translated into 18 Languages and growing

Web-cyradm supports different roles of its users. If you plan to use it 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 Postfix.

> **Deprecated packages for Debian stable and testing:** Debian users probably want to install packages provided by Debian. Unfortunately Debian stable (Woody) and testing (sarge) are using the deprecated version of the software used in this HOWTO. I tested the respective packages from Debian unstable (sid) and the are working. Please note, that the maintainers at Debian are very conservative. The software packages »postfix-mysql«, »libsasl2« and »cyrus21-imapd« are stable, even if they are only available in the »unstable« tree.

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-4.0.18.tar.gz
```

```
cd mysql-4.0.18

./configure \
--prefix=/usr/local/mysql \
--enable-assembler \
--with-innodb \
--without-debug

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
```

To improve security, add a mysql-user on your system i.e. »mysql«, then

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

If you want 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 Unix systems.

```
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 see 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 the most recent version instead. If you already installed Berkeley DB on your Debian Box, please uninstall it to prevent conflicts.

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

> **Berkeley DB versions:** I only tested version 4.0.x versions of bdb. Please let me know if you are successful with newer versions.

3.2.1. Download Berkeley DB

Origin-Site: http://www.sleepycat.com/update/snapshot/db-4.0.14.tar.gz (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-0.9.7d.tar.gz

cd openssl-0.9.7d

./config shared
```

```
make
make test
make install

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

> **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-2.1.18.tar.gz (ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.18.tar.gz)

Origin-Site: ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-imapd-2.2.3.tar.gz (ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-imapd-2.2.3.tar.gz)

3.4.2. Create the cyrus user

On most systems there is no cyrus user and mailgroup by default. Check for a free UID, usually daemons are running with UIDs less that 100. As example I am using UID 96 which is what 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-2.1.18.tar.gz
```

```
cd cyrus-sasl-2.1.18

./configure \
--enable-anon \
--enable-plain \
--enable-login \
--disable-krb4 \
--disable-otp \
--disable-cram \
--disable-digest \
--with-saslauthd=/var/run/saslauthd \
--with-pam=/lib/security \
--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-2.2.3.tar.gz
cd cyrus-imapd-2.2.3

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 startup script. 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 -c -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 will 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
```

3.4.6. Update Cyrus IMAPd

This section describes HOWTO update the IMAPd from version 2.1.x to 2.2.x

Update is critical and can mean complete data loss

Please test this procedure on a test/pre-production server first. Also have close look to `install-upgrade.html` that comes with the cyrus-imapd distribution. Please note, that you shoud plan a downtime for the production server to have the time to solve problems. Also note, that nobody I cannot take responsibility for the update procedure provided here

Cyrus changed the format of the dbd databases used for internal storage of mailboxlist flags etc.

A convert script comes with the distribution. The most important database is `/var/imap/mailboxes.db`. Without that database cyrus-imapd will NOT run. This requires a backup. Lets do a dump and a backup of the database.

```
/etc/init.d/cyrus stop # be sure no cyrus process is running

lsof /var/imap/mailboxes.db # be sure NO process is accessing the mailbox

su - cyrus
/usr/cyrus/bin/ctl_mboxlist -d > /tmp/mailbox.db.dump
cp /var/imap/mailboxes.db /var/imap/mailboxes.db.old
```

Convert the `/var/imap/mailboxes.db`

```
/usr/cyrus/bin/cvt_cyrusdb /var/imap/mailboxes.db berkeley /var/imap/mailb
mv /var/imap/mailboxes.db.new /var/imap/mailboxes.db
```

Convert all the »seen« databases:

```
find /var/imap/user -name \*.seen -exec /usr/cyrus/bin/cvt_cyrusdb \{\} fl
```

Converting the sieve scripts

```
/usr/local/cyrus-imapd-2.2.3/tools/masssievec /usr/cyrus/bin/sievec
```

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 build and install postfix, be sure to create a »postfix« and a »postdrop« user and group if they do not exist 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 numeric UID and GID. In the following example I will use UID and GID 33333 for Postfix and 33335 for the maildrop UID and GID. These ID's correspond 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 section 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 uninstall any sendmail version from RPM based systems. I suggest that you remove sendmail, and install Postfix instead. At least SuSE RPMs need a MTA. After installing the Postfix-RPM, just install Postfix over the RPM installation by following the HOWTO.

```
tar -xvzf postfix-2.0.19.tar.gz

cd postfix-2.0.19

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 symbolic 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 installed by default on almost all Linux distributions. I am not describing how to compile PAM by yourself, because it could break your system. Instead, I will describe how to install the package.

Users of a RPM based distribution can issue the following command:

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

Debian users can install the devel package with the following command:

```
apt-get install libpam0g-dev
```

3.7. Getting and installing pam_mysql

3.7.1. Download

Origin-Site: http://sourceforge.net/projects/pam-mysql/ (http://sourceforge.net/projects/pam-mysql/)

3.7.2. Installing

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

```
cd pam_mysql
```

If you have compiled mysql by yourself, 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 you an go ahead with the pam_mysql compile.

```
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-0.5.4.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 webserver's documentroot.

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

Web-cyradm 0.5.4 is considered stable, and was released on 2003-12-05

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 4.3.4, because a lot of important bugs have been fixed.

A frequent mistake is to forget to touch the logfile and change the owner to the Apache UID. 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 several 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 required tables and populates the database with an initial admin-user and the cyrus user.

The other scripts are used for incremental upgrading from older releases.

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 attempt is always the default username and password supplied by the vendor. It is IMPORTANT that you change 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 0.5.3 to 0.5.4

In version 0.5.4 there is a small database enhancement. You can upgrade your database by issuing the MySQL script that comes with the distribution.

```
mysql mail -u mail -p < \
scripts/upgrade-0.5.3-to-0.5.4_mysql.sql
```

Since Version 0.5.3 web-cyradm has full support for DES crypted passwords. You can use the php-script `migrate.php` to convert the users passwords from plain text 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.

The easiest way is to only 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 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&
```

Restart your MySQL daemon by issuing the command**/etc/init.d/mysql.server start**

To ensure the configuration change was successful, **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 host other than the mail server. This allows you to securely connect from another host since access is allowed only from pre-defined IP addresses.

The example used is from the view of the host serving the MySQL database. Lets assume your mail server 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 attempts 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=mai

auth sufficient pam_unix_auth.so

account required pam_mysql.so user=mail passwd=secret host=localhost db=ma

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 need 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}
```

What does that change affect?

A look to the cyrus man-pages **man deliver** clears up 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 the 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, mail is delivered directly to the destination smtp host. Usually your relayhosts are your internet service provider's 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, mail should be delivered by the cyrus delivery program.

```
mailbox_transport = cyrus
```

At the end of file you need to add:

```
virtual_alias_maps = hash:/etc/postfix/virtual, mysql:/etc/postfix/mysql-v
```

If you don't want to have a overriding /etc/postfix/virtual, skip the hash entry

Outgoing addresses should be rewritten from test0002 at domain to user.name at virtualhost.com. This is important if you want 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
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
# 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_mynetwork
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
broken_sasl_auth_clients = yes
```

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

```
pwcheck_method: saslauthd
```

The next step is to tell postfix how to find the saslauthd socket:

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

6.3. Fighting against SPAM

This section describes how to implement a basic SPAM protection setup with postfix. It does not use any external software like spamassassin, etc.

Postfix has some built-in filters that allow you to stop obvious SPAM attempts. In particular these are:

- smtpd_helo_required = yes

  This switch in `main.cf` means that SMTP clients connecting to your mail server must give a »helo« when connecting.

- smtpd_recipient_restrictions

This option in `main.cf` lets you define different rules on the handling the acceptance of mail. The following example simply rejects all invalid sender and recipient data. Additionally it defines how to lookup known spammers from online blacklists.

```
smtpd_recipient_restrictions =
            reject_invalid_hostname,
            reject_non_fqdn_hostname,
            reject_non_fqdn_sender,
            reject_non_fqdn_recipient,
            reject_unknown_sender_domain,
            reject_unknown_recipient_domain,
            reject_unauth_pipelining,
            permit_mynetworks,
            reject_unauth_destination,
            reject_rbl_client zombie.dnsbl.sorbs.net,
            reject_rbl_client relays.ordb.org,
            reject_rbl_client opm.blitzed.org,
            reject_rbl_client list.dsbl.org,
            reject_rbl_client sbl.spamhaus.org,
            permit
```

- mime_header_checks=pcre:/etc/postfix/body_checks

  MIME header checks let you reject mail which contains malicious MIME content, i.e dangerous attachments such as Windows executables. Create the file `/etc/postfix/body_checks`. The following example rejects all mail that contains potentially dangerous attachments. In my experience, using this example would filter out most of viruses delivered by e-mail. In any event, a virus scanner should always be installed.

  ```
   /^((Content-(Disposition: attachment;|Type:).*|\ +)| *)(file)?name\ *=\
  ```

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`

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.

```
postmaster: postmaster
configdirectory: /var/imap
partition-default: /var/spool/imap
# admins: cyrus # no admins!
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
```

7.1.3. `/etc/imapd-local.conf`

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.

This second file ensures, that admin users only can connect via localhost. Decide by yourself if this additional security feature is needed for your site.

```
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
```

7.1.4. 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
```

7.1.5. `/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="192.168.0.1:imap" prefork=0
  imaplocal     cmd="imapd -C /etc/imapd-local.conf" listen="127.0.0.1:ima
  imaps         cmd="imapd -s" listen="192.168.0.1:imaps" prefork=0
  imapslocal    cmd="imapd -C /etc/imapd-local.conf" listen="127.0.0.1:ima
  pop3          cmd="pop3d" listen="pop3" prefork=0
  pop3s         cmd="pop3d -s" listen="pop3s" prefork=0
  sieve         cmd="timsieved" listen="192.168.0.1:sieve" prefork=0
  sievelocal    cmd="timsieved -C /etc/imapd-local.conf listen="127.0.0.1:

  # 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"
}

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
}
```

Please check your Systems IP address: In the example above the IP 192.168.0.1 is to be replaced with your systems external IP address.

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 distribution's config file, and create the logfile. The logfile must be owned by the user that runs the webserver. This is usually the user »nobody« or »wwwrun«.

```
cd /usr/local/apache/htdocs/web-cyradm/config

cp conf.php.dist conf.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 = array(
        'HOST'  => 'localhost',
```

```
        'PORT'  => 143,
        'ADMIN' => 'cyrus',
        'PASS'  => '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 would like to have web-cyradm on a different server from the server running cyrus-imapd ..

8.2. Database setup

Since version 0.5.2 web-cyradm uses PEAR as a database abstraction layer. This adds more flexibility. MySQL and PostgreSQL are currently supported. Please note that a patch is required for PostgreSQL because Postfix does not support PostgreSQL natively. I strongly suggest that you use MySQL. I know MySQL has some restrictions on transactions and stuff, but it is supported in the distributed Postfix code.

The entries should be self explanatory

```
$DB = array(
        'TYPE'  => 'mysql',
        'USER'  => 'mail',
        'PASS'  => 'secret',
        'PROTO' => 'unix',      // set to "tcp" for TCP/IP
        'HOST'  => 'localhost',
        'NAME'  => 'mail'
);
```

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 encrypted passwords. I strongly suggest the use of encryption. There are three methods supported at the moment: Unix-compatible (crypt), md5 and MySQL. The Unix-compatible encryption allows you to import encrypted passwords from an existing `/etc/shadow`. This is the preferred option.

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 only works 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 constraints?)

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 encryption 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, it is used for all passwords, including the password of the admin users. I STRONGLY suggest the use of Unix Shadow compatible encryption, because it makes you independent of any software vendor.

8.5. Usernames

There are two username schemes 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 Section 7.1.2

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: testing at example.com
250 Ok
rcpt to: tester 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: tester at localhost
451 <tester  at localhost>: Temporary lookup failure
```

Then either 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.

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 m
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. Fighting against Viruses and SPAM

This chapter is optional and describes HOWTO fight against Viruses and SPAM.

10.1. Brief introdcution to viruses

I think I do not need to explain how dangerous Viruses are. Unfortunately in the most recent attacks from SCO.A (aka MyDoom) also more or less experienced users get tricked by viruses. Most of todays viruses and worms comes via the internet, most of them via E-Mail. Needless to say, that viruses should be catched by the SMTP system if possible.

Not a substitute

A mailsystem that filters viruses is NEVER a substitute for a local installed anti-virus software. E-Mails are only one way how viruses can penetrate computers.

10.2. Brief introduction to SPAM

The other harmless but unwanted and disturbing E-Mails are SPAM e-mails. SPAM is originally a disgusting canned meat. It is a synonym for UCE (Unsolicited Commercial Email) and UBE (Unsolicited Bulk Email).

Studies claim, that up to 60 percent of the worldwide e-mail traffic is SPAM. Before I installed the anti-SPAM filters on my SMTP servers, I received about 150 SPAMS's a day. One reason is this document. In ancient time, I noticed my real e-mail address unprotected. E-mail harvesters are scanning websites allover the world for addresses, and try to deliver its commercial, often illegal offers.

10.3. Strategy against viruses

The strategy against viruses is pretty forward: Filtering viruses delivered via e-mail and having a localally installed anti-virus software.

Almost all vendors of anti-virus software have a up-to-date version for Linux and Unix Systems, because most SMTP servers are running on Unix. In this document I'll explain HOWTO implement clamav (http://www.clamav.net), a very active open source anti virus project.

10.4. Strategy against SPAM

Fighting against SPAM is much more difficult than viruses. Why? It is because every virus has a unique signature. SPAM can contain arbitrary content. Some of the SPAM is in english, other is korean, other is in "you-name-it-language".

The best method how to prevent SPAM is to handle your e-mail address as your best treasured secret. NEVER put your address in a web-form or put it on your website. I know, that is against the idea of the internet. Information must be free. You can keep publishing your e-mail address if you implement the configuration further below.

In the beginning of SPAM, filtering for keywords like »viagra« was enough. Todays SPAM techniques are much more sophisticated. It is a war between users and spammers. The solution against sophisticated SPAM is even more sophisticated anti-spam software.Todays anti-spam software checks e-mail for more than just keywords. They are checking for specific mail-header data etc. Also a technique called bayesian (http://en.wikipedia.org/wiki/Epistemic_probability) filters which can learn from particular input, distributed checksum networks etc.

11. The software needed against viruses and SPAM

This chapter describes how to install and handle the software against viruses and SPAM

11.1. Getting and installing ClamAV

11.1.1. Download

Origin-Site: http://prdownloads.sourceforge.net/clamav/clamav-0.68.tar.gz

11.1.2. Building and installing

```
# Adding a group for the clamav user
groupadd clamav

# Adding the clamav user to your system
useradd -g clamav -c "clamav user" clamav

cd /usr/local

tar -xvzf clamav-0.68.tar.gz
cd clamav-0.68

./configure

make && make install
```

11.1.3. Testing and configuring

To test the funtionality of clamav, you can run **clamscan** to get some results from the testpatterns that are included in the clamav distribution run **clamscan -r -i /usr/local/clamav-0.68**

The output should look like this:

```
/usr/local/clamav-0.68/test/test1: ClamAV-Test-Signature FOUND
/usr/local/clamav-0.68/test/test1.bz2: ClamAV-Test-Signature FOUND
/usr/local/clamav-0.68/test/test2.zip: ClamAV-Test-Signature FOUND
/usr/local/clamav-0.68/test/test2.badext: ClamAV-Test-Signature FOUND
/usr/local/clamav-0.68/contrib/clamdwatch/clamdwatch.tar.gz: Eicar-Test-Si
```

```
----------- SCAN SUMMARY -----------
Known viruses: 20482
Scanned directories: 47
Scanned files: 406
Infected files: 5
Data scanned: 5.48 MB
I/O buffer size: 131072 bytes
Time: 2.706 sec (0 m 2 s)
```

Next step is to setup the automated update of the virus database. This is a important step, because the speed of virus spreading is fast and would pick up even further.

Create the needed logfiles

```
touch /var/log/clam-update.log
chmod 600 /var/log/clam-update.log
chown clamav /var/log/clam-update.log
```

I suggest to update the signatures with a hourly cronjob. To edit the crontab issue **crontab -e** and add the following line, and replace the »x« with a random value between 1 and 59. This is some kind of time based loadbalancing to ensure more people can fetch the updated.

```
#x * * * *       /usr/local/bin/freshclam --quiet -l /var/log/clam-update.
```

To test if the update process is working, please issue the command **/usr/local/bin/freshclam -l /var/log/clam-update.log** and have a look at the output.

The output should look similar to this:

```
ClamAV update process started at Tue Mar 23 19:58:11 2004
Reading CVD header (main.cvd): OK
Downloading main.cvd [*]
main.cvd updated (version: 21, sigs: 20094, f-level: 1, builder: tkojm)
Reading CVD header (daily.cvd): OK
Downloading daily.cvd [*]
daily.cvd updated (version: 210, sigs: 596, f-level: 1, builder: acab)
Database updated (20690 signatures) from database.clamav.net (64.74.124.90
```

11.2. Razor

Razor is one of the prerequisites of spamassassin.

11.2.1. Download

Origin-Site: http://prdownloads.sourceforge.net/razor/razor-agents-sdk-2.03.tar.gz?download

Origin-Site: http://prdownloads.sourceforge.net/razor/razor-agents-2.40.tar.gz?download

```
cd /usr/local

tar -xvzf razor-agents-sdk-2.03.tar.gz
cd razor-agents-sdk-2.03

perl Makefile.PL
make && make install

cd /usr/local
tar -xvzf razor-agents-2.40.tar.gz
cd razor-agents-2.40/

perl Makefile.PL
make && make install
```

11.2.2. Registering and setting up

In order to use razor2 you need to register yourself as a user

Choose a unique username and password and issue **razor-admin -register -user=some_user -pass=somepass**

11.3. Getting and installing spamassassin

Spamassassin is the todays leading opensource project to fight against SPAM. To describe how spamassassin works would be too much for this document. For further information please consult http://eu.spamassassin.org/doc.html

11.3.1. Download

Origin-Site: http://eu.spamassassin.org/released/Mail-SpamAssassin-2.63.tar.gz

11.3.2. Prerequisites

Spamassassin depends on a lot of prerequisites. The easiest way is using the CPAN repository. Issue the command **perl -MCPAN -e shell** and answer all questions as needed.

11.3.3. Building and installing

```
cd /usr/local

tar -xvzf Mail-SpamAssassin-2.63.tar.gz

cd Mail-SpamAssassin-2.63

perl Makefile.PL

# You get prompted to run Razor tests which you should answer with "y"
Run Razor v2 tests (these may fail due to network problems)? (y/n) [n] y

make && make install
```

11.4. Getting and installing amavisd-new

Amavisd-new is the software that glues all the software described above together to postfix

11.4.1. Download

Origin-Site: http://www.ijs.si/software/amavisd/amavisd-new-20030616-p8.tar.gz

11.4.2. Prerequisites

Amavisd-new needs a lot of prerequisites.

Run **perl -MCPAN -e shell** and issue:

```
install ExtUtils::MakeMaker
install HTML::Parser
install DB_File
install Digest::SHA1
install Archive::Tar
install Archive::Zip
install Compress::Zlib
```

```
install Convert::TNEF
install Convert::UUlib
install MIME::Base64
install MIME::Parser
install Mail::Internet
install Mail::SPF::Query
install Net::Server
install Net::SMTP
install Net::DNS
install Digest::MD5
install IO::Stringy
install Time::HiRes
install Unix::Syslog
```

At the end run **./amavisd** and have a look at overseen prerequisites.

Edit `/etc/amavisd.conf` and change the variables `$daemon_user` to »amavis« and `$daemon_group` to »amavis«. Another variable to change is `$mydomain to match your domain.`

Please also consider to change the default settings for virus and spam mails to avoid being notified about every intercepted mail

```
$final_virus_destiny      = D_DISCARD;  # (defaults to D_BOUNCE)
$final_spam_destiny       = D_DISCARD;  # (defaults to D_REJECT)
```

In the beginning of SPAM filtering I recommend to set the kill-value to something higher until you tweaked the filters. Change the variable `$sa_kill_level_deflt` to 8 or even higher.

11.4.3. Building and installing

```
cd /usr/local

tar -xvzf amavisd-new-20030616-p8.tar.gz

cd amavisd-new-20030616
cp amavisd /usr/local/sbin
cp amavisd.conf /etc
chown root /etc/amavisd.conf
chmod 644  /etc/amavisd.conf
```

Now it is the the time to define a group and a user for amavisd-new

```
groupadd amavis
useradd -g amavis -c "Amavisd-new user" amavis
```

Next you have to define a directory for the quarantined mail:

```
mkdir /var/virusmails
chown amavis:amavis /var/virusmails
chmod 750 /var/virusmails
mkdir /var/amavis
chown amavis:amavis /var/amavis
chmod 750 /var/amavis
```

The original init script in the amavisd-new distribution does only work work with Redhat. Other distributions need to install my quick and dirty init-script:

```
#!/bin/bash
#
# Amavisd-new startup script

case "$1" in
    start)
        # Starting amavisd
        /usr/local/sbin/amavisd
        ;;

    stop)

 # follows later

        ;;

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

esac
```

11.5. Setting up postfix

Postfix needs to be configured to send each mail to amavis-new in order to get sanitized.

You need to add the following line to `/etc/postfix/main.cf`

```
content_filter = smtp-amavis:127.0.0.1:10024
```

The `/etc/postfix/master.cf` needs also some adjustments to return the results from amavisd-new to the mailingsystem.

Please add the following lines to your configuration:

```
smtp-amavis unix - - y - 2 smtp -o smtp_data_done_timeout=1200

127.0.0.1:10025 inet n  -       n       -       -  smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
```

12. Further Information

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

12.1. News groups

Some of the most interesting news groups are:

- alt.comp.mail.postfix (news:alt.comp.mail.postfix)

  This is low traffic group.

- comp.mail.imap (news: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 (ftp://rtfm.mit.edu/). The WWW versions can be browsed at the FAQ main archive WWW site (http://www.cis.ohio-state.edu/hypertext/faq/usenet/FAQ-List.html).

12.2. Mailing Lists

12.2.1. `<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
(http://www.deja.com/group/mailing.postfix.users)

12.2.2. `<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
(http://asg.web.cmu.edu/archive/index.php?mailbox=archive.info-cyrus)

12.2.3. `<web-cyradm at web-cyradm.org>`

Subscription can be done trough the webinterface
http://www.web-cyradm.org/mailman/listinfo/web-cyradm
(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/
(http://www.web-cyradm.org/pipermail/web-cyradm/)

12.3. 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 (http://www.tldp.org/HOWTO/Cyrus-IMAP.html)` and `Apache-Compile-HOWTO` `(http://www.tldp.org/HOWTO/Apache-Compile-HOWTO/index.html)`. The main site for these is the LDP archive (http://www.tldp.org/).

12.4. Ebooks

There a few other HOWTOs and freely available documentations outside of the TLDP.org

IBM recently released a new Redbook: `BladeCenter, Linux, and Open Source: Blueprint for e-business on demand (http://www.redbooks.ibm.com/redbooks/pdfs/sg247034.pdf)`. Especially chapter 6 is interesting when looking for email solutions.

12.5. 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-2.0.16/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.

12.6. 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 (http://www.tldp.org/) home page, an information central for documentation, project pages and much more.

To get more deepened information about Postfix, then www.postfix.org (http://www.postfix.org) would be the starting point.

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

13. 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

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`

1.2. Messages are bouncing. Postfix/pipe complains that "Mailbox does not exist". Whats wrong?

Check that the cyrus login on web-cyradm (config.inc.php) is correct. The username and password must exist in MySQL on table accountuser. Web-cyradm will not complain if the cyrus login info is incorrect.

1.3. 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

1.4. 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 enough rights to access the database and tables.

1.5. 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.

1.6. 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)

1.7. 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.

1.8. For what platforms does this HOWTO work?

It is primarily for Linux. Until now I only tested it on Linux/IA32. Most probably it will also work on other architectures. FreeBSD is reported working fine. AIX has problems with at least PHP. Please report if you got it running on other platform, so I can update this section.