

Contents

- 1 Install as per normal
- 2 Basic Changes:
- 3 Advanced Changes:
 - ◆ 3.1 To prevent cross over emails between multiple domains.
 - ◆ 3.2 Restrict Mail delivery to Local users
 - ◆ 3.3 Blocking Spam with spamhaus and Postfix
 - ◇ 3.3.1 Testing zen.spamhaus.org
- 4 Debugging and Testing via Telnet
- 5 Managing Postfix
 - ◆ 5.1 Delete an Email from the Queue
 - ◆ 5.2 Checking Mail logs with pflogsumm
 - ◆ 5.3 Show Mail Queue
- 6 Install Postfix for sending mail via relayhost

Install as per normal

```
apt-get install postfix
Choose Internet Site Config.
```

After Install - Main folder = /etc/postfix
Main file = main.cf

Basic Changes:

```
Just the name used to identify server
myhostname = mail.domain.com
```

```
//disable lookup of usernames
disable_vrfy_command = yes
Remove hash beside delay_warning_time = 4h
```

Advanced Changes:

To prevent cross over emails between multiple domains,

e.g. where root@mydomain1.net and root@mydomain2.net are on the same server.

```
Add the following line into /etc/postfix/main.cf:
smtpd_sender_restrictions = check_recipient_access hash:/etc/postfix/restrict
```

```
Create the file: /etc/postfix/restrict
goodemail@mydomain2.net      OK
mydomain2.net                REJECT
```

Postfix_SMTTP

To activate/ add this file into postfix, type in the shell ->
postmap /etc/postfix/restrict

Further Details at:

[http://www.seifried.org/security/index.php/Closet20001122_Postfix - The Sendmail Replacement, Part II](http://www.seifried.org/security/index.php/Closet20001122_Postfix_-_The_Sendmail_Replacement_Part_II)

Restrict Mail delivery to Local users

On a lists (mailman) server I run - I want to disable mail delivery to local users, however I still want Postfix to deliver mail to /etc/aliases. The line below, which is to be put into /etc/postfix/main.cf forces postfix to only consult \$alias_maps (which is: hash:/etc/aliases).

```
local_recipient_maps = $alias_maps
```

Blocking Spam with spamhaus and Postfix

This is commonly referred to as a "Postfix anti-UCE configuration" (UCE - unsolicited emails). Postfix, with a very simply modification can block incoming email via spamhaus RBLs (Real Time Black-Hole Lists). The following line is to be added to /etc/postfix/main.cf:

```
smtpd_recipient_restrictions reject_rbl_client zen.spamhaus.org, reject_rbl_client bl.spamcop.net  
//If there are entries already - thats fine, just comment delimit them.  
//Note: sbl-xbl.spamhaus.org has now changed to zen.spamhaus.org as per http://www.spamhaus.org/zen/
```

The sender is then bounced back an email saying "Blocked by spamhouse" and it is their, or their ISP's responsibility to remove themselves from spamhaus.

Note: "ping sbl-xbl.spamhaus.org" wont resolve. What postfix does when checking an ip (e.g. w.x.y.z), is to "ping z.y.x.w.sbl-xbl.spamhaus.org", and if that resolves - that ip is listed as spam. (thanks davis).

Note: Make sure ICMP packets are allowed through the firewall. Otherwise postfix will get a "Destination Not Reachable" and allow the mail through.

See more details at: <http://jimsun.linuxnet.com/misc/postfix-anti-UCE.txt> and

<http://www.redhat.com/support/resources/howto/RH-postfix-HOWTO/x441.html> and

<http://www.postfix.org/uce.html> and http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions

Further Info on UCE and Postfix:

```
smtpd_sender_restrictions = Restrictions based in the context of the MAIL FROM command. I.e. restric  
smtpd_recipient_restrictions = Restrictions based on the RCPT TO command. I.e. restrictions based on  
smtpd_client_restrictions = SMTP server access restrictions in the context of a SMTP connection requ
```

I have found that blocking mails via DNSBL at "smtpd_sender_restrictions" is not always effective as some spammers can forge the MAIL FROM command. "smtpd_client_restrictions" is the first line of restrictions, and ideally the DNSBL blocks should be put in here, however as outlined on

<http://jimsun.linuxnet.com/misc/postfix-anti-UCE.txt> , "smtpd_recipient_restrictions" is the best place to place DNSBL blocks.

Testing zen.spamhaus.org

Link: <http://www.crynwr.com/spam/>

Simply send an email to the appropriate address on the above website, and it will reply an automated email with the status of whether your email server is blocking correctly using zen.spamhaus.org

Nice :)

Debugging and Testing via Telnet

SENDING AN EMAIL VIA TELNET 25 & Testing forwarding

```
mail from: sri@mara.net
rcpt to: user@lastre.com
data
.
quit
```

If you get "503 5.5.2 Send hello first", type "ehlo" as the first line after telneting to host 25.

Test and get working Normal - Should be able to send and receive via pine etc.

Had to adjust /etc/hosts with domain name (this allowed sending emails ok):

```
127.0.0.1      localhost
136.201.1.250  kartbuilding.net      phidebian
```

Good URLs

<http://www.muine.org/~hoang/postfix.html>

<http://www.debianhelp.co.uk/postfix.htm>

Managing Postfix

Delete an Email from the Queue

For Example - sending an email to someone and it bounces. Default retry is for 3 days. To remove it manually :

```
postsuper -d queue_id
```

Tons more info at: <http://www.postfix.org/postsuper.1.html>

Checking Mail logs with pflogsumm

pflogsumm shows all the essential information from mail.log. It groups information into the following headings:

- Grand Totals - messages sent and recieved.
- Per-Day Traffic Summary
- Per-Hour Traffic Daily Average
- Host/Domain Summary: Message Delivery
- Host/Domain Summary: Messages Received
- Senders by message count
- Recipients by message count
- Senders by message size
- Recipients by message size
- message deferral detail
- message reject detail
- message reject warning detail
- smtp delivery failures
- Warnings

```
apt-get install pflogsumm
pflogsumm /var/log/mail.log | less
```

It is a very useful tool and shows an excellent insight into mail delivery and sending on your server.

Show Mail Queue

If mails are deferred etc. and you want to see a list of them:

```
postqueue -p
```

Install Postfix for sending mail via relayhost

On one server, I want it to be only able to send emails only. Therefore the following config will bind it to 127.0.0.1 on port 25. It will also be sending emails using a "smart host". Below are the uncommented lines only in main.cf:

```
vi /etc/postfix/main.cf
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
append_dot_mydomain = no
myhostname = thunder.burkesys.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination =
relayhost = mail.burkesys.com
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = 127.0.0.1
```

Postfix SMTP

It must also be checked on mail.burkesys.com that thunder is allowed to relay emails.