

ADVANCED E-MAIL SYSTEM - COMPLETE SOLUTION

Remus BRAD, associate professor, Ph.D., “Lucian Blaga” University of Sibiu, Romania
Valentin LUP, system administrator, “Lucian Blaga” University of Sibiu, Romania
Zeno POPOVICI, system administrator, “Lucian Blaga” University of Sibiu, Romania

Abstract.

The paper summarizes the implementation of a complete e-mail system, on a UNIX platform, based on virtual users. The virtual users system presented has many advantages compared to the classic system, which is still widely spread and is based on real UNIX accounts. This article also approaches the long-term viability, flexibility and performances of such a solution. Implementation has been done on a Red Hat 9 platform, using the Postfix MTA. Courier IMAP was used for IMAP and POP3 services, MYSQL for user data storage and Courier MailDrop as Local Delivery Agent and filter control. Additionally the Spam Assassin module was integrated into MailDrop for better Spam processing. For virus checking, we chose a different approach (not open source) and integrated the Softwin’s Bit Defender Antivirus. Results and performance statistics of the system have been included in the conclusions section.

1. Introduction

One of the most important components in an institution's network is the e-mail server. On the other hand, it presents one of the biggest security problems of that network, being the target of spam, virus and many other types of attacks. This paper presents one solution for such a server, solution that we have tried to implement with minimal costs and a maximum in efficiency.

2. Objectives and Assumptions

When our University first offered its own e-mail system, this was achieved by installing the sendmail system on every Linux server in every faculty or department, without an antivirus program or Spam protection. But as time passed this proved an inefficient and time consuming endeavor, given the increasing number of spam e-mail that had to be filtered separately on every system. This is why it has been decided to unify the mail server into a single system and the newer,

more superior postfix module replaced the older sendmail. But this also proved unsatisfying due to the great increase in mail users in our University.

This led to the creation of a newer system, based on an SQL database for mail users data storage, thus eliminating the problem of hundreds of real users on the server, also giving us almost unlimited users and domains management capacity.

3. System Architecture

The following packages have been installed on a system based on RED HAT Linux 9.0 edition:

- MySQL 4.0.18-0 - Client, Server, Devel and Shared RPMs (user data storage)
- Postfix 2.1.5 - source tarball (MTA)
- BitDefender 1.6.11 - RPM (Anti-virus Software)
- Courier MailDrop 1.8.0 - source tarball (MDA)
- SpamAssassin 3.0.2 - RPM (Spam Filtering Software)
- § Razor Agents 2.6.7 - source tarball (Spam Detection Filtering Network Agents)
- Courier IMAP 4.0.2 - source tarball (IMAP/POP3 server with SSL & TLS support)
- Cyrus SASL 2.1.18 - source tarball (SMTP authentication)
- ProFTPD 1.3.0 – source tarball (Optional)

We will assume you have properly installed the MYSQL server. This is done by running the command:

```
$ rpm -ivh *.rpm
```

You now need to create a new MSQL user and a database for the tables that will be used by Postfix, Cyrus SASL and Courier IMAP and ProFTPD (Optional). This user must have full permissions on this database. We will assume the MSQL user name is „ccomadmin”, database name „ccomusers” and table name is „users”. We now need to create the required tables in our new database and create the necessary MYSQL map files for postfix.

```
CREATE TABLE `users` (  
  `UserID` varchar(6) NOT NULL default '',  
  `FirstName` varchar(255) NOT NULL default '',  
  `LastName` varchar(255) NOT NULL default '',  
  `DepOrgName` varchar(50) default NULL,  
  `FTPSDir` varchar(255) default '/home/ftphome/users/',  
  `MailUsername` varchar(255) NOT NULL default '@ulbsibiu.ro',  
  `MailPassword` varchar(255) NOT NULL default '',  
  `MailDir` varchar(255) NOT NULL default 'ulbsibiu.ro/',  
  `DomainName` varchar(255) NOT NULL default 'ulbsibiu.ro',  
  `MailAlias` varchar(255) default NULL,
```

```

`MailForward` text,
`MailQuota` enum('0','1','204800','20971520','41943040','104857600') NOT NULL default '41943040',
  PRIMARY KEY (`UserID`),
  UNIQUE KEY `username_2` (`MailUsername`),
  UNIQUE KEY `UserID` (`UserID`),
) TYPE=MyISAM COMMENT='Mail/FTP Users';

```

The postfix file must also be edited accordingly. Transport map example:

```

$ vi /etc/postfix/maps/mysql_transport_maps.conf
hosts = localhost
user = ccomadmin
password = *****
dbname = ccomusers
table = maildomain
select_field = Destination
where_field = Domain

```

3.1. Authentication Layer

After installing the MySQL components, we need to set up the Cyrus SASL package. We are using SASL for SMTP relay authentication.

The parameters used for compiling this package:

```

$ export CPPFLAGS="-I/usr/include/mysql"
$ export LDFLAGS="-L/usr/lib/mysql -lmysqlclient -lz -lm"
$ ./configure --enable-anon --enable-plain --enable-login --enable-sql
  --disable-krb4 --disable-otp --disable-cram --disable-digest
  --with-mysql=/usr/lib/mysql --without-pam --without-saslauthd
  --without-pwcheck --with-openssl=/usr/local/ssl
  --with-pluginindir=/usr/local/lib/sasl2

```

Check to make sure that the path /usr/local/lib is in /etc/ld.so.conf. If it is not, append that path to the file and run ldconfig (as root). We now need to tell Cyrus SASL to use a MySQL database for authentication and which table contains the authentication details.

```

$ vi /usr/local/lib/sasl2/smtpd.conf

pwcheck_method: auxprop
auxprop_plugin: sql
sql_engine: mysql
mech_list: sql plain login
sql_hostnames: localhost
sql_user: ccomadmin
sql_passwd: *****
sql_database: ccomusers
sql_statement: SELECT clear FROM users WHERE MailUsername = '%u@%r'
sql_verbose: yes

```

3.2. The Mail System

Next comes the installation of the POSTFIX module. The install process is realized by compiling several needed options into the latest package offers by the producer. This is followed by the creation of "postfix" user and the "postdrop" group and by the final building of the module:

```

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

```

We now need to configure Postfix to use MySQL. We will be editing the `/etc/postfix/main.cf` file and also creating a series of MySQL specific `.cf` files that are used to connect to the MySQL tables.

```
$ vi /etc/postfix/mysql/mysql_client_access.cf
hosts = localhost
user = ccomadmin
password = *****
dbname = ccomusers
table = users
select_field = MailUsername
where_field = MailEnabled
additional_conditions = and MailEnabled = 'Y'
```

You will now need to create an user, group and the directory where email for virtual users will be stored. This is the only real user created on this system and it is used by all systems to access user mailboxes and personal storage. We will assume this users and group are called "vmail". This user will have a "502" GID and UID. Please note that the UID and GID has to be the same in all configuration files!

3.3. The IMAP/POP3 Services

Courier IMAP is the next to be installed, also using and building the program's sources. This is done because of the number of parameters that have to be passed to this module. Courier-IMAP is a fast, scalable enterprise IMAP server that uses MailDir. MailDir is superior to single file storage (mail spools) in speed and structure management of the user's mailbox. Many e-mail service providers use Courier-IMAP to easy handle hundreds of thousands of mail accounts.

```
<as non root user>
$~ ./configure
--prefix=/usr/local/courier --with-authmysql --with-mysql-libs=/usr/lib/mysql
--with-mysql-includes=/usr/include/mysql --with-redhat
--enable-workarounds-for-imap-client-bugs --enable-unicode --with-trashquota
--with-redhat
$~ make

<as root>
$ make install
$ make install-configure
```

It is very important to do the configure part as a non-root user. The `/usr/local/courier/bin/` contains the IMAP and POP init.d scripts that have to be copied into their correct location:

```
$ cp /usr/local/courier/libexec/imapd.rc /etc/init.d/imapd
$ cp /usr/local/courier/libexec/pop3d.rc /etc/init.d/ipop3d
$ cp /usr/local/courier/libexec/imapd-ssl.rc /etc/init.d/imapd-ssl
$ cp /usr/local/courier/libexec/pop3d-ssl.rc /etc/init.d/pop3d-ssl
$ cp /usr/local/courier/libexec/authlib/authdaemond /etc/init.d/authdaemond
$ chmod 700 /etc/init.d/imapd
$ chmod 700 /etc/init.d/ipop3d
```

We now need to tell Courier IMAP to use a MySQL database for authentication and which table contains the authentication details.

```
$ vi /usr/local/courier/etc/authdaemonrc
```

```
authmodulelist="authmysql authpam"
```

```
$ vi /usr/local/courier/etc/authmysqlrc
```

```
MYSQL_SERVER                localhost
MYSQL_UID_FIELD             '502'
MYSQL_USERNAME              ccomadmin
MYSQL_PASSWORD              *****
MYSQL_DATABASE              ccomusers
MYSQL_USER_TABLE            users
DEFAULT_DOMAIN              ulbsibiu.ro
MYSQL_CLEAR_PWFIELD         MailPassword
MYSQL_GID_FIELD             '502'
MYSQL_HOME_FIELD            '/home/vmail/'
MYSQL_LOGIN_FIELD           MailUsername
MYSQL_MAILDIR_FIELD         MailDir
MYSQL_NAME_FIELD            CONCAT(FirstName, ' ', LastName)
MYSQL_OPT                   0
MYSQL_QUOTA_FIELD           MailQuota
MYSQL_AUXOPTIONS_FIELD      CONCAT("disableimap=", IMAPDisabled, ",disablepop3=", POP3Disabled, ",disablewebmail=", '0', ",sharedgroup=", '0')
MYSQL_WHERE_CLAUSE          MailEnabled='Y'
```

3.4. The Delivery Agent

We got to the MailDrop system needed by the solution. Maildrop is the mail filter/mail delivery agent that's used by the **Courier Mail Server**. Maildrop is a replacement for your local mail delivery agent. It reads a mail message from standard input, then delivers the message to your mailbox.

MailDrop optionally reads instructions from a file, which describe how to filter incoming mail. These instructions can direct maildrop to deliver the message to an alternate mailbox, or forward it somewhere else.

```
$export CPPFLAGS="-I/usr/include/mysql"
$export LDFLAGS="-L/usr/lib/mysql"
$./configure
    --prefix=/usr/local/courier
    --enable-maildirquota
    --enable-maildropmysql
    --with-mysqlconfig=/usr/local/courier/etc/maildropmysql.config
    --enable-maildrop-uid=502
    --enable-maildrop-gid=502
    --with-trashquota
$make
$make install
```

We will now need to set up the configuration file.

```
$ vi /usr/local/courier/etc/maildropmysql.config
hostname                localhost

port                   3306
database               ccomusers
dbuser                 ccomadmin
dbpw                   adminpower
dbtable                users
default_uidnumber      502
default_gidnumber      502
uid_field              MailUsername
uidnumber_field        502
gidnumber_field        502
maildir_field          MailDir
homedirectory_field    '/home/vmail/'
```

```
quota_field      MailQuota
mailstatus_field MailEnabled
where_clause     AND MailEnabled = 'Y'
```

The filter rules file for Spam delivery and user mailbox creation must be edited here:

```
$vi /etc/maildroprc
```

3.5. Testing the Installation

After a series of tests fine tuning can be done to the system in order to achieve maximum performance and accessibility. System has been configured to host 3 domains and has a pool of 600 users.

4. Conclusions

To ensure a better protection of the system, besides all these filtering modules the linux server version of the Bitdefender Antivirus has been installed. A system configured in this manner is very easy to manage, and in case of a problem, it can be rebuilt and restarted in less than an hour, provided the user database has been previously backed up. Also, this being a system built upon an SQL database, new users can be easily added, groups can be created, mailboxes can be shrunk or enlarged as needed and also aliases for the users can be created (because we use a standard "name.surname" when creating users).

Another positive aspect of the system would be the reutilisation of its database. For example, in our network structure, web pages belonging to different faculties are kept up to date by members of those particular faculties, by means of an FTP account. Authentication for these accounts (on the WWW server, a different system from the MAIL server) is done through the same user database. The costs of building such a system (besides the cost of the system and of the antivirus program) is ZERO!

The mail system presently running at the LBUS is based on the architecture described here, having over 600 users, and offering POP/IMAP and Web access. For our web interface the Squirrel Mail was used, but modified to suit our users' needs. We provide a Webdisk interface, an online Calendar, Bookmarks storage and more.

5. References

[1]