The Postfix-Cyrus-Sasl-Auxprop-MySQL-Web-Cyradm FQUN Howto with Virtual Domain Support on Fedora Core Three

Amin Astaneh

October 9, 2005

Contents

1 Revisions

```
1.0.4
Formatted in LaTex (to be later converted to DocBook)

1.0.3
Added information regarding exclusivity of Fedora repositories 08/29/05

1.0.2
Added a postfix lookup for mail forwarding as configured in web-cyradm (table virtual)
Added chkconfig entries for mail daemons
Added simple test protocols for pop3, imap, and smtp services
Added appendix, including Michael Hsu's PHP patch 8-12-05

1.0.1.1
Corrected errors related to crypt call in incorrect position

1.0.1
Rewrite for TLDP

1.0.0
Initial Release (6-7-2005)
```

2 Introduction

This howto is a variant of the Original HOW-TO by Luc Delouw (http://www.tldp.org/HOWTO/Postfix-Cyrus-Web-Cyradm-HOWTO/), such that the authentication method, the mailbox name format, the manner of database entry, and manner of Cyrus delivery vary from the original howto. The main purpose of this change is to adapt the original inplementation for the application to multi-domain mail services for web-hosting on the same mail

system, as well as making the authentication mechanism more user-friendly (no longer need to login as "user001" instead of actual mail address). This HOWTO also is related to Morpheus' Guide for the original How-to for Fedora Core Three.
(http://www.totalinfosecurity.com/howto/t1.html)

3 Installing the Software

3.1 Install Fedora Core Three

3.2 SELinux

If you choose to enable SELinux for security purposes (recommended), it is necessary to execute this command on the apache document root so that apache will serve the web-cyradm interface to users.

```
chcon -R -t httpd_sys_content_t /var/www/html
```

3.3 Installing the Packages

List of packages to install (via yum, apt-get, etc):
NOTE*: Ensure that these packages (when available) are downloaded from the Redhat Fedora Core 3 Linux repositories if you are enabling SELinux. If not, you are risking the chance of having improper file security contexts and certain programs will malfunction as a result (Cyrus-Imapd, for example, will not have access to write to it's own database).

```
cyrus-imapd
cyrus-imapd-devel
cyrus-imapd-utils
cyrus-sasl-devel
cyrus-sasl
cyrus-sasl-md5
cyrus-sasl-gssapi
perl-cyrus
perl-Date-Calc
cyrus-sasl-sql
mysql
mysql-server
mysql-devel
php
php-mysql
httpd
db4
db4-devel
```

(The cyrus packages will have same version numbers, cyrus-sasl packages will also have the same version numbers)

3.4 Building Postfix

The Postfix .rpm binaries do not come with mysql support enabled- therefore you must compile your own. Download the Postfix SRPM and build the packages this way:

```
rpm -ivh postfix-2.1.5-2.4.FC3.src.rpm
cd /usr/src/redhat/SPECS
```

Fire up your favorite text editor and edit postfix.spec
Change the line from:

```
%define MYSQL 0
```

to:

```
%define MYSQL 1
```

Exit editor, then:

```
cd ../
rpmbuild -ba SPEC/postfix.spec
```

(that'll take a while to finish compiling)

```
cd RPMS/i386
```

Then, install the RPMs:

```
rpm -Uvh postfix-2.1.5-2.4.FC3.i386.rpm --replacefiles
rpm -Uvh postfix-debuginfo-2.1.5-2.4.FC3.i386.rpm --replacefiles
rpm -Uvh postfix-pflogsumm-2.1.5-2.4.FC3.i386.rpm --replacefiles
```

3.5 Installing Web-Cyradm (Currently 0.5.4)

Get the latest release (http://www.web-cyradm.org) Extract these files into the /var/www/html/ directory(as root)-

```
cd /var/www/html/
tar -xvzf /path/to/web-cyradm.tar.gz
mv <name of directory> web-cyradm
```

Then download and install the Web-Cyradm FQUN patch (By Michael Hsu, cheeto (at) shaolinux.org) (This patch will enable our FQUN feature to be enabled in Web-Cyradm.)

```
cd /var/www/html/web-cyradm
patch -b --verbose change_password.php /path/to/patch.diff
```

The patch program will ask for the following file to patch, so enter:

```
/var/www/html/web-cyradm/config/conf.php.dist
```

The patch will finish, and then copy to active config file:

```
cp conf.php.dist conf.php
```

3.6 Ensuring Daemons Run On Startup

Execute these commands in the shell to make daemons run at startup.

```
chkconfig --level 2345 postfix on
chkconfig --level 2345 cyrus-imapd on
chkconfig --level 2345 httpd on
chkconfig --level 2345 mysqld on
```

4 Configuring the Software

4.1 Create the MySQL Databases and tables

4.1.1 /var/www/html/web-cyradm/scripts/create-mysql.sql

There are two reasons to change this script. First is to specify passwords for the Web-Cyradm admin user and the cyrus user. Secondly is that we are using plaintext passwords.
These two lines on the bottom of the file must be changed from this:

```
INSERT INTO adminuser (username, password) VALUES ('admin', CRYPT('test'));
INSERT INTO accountuser (username, password) VALUES ('cyrus', CRYPT('secret'));
```

to this:

```
INSERT INTO adminuser (username, password) VALUES ('admin', '<whatever you wish>');
INSERT INTO accountuser (username, password) VALUES ('cyrus', '<whatever you wish>');
```

You will need to remember these passwords since you will be logging into web-cyradm with the admin user and will be putting the cyrus username and password in the configuration files.

4.1.2 /var/www/html/web-cyradm/scripts/insertuser-mysql.sql

Define the password for mysql user mail by changing line 2 from:

```
INSERT INTO user (Host, User, Password, Select_priv, Insert_priv, Update_priv,
Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv,
File_priv, Grant_priv, References_priv, Index_priv, Alter_priv) VALUES
('localhost', 'mail', PASSWORD('secret'), 'N','N', ...
```

to:

```
INSERT INTO user (Host, User, Password, Select_priv, Insert_priv, Update_priv,
Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv,
File_priv, Grant_priv, References_priv, Index_priv, Alter_priv) VALUES
('localhost', 'mail', PASSWORD('<specify mail password>)', 'N', 'N', ...
```

You will also need to remember the password you set for user mail.

4.1.3 Executing the Scripts

```
/"pathtomysql"/mysql -u root -p < \
/var/www/html/web-cyradm/scripts/insert_user_mysql.sql
```

(type in mysql root password, if any)
Then:

```
/pathtomysql/mysql mail -u mail -p < \
/var/www/html/web-cyradm/scripts/create_mysql.sql
```

(enter password for mail database)

4.2 Postfix

4.2.1 /etc/postfix/master.cf

Only one line to edit:
The line corresponding for cyrus- change from:

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

to:

```
user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -r ${sender} -m ${extension} ${user}
```

4.2.2 /etc/postfix/main.cf

The Postfix configuration has 300+ parameters. You are responsible to configure
Postfix specifically for your needs. Here are the REQUIRED parameters:

```
mydestination = your.host.name, localhost.$mydomain,
mysql:/etc/postfix/mysql-mydestination.cf
mailbox_transport = lmtp:unix:/var/lib/imap/socket/lmtp
virtual_alias_maps = hash:/etc/postfix/virtual, mysql:/etc/postfix/mysql-forward.cf,
                     mysql:/etc/postfix/mysql-virtual.cf
```

Here is the recommended SMTP SASL configuration:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = your.host.name
broken_sasl_auth_clients = yes

smtpd_recipient_restrictions =
permit_mynetworks,
  permit_sasl_authenticated,
reject_maps_rbl,
permit_auth_destination,
reject
```

```
maps_rbl_domains =
relays.ordb.org,
  dnsbl.sorbs.net
```

(merely examples, you can choose as many DNS blacklists you want)
Here is a sample UCE configuration:

```
smtpd_banner= $myhostname NO UCE
smtpd_helo_required = yes
disable_verify_command = yes

smtpd_client_restrictions =
  permit_sasl_authenticated,
reject_rbl_client dnsbl.sorbs.net,
  allow
```

4.2.3 /etc/postfix/mysql-mydestination.cf

Create this file as root, and insert these lines. Brackets indicate server-specific information.

```
# 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 = <mysql ip>
user = mail
password = <the mysql user mail's password>
# the database name on the servers
dbname = mail

# the table name
table = domain
#
select_field = domain_name
where_field = domain_name
```

4.2.4 /etc/postfix/mysql-virtual.cf

Create this file as root, and insert these lines. Brackets indicate server-specific information.

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

```
# the user name and password to log into the mysql server
hosts = <mysql ip>
user = mail
password = <the mysql user mail's password>

# the database name on the servers
dbname = mail

# the table name
table = accountuser

#
select_field = username
where_field = username
```

4.2.5 /usr/lib/sasl2/smtpd.conf

Create this file as root, and insert these lines. Brackets indicate server-specific information.

```
pwcheck_method: auxprop
auxprop_plugin: sql
mech_list: PLAIN LOGIN
sql_engine: mysql
sql_user: mail
sql_passwd: <the mysql user mail's password>
sql_hostnames: <the mysqld hostname>
sql_database: mail
sql_select: SELECT password FROM accountuser WHERE username = '%u@%r'
      OR (username ='%u' AND domain_name = '') (all one line)
```

4.3 Cyrus IMAP

4.3.1 /etc/imapd.conf

Here is the basic required information:

```
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: cyrus
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
sasl_pwcheck_method: auxprop
sasl_auxprop_plugin: sql
sasl_mech_list: PLAIN LOGIN
sasl_sql_engine: mysql
```

```
sasl_sql_user: mail
sasl_sql_passwd: <the mysql user mail's password>
sasl_sql_hostnames: <HOSTNAME OR IP OF MYSQL MACHINE>
sasl_sql_database: mail
sasl_sql_select: SELECT password FROM accountuser WHERE username = '%u@%r'
          OR (username ='%u' AND domain_name = '') (all one line)
virtdomains: userid
unixhierarchysep: yes
altnamespace: yes
```

4.3.2 /etc/cyrus.conf

Nothing is required to change here, however to allow daily Squatter indexing of mailboxes insert this at the bottom of the file:

```
squatter cmd="/usr/lib/cyrus-imapd/squatter -r -v  user/%" at=0405
```

4.4 Web-Cyradm

4.4.1 /var/www/html/web-cyradm/config/conf.php

Set:

```
$CYRUS = array(
'HOST'  => '<name of mail system>',
'PORT'  => 143,
'ADMIN' => 'cyrus',
'PASS'  => '<the cyrus password>'
);

$DB = array(
'TYPE'  => 'mysql',
'USER'  => 'mail',
'PASS'  => '<the mysql user mail's password>',
'PROTO' => 'unix',       // set to "tcp" for TCP/IP
'HOST'  => '<the mysql ip>',
'NAME'  => 'mail'
```

also:

```
$crypt = "plain"
$DOMAIN_AS_PREFIX = 1;
$ENABLE_FQUN = 1;
```

If you wish to add error-logging to web-cyradm add this to bottom of script:

```
error_reporting(E_ALL);
ini_set("log_errors",1);
ini_set("error_log","/var/log/web-cyradm-error.log");
```

Then create the log itself in the shell:

```
touch /var/log/web-cyradm-error.log
chown apache:apache web-cyradm-error.log
```

5 Testing the Software

5.1 Testing That All Necessary Services Are On

You can check by executing

```
service foo status
```

If a service is running, it should give you a PID number of the service.
A common issue is when cyrus-imapd fails to start. The output generated is

```
Starting cyrus-imapd: preparing databases... FAILED!
```

That usually is a result of a corrupted database file at build, specifically mailboxes.db or annotations.db in the /var/lib/imap directory. Rename them to a backup filename and then restart the service. Cyrus should create new working database files and the service should start with no problems.

5.2 Testing SMTP

Telnet into the postfix machine on port 25 and send a mail in this fashion. If you are in the $mynetworks in /etc/postfix/main.cf, you will not need to authenticate. If you are not, it might be best to use a mail client and send a username and password. Otherwise, SMTP will reject you.

```
[root\@mail postfix]\# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 mail.foobar.com NO UCE
helo localhost.localdomain
250 mail.foobar.com
mail from: foobar@foobar.com
250 Ok
rcpt to: bill.gates@microsoft.com
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Your mother is a hamster, and your father smells of elderberries. <enter>
. <enter>
250 Ok: queued as DE505FCE0
quit
221 Bye
Connection closed by foreign host.
```

If you see the output "250 Ok: queued as 'some number' ", the mail was sent. // Another good test is sending a mail from the command line on the mail machine while running

```
tail -f /var/log/maillog
```

on another terminal (tty1, tty2, etc)

```
echo hello | mail foobar@foobar.com
```

The tail command should show something like this:

```
Aug 12 16:27:17 mail postfix/pickup[20749]: 50F24FDD6: uid=0 from=<root>
Aug 12 16:27:17 mail postfix/cleanup[20930]: 50F24FDD6:
message-id=<20050812202717.50F24FDD6@mail.foobar.com>
Aug 12 16:27:17 mail postfix/qmgr[19739]: 50F24FDD6:
from=<root@mail.foobar.com>, size=275, nrcpt=3 (queue active)
Aug 12 16:27:17 mail lmtpunix[20768]: duplicate_check:
<20050812202717.50F24FDD6@mail.foobar.com> foobar.com!user.foobar 0
Aug 12 16:27:17 mail lmtpunix[20768]: mystore: starting txn 2147483855
Aug 12 16:27:17 mail lmtpunix[20768]: mystore: committing txn 2147483855
Aug 12 16:27:17 mail lmtpunix[20768]: duplicate_mark:
<20050812202717.50F24FDD6@mail.foobar.com> foobar.com!user.foobar 1123878437 17
Aug 12 16:27:17 mail lmtpunix[20768]: mystore: starting txn 2147483856
Aug 12 16:27:17 mail lmtpunix[20768]: mystore: committing txn 2147483856
Aug 12 16:27:17 mail lmtpunix[20768]: duplicate_mark:
<20050812202717.50F24FDD6@mail.foobar.com> .foobar+@foobar.com.sieve. 1123878437 0
Aug 12 16:27:17 mail postfix/lmtp[20933]: 50F24FDD6: to=<foobar@foobar.com>,
relay=/var/lib/imap/socket/lmtp[/var/lib/imap/socket/lmtp], delay=0,
status=sent (250 2.1.5 Ok)
Aug 12 16:27:18 mail postfix/qmgr[19739]: 50F24FDD6: removed
```

5.3 Testing POP3

Create a test account on web-cyradm and telnet to the cyrus machine on the pop3 port and authenticate like this:

```
[root@mail postfix]# telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
+OK mail.foobar.com Cyrus POP3 v2.2.12-Invoca-RPM-2.2.12-1.1.fc3 server ready
<36382431.1123872629@mail.foobar.com>
user foo@foobar.com
+OK Name is a valid mailbox
pass secret123
+OK Mailbox locked and ready
quit
```

```
+OK
Connection closed by foreign host.
```

If you get a "+OK Mailbox locked and ready", the POP3 authentication mechanism is working.

5.4 Testing IMAP

Run the program imtest on the mail machine with a test username:

```
[root@mail postfix]# imtest -a foobar@foobar.com mail.foobar.com
S: * OK mail.foobar.com Cyrus IMAP4 v2.2.12-Invoca-RPM-2.2.12-1.1.fc3 server ready
C: C01 CAPABILITY
S: * CAPABILITY IMAP4 IMAP4rev1 ACL QUOTA LITERAL+ MAILBOX-REFERRALS NAMESPACE UIDPLUS
ID NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND BINARY  SORT THREAD=ORDEREDSUBJECT
THREAD=REFERENCES ANNOTATEMORE IDLE STARTTLS LISTEXT LIST-SUBSCRIBED X-NETSCAPE
S: C01 OK Completed
Please enter your password:
C: L01 LOGIN foobar@foobar.com {4}
S: + go ahead
C: <omitted>
S: L01 OK User logged in
Authenticated.
Security strength factor: 0
. logout
* BYE LOGOUT received
. OK Completed
Connection closed.
```

If you see the word "Authenticated", imap is working.