

Implementing POP3 and IMAP4 Using Dovecot

AfNOG 2012

Scalable Internet Services (SS-E)

Serrekunda, Gambia

Presented by Michuki Mwangi

(Built on materials developed by Joel Jaeggli)

What is POP3

- POP3 stands for Post Office Protocol ver 3
- Described in RFC1913
- Runs on TCP Port 110 as a client server function
- Allows for a maildrop service (similar to the post box mail service) hence the name
- By design its limited in features to download and delete email from server
- Security was also limited to using APOP (md5 hash for authentication)
- RFC 2449 proposed POP3 extensions which included SASL Mechanism, Expiry, Pipelining, etc.
- RFC 2595 describes using TLS with POP3 also known as POP3s and runs on port 995

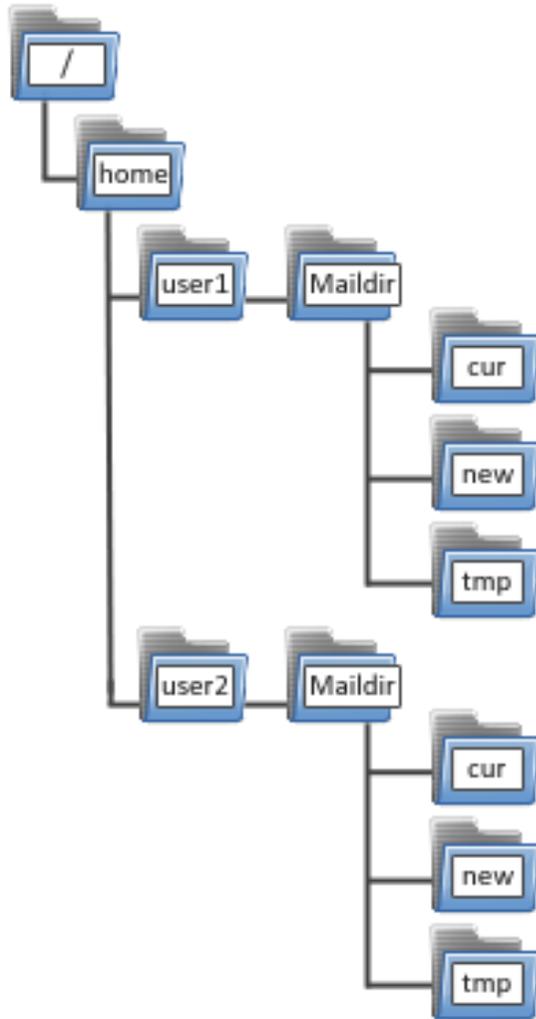
What is IMAP4?

- Internet Message Access Protocol version 4
- Described in RFC 1730
- Runs on TCP Port 143 as client-server function
- More advanced in features compared to POP3
- IMAP4 stores mail on server and copies can be transferred to the client on request.
- By default only the message headers are sent to the client, the rest of the message is accessed on opening the email.
- Allows client to access and manipulate email residing on a server, creation of folders, filters, etc.
- RFC 1731 describes the IMAP Authentication Mechanisms
- RFC 2595 describes using TLS with IMAP4 running on TCP port 993

Mail Storage Formats

- Mailbox Format (Mbox)
- Defined in RFC 4155
- All messages in an Mbox mailbox are concatenated and stored as a plain text in a single file
- Mails are stored in RFC822 format with a blank space separating each message (2 spaces as each message has one space) and “From” determining start of next message.
- Mbox has a distinct disadvantage in cases of large mailbox (a single large file) requires more resources to read/open and can be slow depending on the servers load.

Maildir Storage Format



.Mail Directory Format (Maildir)

.Each message is stored in a separate file with a unique name and each folder in a directory

.Maildir++ provides extension to the Maildir specification providing support for subfolders and quotas.

.Maildir directory has 3 folders **temp**, **new** and **current**

How Maildir Works

- The mail delivery agent stores all new emails to the mailbox in the tmp directory with a unique filename. (unique = time + hostname+ random generated number)
- The MDA creates a hard link to the file in tmp/unique to new/unique
- The Mail User Agent will check for new emails in new folder and move them to current folder
- The MUA modifies the filename to add a colon (:), a '2' and various flags to represent message status i.e read, replied, forwarded, deleted, etc
-

What is Dovecot?

- High-performance POP and IMAP server
- Developed by Timo Sirainen
- Unlike say UW IMAP it wasn't written in the 80s
- Transparently indexes mailbox contents (Why is this important?)
- Supports both mbox and maildir formats
- Capable of operating in an environment with minimal locking. (Why is this important)
- Graceful around failures (index repair for example)
- Designed with Security in mind – support for Authentication Mechanism and SSL/TLS

Let's install it the FreeBSD way

- `#cd /usr/ports/mail/dovecot`

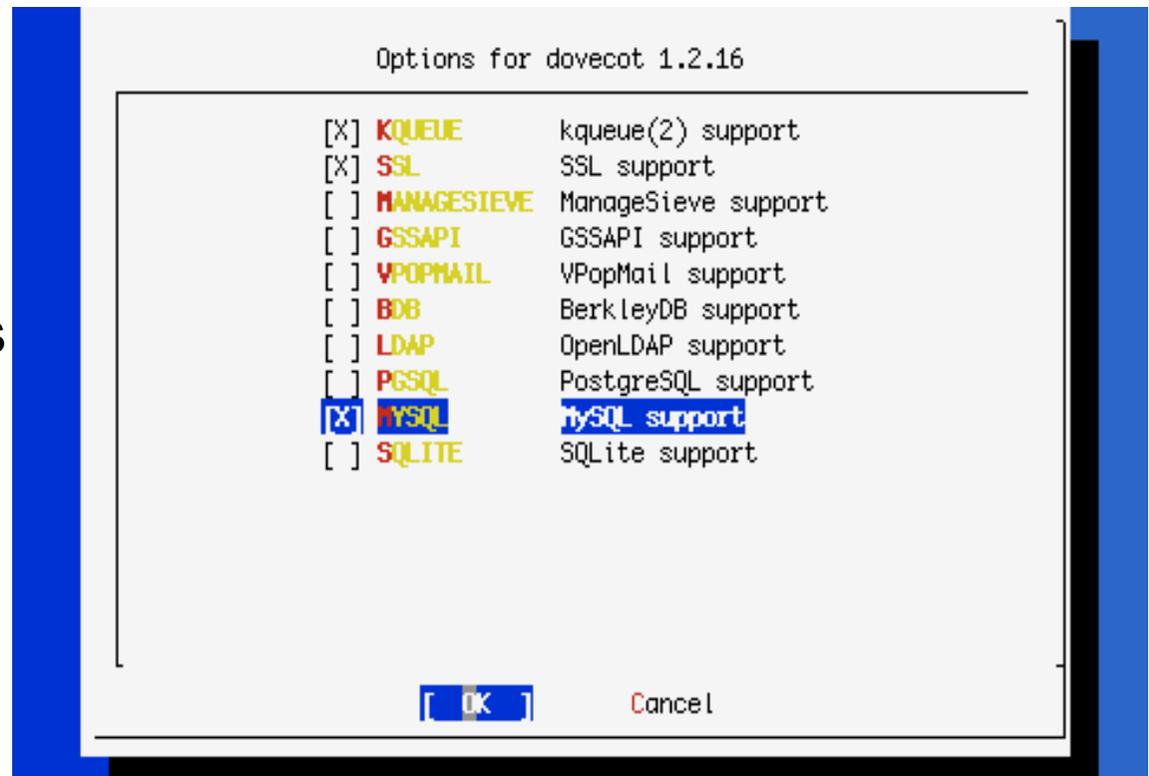
- `#make install clean`

- Note all the options for databases!

- It is typical for small applications to do authentication of users using the unix password file or PAM.

- Big mail installations can use an SQL database interface for the storage of user credentials.

- Select the Mysql Option for this exercise



FreeBSD install cont

- Take a look at `/usr/local/etc/rc.d/dovecot`
- Edit `/etc/rc.conf`
- `dovecot_enable="YES"`
- Ok, now we could start it but we really need to configure it first.
- Look at `/usr/local/etc/dovecot.conf`

Dovecot Configuration

- ***If you do not have a working SSL Certificate, ignore steps above and find the line***
 - `# ssl = yes`
- ***Uncomment the line and modify it to NO***
 - `ssl = no`
- Else if you have SSL Certs Working during Apache Session, find the lines:
 - `#ssl_cert_file = /etc/ssl/certs/dovecot.pem`
 - `#ssl_key_file = /etc/ssl/private/dovecot.pem`
- ***Uncomment*** them, and modify the ***PATH*** to point at the certificate and keyfile that we created during the apache tutorial. i.e.
 - `ssl_cert_file = /usr/local/etc/apache22/server.crt`
 - `ssl_key_file = /usr/local/etc/apache22/server.key`
- Disable plaintext authentication by finding the line below
 - `disable_plaintext_auth = no`
- Set the value to yes as below
 - `disable_plaintext_auth = yes`
 - Note: unencrypted connections can still be made from localhost!

Dovecot Configuration 2

- Note that the default listening services are:
 - `protocols = imap imaps pop3 pop3s managesieve`
 - TCP listeners are on 110, 143, 993, and 995
 - If you need the unencrypted versions of the protocol for some reason (e.g. a webmail application) then you should firewall them off from the rest of your end users (end-user clients should never be allowed to connect insecurely)
 - Otherwise disable `imap` and `pop3` (***optional***)
 - ***If you don't have SSL Certificate (from Apache-SSL session), disable (remove) imaps and pop3s and remain with imap and pop3.***
 - ***Remove "managesieve" option in the protocols section***

Dovecot Configuration – mailbox location

- The mail storage by default on Exim is in /home/%u/mail in Maildir format
- The default Dovecot storage format is set to Mbox and we shall change this format to Maildir.
- To change this to use a different storage format and location
- Locate the line:
 - ***mail_location = mbox:~/mail:INBOX=/var/mail/%u***
 - And change it to the following line
 - ***mail_location = maildir:~/mail/***
- Ok we should have a sufficiently tuned dovecot to be able to start it.
- ***/usr/local/etc/rc.d/dovecot start***

Done

- If everything works correctly you should be able to point an imap client towards your system at port 993 or pop3 clients on port 110
- Alternatively; using telnet

telnet localhost 110

user afnog

pass afnog

list

quit

Scaling Dovecot using Mysql and Virtual Users

Mailbox Location

- Change location of mailbox by editing `/usr/local/etc/dovecot.conf`
- ***# vi /usr/local/etc/dovecot.conf***
- Locate the line:
 - *mail_location = maildir:~/mail/*
- Change it to
- ***mail_location = maildir:/home/vmail/%n/Maildir***

Adding Mysql Authentication

Edit the dovecot config file and make the following changes.

```
vi /usr/local/etc/dovecot.conf
```

Find and Comment the following to disable PAM Authentication.

```
#passdb pam  
#args = session=yes dovecot  
#}
```

Uncomment the following line

```
passdb sql {  
  args = /usr/local/etc/dovecot-sql.conf  
}
```

Comment Static

```
#userdb passwd {  
#args = blocking=yes  
#}
```

Uncomment the following

```
userdb sql {  
  args = /usr/local/etc/dovecot-sql.conf  
}
```

Additional Changes

Add the following values in bold

- ***Postmaster_address = valid.email@address***

Uncomment the following

- ***mail_plugin_dir = /usr/local/lib/dovecot/lda***
- ***auth_socket_path = /var/run/dovecot/auth-master***

...cont'd

- The file `/usr/local/etc/dovecot-sql.conf` does not exist.
- We have created a template for purposes of this class and placed it at `/home/afnog/dovecot-sql.conf`
- ***#cp /home/afnog/dovecot-sql.conf /usr/local/etc/***
- For more information on the `dovecot-sql.conf` file please see;
- `/usr/local/share/examples/dovecot/dovecot-sql.conf`

Creating Dovecot's Mysql DB

- Having configured dovecot to use Mysql, we need to setup create the database in Mysql and populate the database with a user information
- We have provided for a basic sql schema that will be used in this class and placed it at `/home/afnog/dovecot-mysql-schema.sql`
- Change directory to `/home/afnog`
- **`#cd /home/afnog`**
- Check to see that the file exists in the directory
- **`#ls`**
- Run the schema in mysql to create the database
- **`#mysql -p <dovecot-mysql-schema.sql`**

...Cont'd

- Edit the file and change the username and password to the Mysql database (*as was created during the Radius setup*)
- *Create a user that will manage the virtual users*
- ***#pw adduser vmail -m***
- check the the UID of the vmail user and take note of it for the next steps
- ***# cat /etc/passwd | grep vmail***

Inserting records in Mysql DB

- The database created by the dovecot-mysql-schema.sql is empty
- To populate data on the mysql database there are two options;
 - i) Manually from the mysql CLI
 - ii) Using Web/GUI like PHPMyAdmin
- For this class we shall use the mysql CLI to get more hands on experience
- **Replace UID and GID below with the “vmail” UID/GID for example GID is ‘1002’**
- **xxxx.afnogws.gh** is the domain created in the **DNS class**.

```
#mysql -p
```

```
Mysql> use dovecot;
```

```
Mysql> insert into users (userid, domain, password, home, uid, gid) values ('afnog',  
'xxxx.afnogws.gh', md5('success'), '/home/vmail/%n/Maildir', 'UID', 'GID');
```

```
Mysql> insert into users (userid, domain, password, home, uid, gid) values ('yourname',  
'xxxx.afnogws.gh', md5('afnog'), '/home/vmail/%n/Maildir', 'UID', 'GID');
```

Important Replace UID and GID above with that of vmail user.

Exim Delivery to Virtual Users using Dovecot Delivery

Exim Email Accepting

Open and Edit /usr/local/etc/exim/configure

```
# vi /usr/local/etc/exim/configure
```

Add the Mysql database access config line below primary_hostname

```
hide mysql_servers = localhost/dovecot/root/afnog
```

Then change the localuser Router the following lines in the “Routers Section”

```
dovecot_router:
```

```
driver = accept
```

```
#local_part_suffix = +*
```

```
#local_part_suffix_optional
```

```
condition = ${lookup mysql {SELECT home FROM users WHERE userid='$local_part'}}
```

```
transport = dovecot_delivery
```

Exim Delivery to Dovecot

Modify the `local_delivery` with the following lines under the transport section in the configure file.

dovecot_delivery:

driver = pipe

command = /usr/local/libexec/dovecot/deliver

message_prefix =

message_suffix =

delivery_date_add

envelope_to_add

return_path_add

log_output

user = vmail

temp_errors = 64 : 69 : 70 : 71 : 72 : 73 : 74 : 75 : 78

Restart Exim & Dovecot

Restart both Exim and Dovecot

/usr/local/etc/rc.d/exim restart

/usr/local/etc/rc.d/dovecot restart

Send email tests and watch the logfiles.

***Try and log in using the virtual user names
and passwords.***