

How To Install Postfix & Dovecot + GNU mailman

1. INSTALL UBUNTU 16.04 DESKTOP	1
2. FOR TESTING PURPOSES I DO THE FOLLOWING	2
3. COMMERCIAL SSL	2
4. VISIT THE EXRATIONE PAGE FOR INSTRUCTIONS	2
5. INSTALL LAMP SERVER	2
6. INSTALL MAIL SERVER	3
1. PostfixAdmin tweaks.	3
2. Dovecot tweaks.	4
3. Postfix tweaks.	5
4. Roundcube tweaks.	7
7. INSTALL MAILMAN	8
9. THAT'S IT.	12
10. TIPS & TRICKS:	12

1. Install Ubuntu 16.04 Desktop

I like the GUI. The Server does not have a GUI, for Ubuntu server you'd have to install the GUI yourself and that's another challenge in itself.

<https://www.ubuntu.com/download/desktop/thank-you?country=US&version=16.04.1&architecture=amd64>

2. Testing Purposes

I do the following.

In /etc/hosts I add the machine and domain name

```
127.0.0.1 mail.yourdomain.com yourdomain.com localhost
```

In /etc/hostname I use

```
mail.yourdomain.com
```

in /etc/mailname I use

```
mail.yourdomain.com
```

3. Commercial SSL

If you desire SSL commercial functionality, install it now, a number of SSL configurations depend on a working SSL certificate configuration and naming later.

An inexpensive place for certificates is <http://www.namecheap.com> for as low as \$10.- a year.

Otherwise during installation of the Mail Server a free self-signed certificate is generated.

4. Visit the Exratione page for instructions

<https://www.exratione.com/2016/05/a-mailserver-on-ubuntu-16-04-postfix-dovecot-mysql/>

Ignore Amazon Web Services (AWS) section if you're not using AWS.

Enable firewall and open our required ports

```
sudo apt-get install ufw
```

```
sudo ufw allow 25
```

```
sudo ufw allow 80
```

```
sudo ufw allow 443
```

```
sudo ufw allow 587
```

```
sudo ufw allow 993
```

```
sudo ufw enable
```

5. Install LAMP Server

Please install according to step 4. Once done test browsing to

<http://localhost>

Your browser might complain about the certificate, accept the exception so you can proceed.

If all works, you should see a page titled: "Apache2 Ubuntu Default Page"

6. Install Mail Server

DO NOT INSTALL POSTGREY! There will be a point in the Exratione page where Postgrey is included in the apt-get statement. REMOVE IT! Otherwise your inbound mail will be rejected most of the time.

I use the following instead of what's on the Exratione page

```
sudo apt-get install --assume-yes \  
  postfix-mysql \  
  dovecot-mysql \  
  amavis \  
  clamav \  
  clamav-daemon \  
  spamassassin \  
  libdbi-perl \  
  libdbd-mysql-perl \  
  php7.0-imap
```

If you have already installed Postgrey, remove it with **sudo apt-get purge postgrey**. Otherwise, it will cause a lot of grief troubleshooting why recipients get rejected.

Please install according to step 4.

1. PostfixAdmin tweaks.

Instead of what is provided in the Exratione page. This will provide a better organization of mail folders in /var/vmail (per domain then per user).

```
Use the following section in /var/www/html/postfixadmin/config.local.php  
// Mailboxes  
// If you want to store the mailboxes per domain set this to 'YES'.  
// Examples:  
// YES: /usr/local/virtual/domain.tld/username@domain.tld  
// NO: /usr/local/virtual/username@domain.tld  
$CONF['domain_path'] = 'YES';  
// If you don't want to have the domain in your mailbox set this to 'NO'.  
// Examples:  
// YES: /usr/local/virtual/domain.tld/username@domain.tld  
// NO: /usr/local/virtual/domain.tld/username  
// Note: If $CONF['domain_path'] is set to NO, this setting will be forced to  
// YES.
```

```
$CONF['domain_in_mailbox'] = 'NO';
```

Browse <https://localhost/postfixadmin/setup.php> instead of <https://mail.example.com/postfixadmin/setup.php>. That will help where the machine doesn't have a real world domain yet.

I'm using `admin@yourdomain.com` as the PostfixAdmin admin user with password `testserver12`.

I created the following in PostfixAdmin domains: `testdomain1.com` and `testdomain2.com`

I've added a mailbox for `testdomain1.com` as `test1@testdomain1.com` also with password `testserver12`.

I'm also using `admin@testdomain2.com` as the admin user with password `testserver12`.

I've added a mailbox for `testdomain2.com` as `test2@testdomain2.com` also with password `testserver12`.

2. Dovecot tweaks.

We'll use the free certificates created & installed during LAMP server installation.

For `/etc/dovecot/conf.d/10-ssl.conf` instead of what Exratione page says:

```
ssl_cert = </etc/ssl/certs/ssl-cert-snakeoil.pem
ssl_key = </etc/ssl/private/ssl-cert-snakeoil.key
```

Comment these out:

```
#ssl_cert = </etc/ssl/certs/example.com.crt
#ssl_key = </etc/ssl/private/example.com.key
#ssl_ca = ...
```

For `/etc/dovecot/conf.d/10-master.conf` disable enable secure IMAP and disable POP3

```
service imap-login
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
```

```

service pop3-login {
    inet_listener pop3 {
        port = 0
    }
    inet_listener pop3s {
        port = 0
        #ssl = yes
    }
}

```

ClamAV database.

Running freshclam almost always generates an error for. This is because the ClamAV process is running and has locked the `/var/log/freshclam.log` file lock. You can ignore this error.

3. Postfix tweaks.

For `/etc/postfix/main.cf` we're making the following change from the Exrationale page.

This is to disable postgrey in case you've already installed it. Or if you didn't install it, you need to remove the "check_policy ..." entries anyway, otherwise recipients get rejected by postfix.

Change the section to:

```

# Requirement for the recipient address. Note that the entry for
# "check_policy_service inet:127.0.0.1:10023" enables Postgrey.
smtpd_recipient_restrictions = reject_unauth_pipelining,
    permit_mynetworks, permit_sasl_authenticated,
    reject_non_fqdn_recipient, reject_unknown_recipient_domain,
    reject_unauth_destination, permit smtpd_data_restrictions =
    reject_unauth_pipelining
# This is a new option as of Postfix 2.10, and is required in addition to
# smtpd_recipient_restrictions for things to work properly in this
# setup.
smtpd_relay_restrictions = reject_unauth_pipelining,
    permit_mynetworks, permit_sasl_authenticated,
    reject_non_fqdn_recipient, reject_unknown_recipient_domain,
    reject_unauth_destination, permit

```

Update mydestination as follows, this is required by mailman later:

```

mydestination = localhost, localhost.localdomain

```

For /etc/postfix/master.cf we're making the following changes from the Exrationale page. This is to provide a secure way for smtp clients to submit emails.

```
submission inet n    -    y    -    -    smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_enforce_tls=yes
# -o
smtpd_client_restrictions=permit_sasl_authenticated,reject_unauth_destination,reject
# -o smtpd_sasl_tls_security_options=noanonymous
```

Testing the Mail Server with Thunderbird Mail.

Before testing add the following line in your /etc/hosts file:

```
127.0.0.1    testdomain1.com testdomain2.com
```

Note that:

Thunderbird will auto detect and fail. Go to manual config and change settings.

When creating the account Thunderbird will complain about an invalid certificate, which is valid as we're using a certificate we generated on our own. Make sure to set "Permanently Store this Exception" and click on "Confirm Security Exception".

The first time Thunderbird sends mail it will complain about the an invalid certificate. Do the same as above and then retry sending an email.

Use the following settings for Thunderbird accounts (do manual config):

Account 1:

Yourname: test1

Email address: test1@testdomain1.com

Password: linuxmint12

Incoming: IMAP, port 993, SSL/TLS, Normal password

Incoming Server Name: mail.yourdomain.com

Outgoing: SMTP, port 587, STARTTLS, Normal password

Account 2:

Yourname: test2

Email address: test2@testdomain2.com

Password: linuxmint12

Incoming: IMAP, port 993, SSL/TLS, Normal password

Incoming Server Name: mail.yourdomain.com

Watch /var/log/mail.log for errors (I use tail -f -n20 /var/log/mail.log, it prints out the last 20 lines of the log and updates it as new lines come around).

4. Roundcube tweaks.

Note that installing Roundcube is optional. It is needed only if you desire a web based email interface for your email users. It's equivalent to say Squirrel Mail.

For /var/lib/roundcube/plugins/jqueryui/config.inc.php we need to add a line of code to the top of the file, right after <?php:

```
$config = array();
```

For /var/lib/roundcube/plugins/zipdownload/config.inc.php we need to add a line of code to the top of the file, right after <?php:

```
$config = array();
```

Test Roundcube by browsing to, and logging in as test1 or test2 email accounts

<https://localhost/roundcube>

Note the basic configuration for Roundcube is for single server where Roundcube runs on the mail server, hence the use of insecure IMAP at port 143.

To run Roundcube on a separate server configure you must

```
Configure /etc/roundcube/config.inc.php with  
For SSL: $config['default_host'] = 'ssl://yourIMAPSserver/  
or you could use TLS: $config['default_host'] =  
'ssl://yourIMAPSserver/';
```

Do not create certificates until you have configured the right /etc/hosts and hostnames. If you change this after certificates are created, Roundcube will complain that the CN's don't match in its error logs and refuse to connect with IMAPS on port 993.

Take care to use the right certificates

Watch /var/log/roundcube/errors log for errors.

```
sudo tail -f -n20 /var/log/roundcube/errors
```

7. Install Mailman

Download mailman v 2.1.23 from

<http://packages.ubuntu.com/zesty/mailman>

Install python-dnspython first, it's a dependency of mailman.

```
sudo apt-get install python-dnspython
```

Install the mailman package using dpkg

```
sudo dpkg -i mailman_2.1.23-1_amd64.deb
```

Refresh aliases.db as it sometimes gets corrupted

```
sudo rm /etc/aliases.db
```

```
sudo newaliases
```

Enable CGI

```
sudo a2enmod cgi
```

```
sudo service apache2 restart
```

Copy configuration file for apache (this configures the web URL for mailman)

```
sudo cp /etc/mailman/apache.conf /etc/apache2/sites-available/mailman.conf
```

Edit the /etc/apache2/sites-available/mailman.conf file

Change

```
<Directory /usr/lib/cgi-bin/mailman/>
```

```
    AllowOverride None
```

```
    Options ExecCGI
```

```
    AddHandler cgi-script .cgi
```

```
    Require all granted
```

```
</Directory>
```

```
<Directory /var/lib/mailman/archives/public/>
```

```
    Options FollowSymLinks
```

```
    AllowOverride None
```

```
    Require all granted
```

```
</Directory>
```

To

```
<Directory "/usr/lib/cgi-bin/mailman">
```

```
    Options +ExecCGI
```

```
    AddHandler cgi-script .cgi
```

```
    Options FollowSymLinks
```

```
    Require all granted
```

```
</Directory>
```

```
<Directory /var/lib/mailman/archives/public/>
```

```
    Order allow,deny
```

```
    Allow from all
```

```
    Options Indexes FollowSymLinks
```



```
    Require all granted
</Directory>
```

Replace everything under

```
#DEFAULT_PATTERN = 'http ...
```

With

```
<VirtualHost *:80>
ServerName mail.yourdomain.com
ServerAdmin admin@yourdomain.com
Redirect / https://mail.yourdomain.com/
```

```
ErrorLog /var/log/apache2/mailman-error.log
CustomLog /var/log/apache2/mailman-access.log combined
```

```
<Directory /var/lib/cgi-bin/mailman>
    Options FollowSymLinks
AllowOverride All
    Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
    Require all granted
</Directory>
```

```
</VirtualHost>
```

```
<VirtualHost *:443>
ServerName mail.yourdomain.com
ServerAdmin admin@yourdomain.com
```

```
ErrorLog /var/log/apache2/mailman-error.log
CustomLog /var/log/apache2/mailman-access.log combined
```

```
<Directory /var/lib/cgi-bin/mailman>
    Options FollowSymLinks
AllowOverride All
    Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
    Require all granted
</Directory>
```

```
</VirtualHost>
```

```
Alias /pipermail/ /var/lib/mailman/archives/public/
Alias /postfixadmin /var/www/html/postfixadmin
Alias /roundcube /var/www/html/roundcube
Alias /images/mailman/ /usr/share/images/mailman/
ScriptAlias /admin /usr/lib/cgi-bin/mailman/admin
ScriptAlias /admindb /usr/lib/cgi-bin/mailman/admindb
```

```
ScriptAlias /confirm /usr/lib/cgi-bin/mailman/confirm
ScriptAlias /create /usr/lib/cgi-bin/mailman/create
ScriptAlias /edithtml /usr/lib/cgi-bin/mailman/edithtml
ScriptAlias /listinfo /usr/lib/cgi-bin/mailman/listinfo
ScriptAlias /options /usr/lib/cgi-bin/mailman/options
ScriptAlias /private /usr/lib/cgi-bin/mailman/private
ScriptAlias /rmlist /usr/lib/cgi-bin/mailman/rmlist
ScriptAlias /roster /usr/lib/cgi-bin/mailman/roster
ScriptAlias /subscribe /usr/lib/cgi-bin/mailman/subscribe
ScriptAlias /mailman/ /usr/lib/cgi-bin/mailman/
ScriptAlias / /usr/lib/cgi-bin/mailman/listinfo
```

Enable the mailman apache2 site

```
sudo a2ensite mailman
sudo service apache2 restart
```

Edit the /etc/mailman/mm_cfg.py file

Change

```
DEFAULT_URL_PATTERN = 'http://%s/cgi-bin/mailman/'
To (this lets us have clean URLs without "cgi-bin" in the path)
DEFAULT_URL_PATTERN = 'http://%s/'
```

Change (lets us have a clean list email, e.g. mailman@yourdomain.com) instead of a long mailman@mail.yourdomain.com email.

```
DEFAULT_EMAIL_HOST = 'mail.yourdomain.com'
To
DEFAULT_EMAIL_HOST = 'yourdomain.com'
```

Uncomment

```
# MTA='Postfix'
To (as we're using Postfix for our mail server)
MTA='Postfix'
```

Add the following lines at the end of the file

```
POSTFIX_STYLE_VIRTUAL_DOMAINS = ['yourdomain.us']
VIRTUAL_MAILMAN_LOCAL_DOMAIN = 'localhost'
OWNERS_CAN_DELETE_THEIR_OWN_LISTS = yes
PUBLIC_ARCHIVE_URL = 'https://%s/pipermail/%(listname)s'
```

Create mailman list as it is required for mailman to startup

```
sudo /usr/lib/mailman/bin/newlist mailman
Enter admin@yourdomain.com as the person running the list
```

Enter a suitable password for mailman administrator (I use testserver12)

Just to be extra sure, recreate the /etc/aliases.db file

Start mailman

sudo service mailman start

For /etc/postfix/master.cf make sure you have the following line (you can add it at the end of the file is necessary)

```
mailman unix - n n - - pipe
flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
${nexthop} ${user}
```

For /etc/postfix/main.cf

Change

```
virtual_alias_maps =
mysql:/etc/postfix/mysql_virtual_alias_maps.cf,
mysql:/etc/postfix/mysql_virtual_alias_domainaliases_maps.cf
```

To

```
virtual_alias_maps =
mysql:/etc/postfix/mysql_virtual_alias_maps.cf,
mysql:/etc/postfix/mysql_virtual_alias_domainaliases_maps.cf,
hash:/var/lib/mailman/data/virtual-mailman
```

Add the following to the end of the file

```
# -----
# Mailman
# -----

alias_maps =
hash:/etc/aliases,hash:/var/lib/mailman/data/aliases
virtual_alias_domains =

mydomain = yourdomain.com
```

Run the following until there is a low amount (10 or so) or no errors

sudo /usr/lib/mailman/bin/check_perms -f

Run (to restart mailman service)

sudo service mailman restart

Run (to enable mailman.conf)

sudo a2ensite mailman

Run (to restart apache2 obviously)
sudo service apache2 restart

9. That's it.

You should now be able to visit <http://mail.yourdomain.com/listinfo> and see the Mailman list.

Log in to the administrative interface and add memberships (add at least test1@testdomain1.com and test2@testdomain2.com).

Once that is done, test1 and test2 should be able to send an email to mailman@yourdomain.com and a little while later be received by the members (test1 and test2 both).

10. Tips & tricks:

Don't forget to do **sudo postmap /etc/postfix/transport** if you created, copied, or modified transport file. Then restart Postfix "sudo service postfix restart".

Sometimes the aliases.db gets corrupted, you'll see this logged in `/var/log/mail.err` as "alias.db not found". Fix this by running **sudo newaliases** and then restart Postfix with **sudo service postfix restart**