**Title:** Mail Server on Ubuntu

**Abstract :** The MDA gets messages from the mail server into the users' inboxes, most commonly with the POP or IMAP mail protocols. Except under some very limited circumstances, an MTA isn't going to do you much good without an MDA, so we're going to be using Dovecot as our MDA.

**Introduction:** A remote mail server requests a TCP connection on port 25 to your mail server. Your firewall lets that connection through and the Postfix "smtpd" process will accept it. Postfix starts speaking SMTP (the "simple mail transfer protocol") and gathers information who the alleged sender and the intended recipient addresses are. While the connection is still active Postfix does a couple of checks and may decide to reject the email. Postfix will also check real-time black lists (RBLs) via DNS to see if the sending IP address should be distrusted. For example it will reject senders running on a dynamic IP address because that almost always means the email is coming from yet another infected Windows workstation or hacked server and is likely spam. Postfix asks Dovecot whether the recipient email address belongs to an actually known user. Dovecot checks the MySQL database and looks for an entry for the email address in question. If the user exists then Postfix will accept the email and forward it to Dovecot. Dovecot stores the received email in a file in the /var/vmail directory. The user fetches new email using the POP3 or IMAP protocols from Dovecot. Now let's assume the user replies to the email and wants to send the reply.

The user's mail client establishes an SMTP connection to Postfix. It sends a username and password to authenticate.

Postfix asks Dovecot whether the username and password are correct. This prevents accepting unauthorized email from untrusted parties.

Dovecot searches for the account information of the sending user in the MySQL database. It tells Postfix whether the authentication was successful.

Postfix needs to find out which server on the internet the email needs to be sent to. It asks a DNS (domain name service) server for an MX (mail exchanger) record of the receiving domain. If successful it will get the name of the server back and will know where to send the email.

Postfix connects to the responsible server of the receiving user, establishes an SMTP connection and sends the email.

## Implementation Details:

### MTAs, MDAs, and MUA's

The applications that send, receive, and deliver e-mails.

Most people are familiar with their MUA—that's a Mail User Agent, more commonly called an "e-mail client" or an "e-mail program."

At the apex is the MTA, or Mail Transfer Agent. This is the core application that actually transmits e-mail around between servers—applications like Exim, sendmail, Postfix, and qmail.

Sandwiched in the middle between the MUA on your desktop and the MTA on the server is another application category: the MDA, or Mail Delivery Agent. We will be using Dovecot as our MDA.

The MDA gets messages from the mail server into the users inboxes, most commonly with the POP or IMAP mail protocols. Except under some very limited circumstances, an MTA isn't going to do you much good without an MDA, so we're going to be using Dovecot as our MDA.

### COURIER

The courier mail server is a mail transfer agent server that provides ESMTP, IMAP, POP3, SMAP services with individual components.

Courier can function as an intermediate mail relay between an internal LAN and Internet.it can provide mail services for regular operating system accounts and for virtual mail accounts.

### SSL/TLS

For a mail server to have a SSL/TLS certificate issued by a recognized Certificate Authority is a must.

First a private key is created 4096 bits as the key-size and SHA2 as the algorithm. The key is encrypted using a password.

The private key and the SSL/TLS certificate is stored in the directory /etc/ssl/private in files ssl-key-encrypted-mail-yourdomain.key and ssl-cert-mail-yourdomain.pem respectively.

The private key is decrypted so that applications like postfix and dovecot can use it.

Finally the SSL/TLS certificate is plugged in to the server by making the following changes to the file /etc/postfix/main.cf

## SPAM ASSASSIN

Spam assassin runs sanity checks on an incoming mail to determine how likely it is to be spam

It is a computer program used for email spam filtering. It uses a variety of spam detection techniques including DNS based, checksum based spam detection, regular expressions, pattern matching techniques etc.

The program can be integrated with the mail server to automatically filter all mail for a site.

Spam assassin is a highly configurable ; if it is used as a system wide filter can still be configured to support per user preferences

## CLAM AV

Clam Antivirus is a free and open source, cross platform antivirus software toolkit available to detect many types of malicious software and viruses.

One of its main use is it is used on mail servers as server side email virus scanner.

Clam AV includes a number of utilities such as command line scanner Automatic database updater and scalable multithreaded daemon, running on antivirus engine from a shared library.

Clam AV database is updated atleast every 4 hours.

## AMAVIS

Amavis is an open source content filter for electronic mail used for message transfer, decoding and some other processing and checking and interfacing with external content filter to provide protection against spam ,viruses and other malwares.

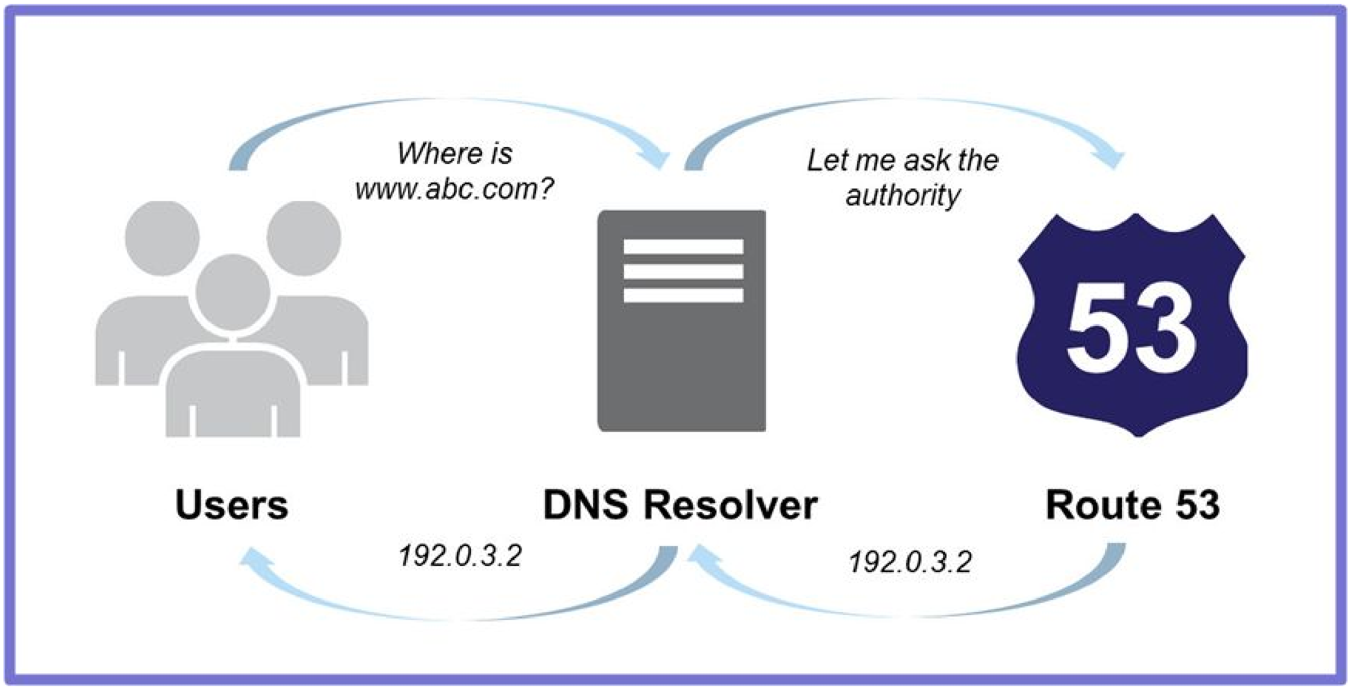
It can be considered as an interface between a mailer and one or more content filters.

Amavis can be used for detecting viruses, spams, banned content types, syntax errors etc.

It can be used for redirect or forward of emails, it can be used for archiving of mail messages to files, to mailboxes, to an SQL database.

It is used to sanitize  passed messages through external sanitizer

It can be further interfaced with spam assassin to provide reliability, security, performance.



```
groupadd virtual -g 5000 useradd -r -g "virtual" -G "users" -c "Virtual User" -u 5000 virtual mkdir
/var/spool/mail/virtual chown virtual:virtual /var/spool/mail/virtual
mv /etc/postfix/main.cf{,.dist} vi /etc/postfix/main.cf
myorigin = /etc/mailname smtpd_banner = $myhostname ESMTP $mail_name biff = no
append_dot_mydomain = no readme_directory = no mydestination = relayhost = mynetworks =
127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 mynetworks_style = host mailbox_size_limit = 0
virtual_mailbox_limit = 0 recipient_delimiter = + inet_interfaces = all message_size_limit = 0 # SMTP
Authentication (SASL) smtpd_sasl_auth_enable = yes broken_sasl_auth_clients = yes
smtpd_sasl_security_options = noanonymous smtpd_sasl_local_domain = # Encrypted transfer
(SSL/TLS)
smtp_use_tls = yes smtpd_use_tls = yes smtpd_tls_cert_file = /etc/ssl/private/mail.example.com.crt
smtpd_tls_key_file = /etc/ssl/private/mail.example.com.key smtpd_tls_session_cache_database =
btree:${data_directory}/smtpd_scache smtp_tls_session_cache_database =
btree:${data_directory}/smtp_scache # Basic SPAM prevention smtpd_helo_required = yes
smtpd_delay_reject = yes disable_vrfy_command = yes
smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks # Force incoming mail to
go through Amavis content_filter = amavis:[127.0.0.1]:10024 receive_override_options =
no_address_mappings # Virtual user mappings alias_maps = hash:/etc/aliases alias_database =
hash:/etc/aliases virtual_mailbox_base = /var/spool/mail/virtual virtual_mailbox_maps =
mysql:/etc/postfix/maps/user.cf virtual_uid_maps = static:5000 virtual_gid_maps = static:5000
virtual_alias_maps = mysql:/etc/postfix/maps/alias.cf virtual_mailbox_domains =
mysql:/etc/postfix/maps/domain.cf
mv /etc/postfix/master.cf{,.dist} vi /etc/postfix/master.cf
# Postfix master process configuration file. For details on the format # of the file, see the master(5)
manual page (command: "man 5 master"). # # Do not forget to execute "postfix reload" after editing this
file. # #
==========================================================================
# service type private unpriv chroot wakeup maxproc command + args # (yes) (yes) (yes) (never) (100)
#
==========================================================================
smtp inet n - - - - smtpd smtps inet n - - - - smtpd -o smtpd_tls_wrappermode=yes submission inet n - - -
- smtpd pickup fifo n - - 60 1 pickup -o content_filter= -o
receive_override_options=no_header_body_checks cleanup unix n - - - 0 cleanup
qmgr fifo n - n 300 1 qmgr tlsmgr unix - - - 1000? 1 tlsmgr rewrite unix - - - - - trivial-rewrite bounce
unix - - - - 0 bounce defer unix - - - - 0 bounce trace unix - - - - 0 bounce verify unix - - - - 1 verify flush
unix n - - 1000? 0 flush proxymap unix - - n - - proxymap proxywrite unix - - n - 1 proxymap smtp unix
- - - - - smtp # When relaying mail as backup MX, disable fallback_relay to avoid MX loops relay unix -
- - - - smtp -o smtp_fallback_relay= showq unix n - - - - showq error unix - - - - - error retry unix - - - - -
error discard unix - - - - - discard local unix - n n - - local virtual unix - n n - - virtual lmtp unix - - - - -
```

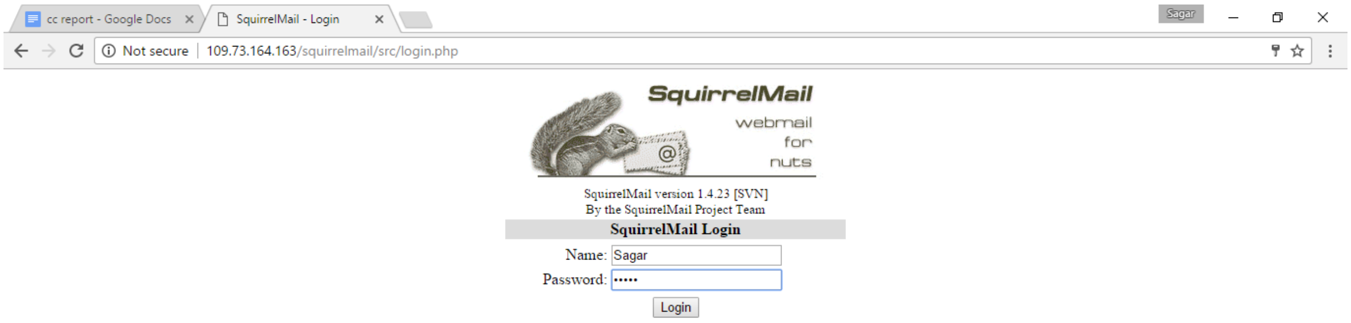
```
lmtp anvil unix - - - - 1 anvil scache unix - - - - 1 scache # #
====================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual # pages of the non-Postfix software
to find out what options it wants. # # Many of the following services use the Postfix pipe(8) delivery #
agent. See the pipe(8) man page for information about ${recipient} # and other message envelope
options. #
=========================================================================== # #
maildrop. See the Postfix MAILDROP_README file for details. # Also specify in main.cf:
maildrop_destination_recipient_limit=1 # maildrop unix - n n - - pipe flags=DRhu user=vmail
argv=/usr/bin/maildrop -d ${recipient} # # See the Postfix UUCP_README file for configuration
details. # uucp unix - n n - - pipe flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail #
# Other external delivery methods.
# ifmail unix - n n - - pipe flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient bsmtp
unix - n n - - pipe flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender
scalemail-backend unix - n n - 2 pipe flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
mailman unix - n n - - pipe flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.
${nexthop} ${user} amavis unix - - - - 2 smtp -o smtp_data_done_timeout=1200 -o
smtp_send_xforward_command=yes -o disable_dns_lookups=yes -o max_use=20 127.0.0.1:10025 inet
n - - - - smtpd -o content_filter= -o local_recipient_maps= -o relay_recipient_maps= -o
smtpd_restriction_classes= -o smtpd_delay_reject=no -o
smtpd_client_restrictions=permit_mynetworks,reject -o smtpd_helo_restrictions= -o
smtpd_sender_restrictions= -o smtpd_recipient_restrictions=permit_mynetworks,reject -o
smtpd_data_restrictions=reject_unauth_pipelining -o smtpd_end_of_data_restrictions= -o
mynetworks=127.0.0.0/8
-o smtpd_error_sleep_time=0 -o smtpd_soft_error_limit=1001 -o smtpd_hard_error_limit=1000 -o
smtpd_client_connection_count_limit=0 -o smtpd_client_connection_rate_limit=0 -o
receive_override_options=no_header_body_checks,no_unknown_re
mkdir /etc/postfix/maps vi /etc/postfix/maps/alias.cf
```

```
user = mail password = mailpassword dbname = mail table = alias select_field = destination where_field
= source hosts = 127.0.0.1 additional_conditions = AND `enabled` = 1
vi /etc/postfix/maps/domain.cf
user = mail password = mailpassword dbname = mail table = domain select_field = domain where_field
= domain hosts = 127.0.0.1 additional_conditions = AND `enabled` = 1
vi /etc/postfix/maps/user.cf
user = mail password = mailpassword dbname = mail table = user select_field =
CONCAT(SUBSTRING_INDEX(`email`, "@", -1), "/", SUBS
where_field = email hosts = 127.0.0.1 additional_conditions = AND `enabled` = 1
chmod 700 /etc/postfix/maps/* chown postfix:postfix /etc/postfix/maps/*
usermod -aG sasl postfix mkdir -p /etc/postfix/sasl vi /etc/postfix/sasl/smtpd.conf
pwcheck_method: saslauthd auxprop_plugin: sql mech_list: plain login sql_engine: mysql
sql_hostnames: 127.0.0.1 sql_user: mail sql_passwd: mailpassword sql_database: mail sql_select:
SELECT `password` FROM `user` WHERE `email` = "%u@%r"
mkdir -p /var/spool/postfix/var/run/saslauthd mv /etc/default/saslauthd{,.dist} vi /etc/default/saslauthd
MYSQL_SERVER localhost MYSQL_USERNAME mail MYSQL_PASSWORD mailpassword
MYSQL_PORT 0 MYSQL_DATABASE mail MYSQL_USER_TABLE user
MYSQL_CRYPT_PWFIELD password MYSQL_UID_FIELD 5000 MYSQL_GID_FIELD 5000
MYSQL_LOGIN_FIELD email MYSQL_HOME_FIELD "/var/spool/mail/virtual"
MYSQL_MAILDIR_FIELD CONCAT(SUBSTRING_INDEX(`email`, "@", -1), "/",
MYSQL_NAME_FIELD name MYSQL_QUOTA_FIELD quota
```

```
CREATE DATABASE `mail`; GRANT ALL ON `mail`.* TO "mail"@"localhost" IDENTIFIED BY
"mailpassword" FLUSH PRIVILEGES; USE `mail`; CREATE TABLE IF NOT EXISTS `alias` (
`source` VARCHAR(255) NOT NULL, `destination` VARCHAR(255) NOT NULL DEFAULT "",
`enabled` TINYINT UNSIGNED NOT NULL DEFAULT 1,
PRIMARY KEY (`source`) ) ENGINE=InnoDB DEFAULT CHARSET=utf8; CREATE TABLE IF
NOT EXISTS `domain` ( `domain` VARCHAR(255) NOT NULL DEFAULT "", `transport`
VARCHAR(255) NOT NULL DEFAULT "virtual:", `enabled` TINYINT UNSIGNED NOT NULL
DEFAULT 1, PRIMARY KEY (`domain`) ) ENGINE=InnoDB DEFAULT CHARSET=utf8; CREATE
TABLE IF NOT EXISTS `user` ( `email` VARCHAR(255) NOT NULL DEFAULT "", `password`
VARCHAR(255) NOT NULL DEFAULT "", `name` VARCHAR(255) DEFAULT NULL, `quota` INT
UNSIGNED DEFAULT NULL, `enabled` TINYINT UNSIGNED NOT NULL DEFAULT 1,
PRIMARY KEY (`email`) ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```
service saslauthd restart service postfix restart service courier-authdaemon restart service courier-pop
restart service courier-pop-ssl restart service courier-imap restart service courier-imap-ssl restart
```

## Results and Snapshots:



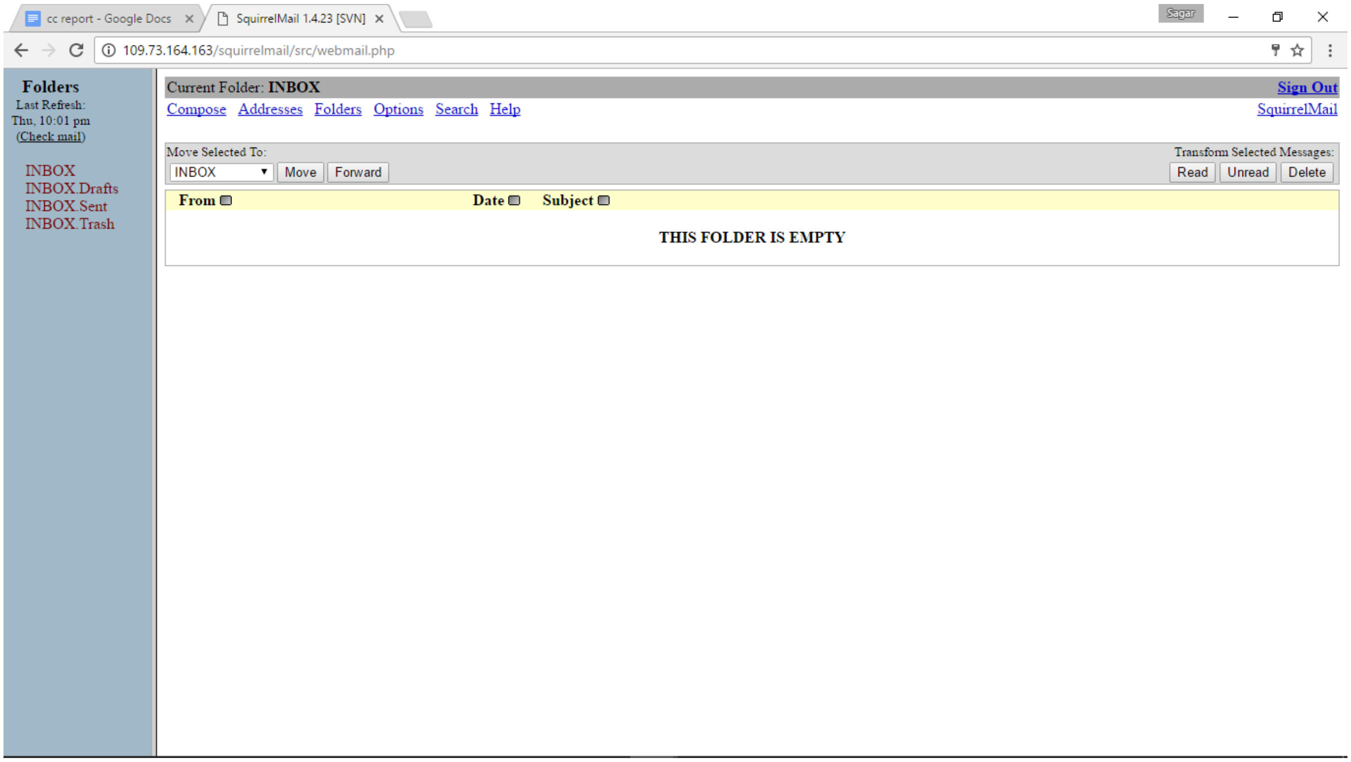
109.73.164.163/squirrelmail/src/login.php

SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

SquirrelMail Login

Name: Sagar
Password: •••••

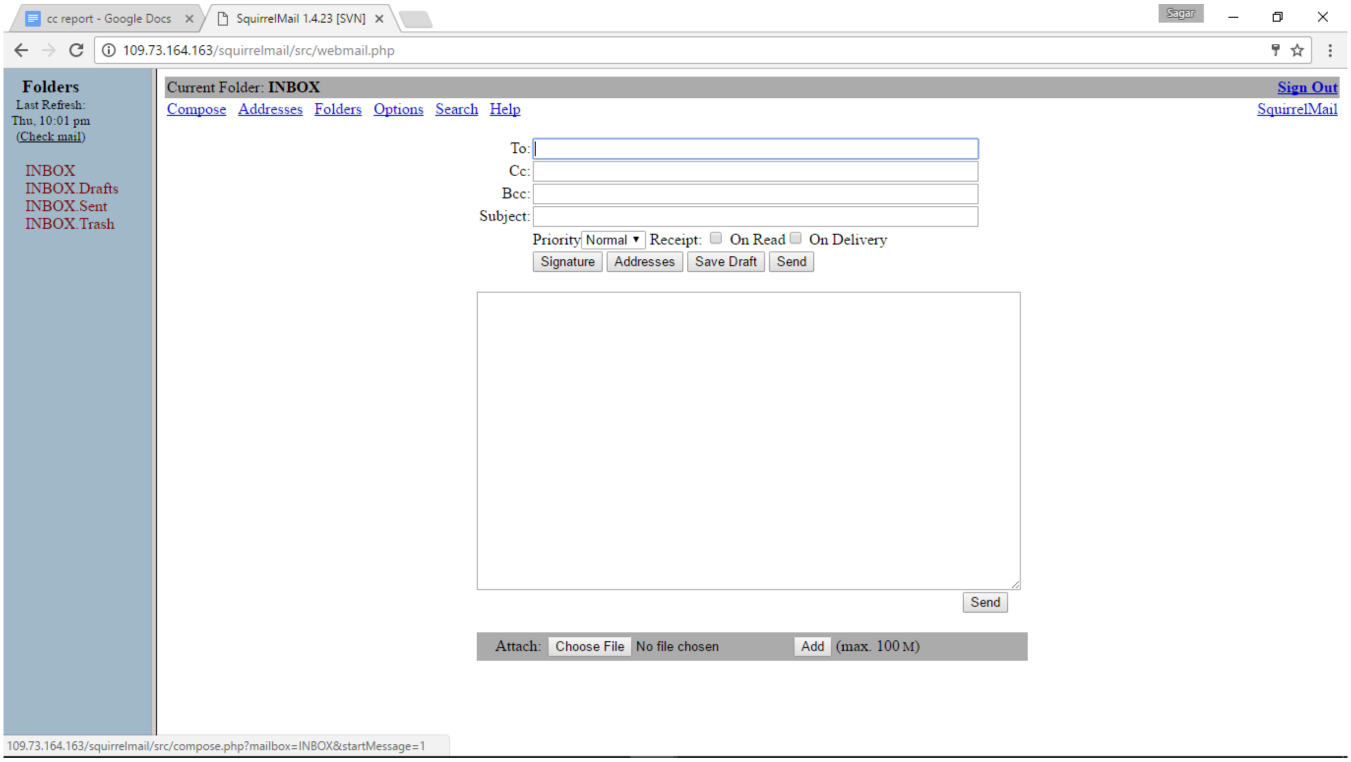
Login



109.73.164.163/squirrelmail/src/webmail.php

Current Folder: INBOX

THIS FOLDER IS EMPTY



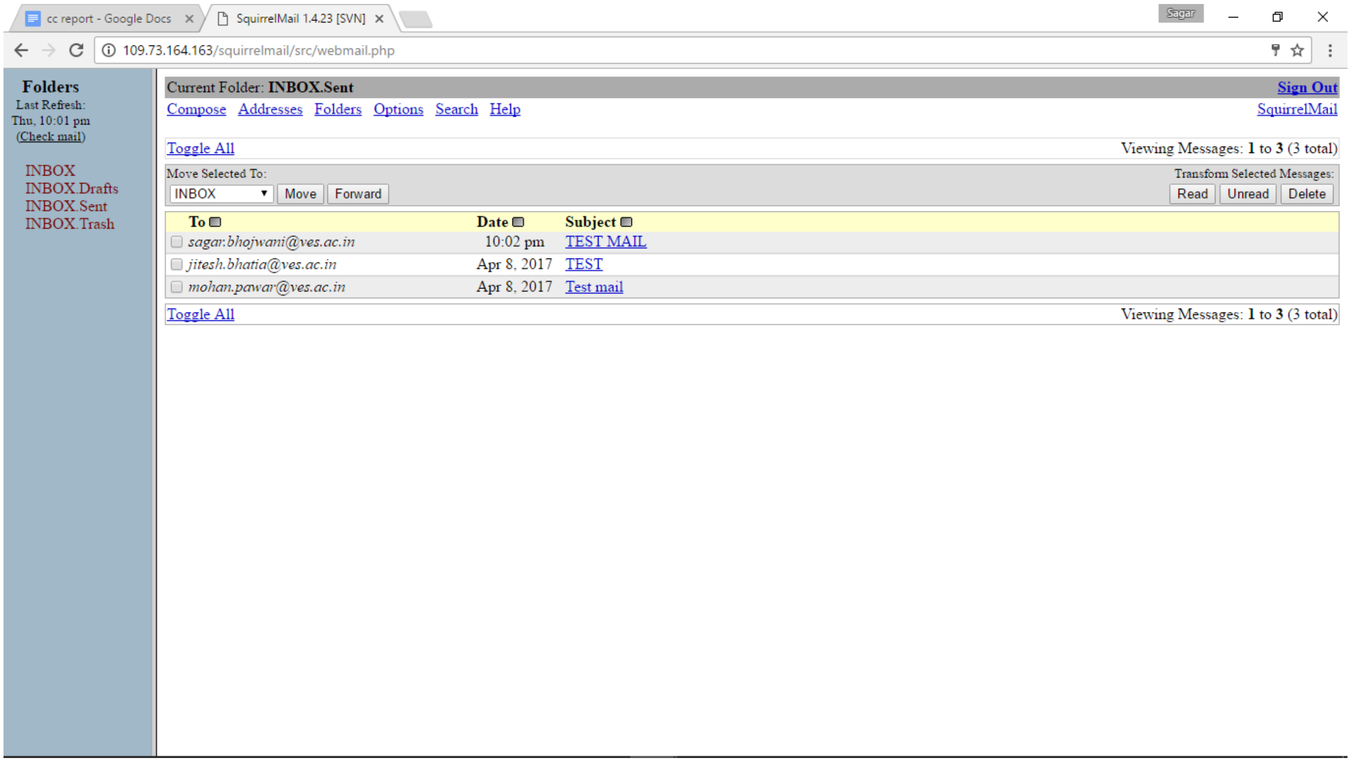
109.73.164.163/squirrelmail/src/webmail.php

Current Folder: INBOX

Priority Normal Receipt: □ On Read □ On Delivery

Attach: No file chosen (max. 100 M)

109.73.164.163/squirrelmail/src/compose.php?mailbox=INBOX&startMessage=1

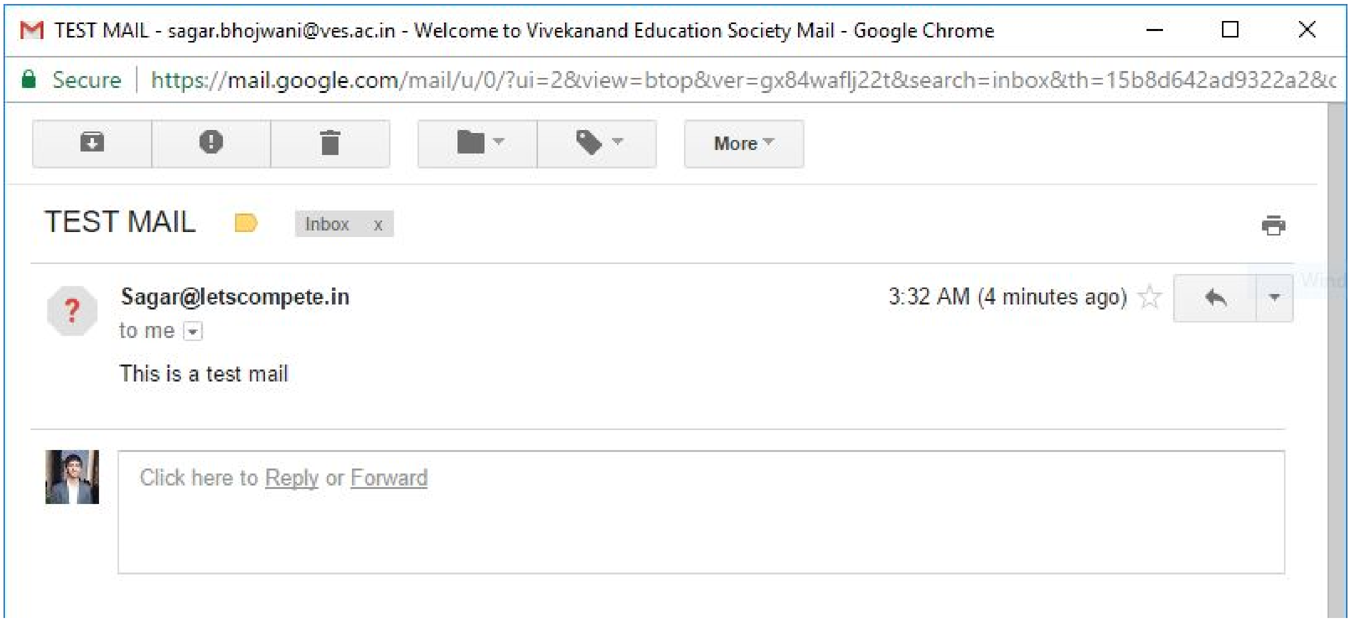


Current Folder: **INBOX.Sent**

Viewing Messages: **1** to **3** (3 total)

| | To | Date | Subject |
|---|---|---|---|
| □ | *sagar.bhojwani@ves.ac.in* | 10:02 pm | TEST MAIL |
| □ | *jitesh.bhatia@ves.ac.in* | Apr 8, 2017 | TEST |
| □ | *mohan.pawar@ves.ac.in* | Apr 8, 2017 | Test mail |

Viewing Messages: **1** to **3** (3 total)


TEST MAIL - sagar.bhojwani@ves.ac.in - Welcome to Vivekanand Education Society Mail - Google Chrome
Secure
https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=gx84waflj22t&search=inbox&th=15b8d642ad9322a2&c
More
Inbox x

TEST MAIL

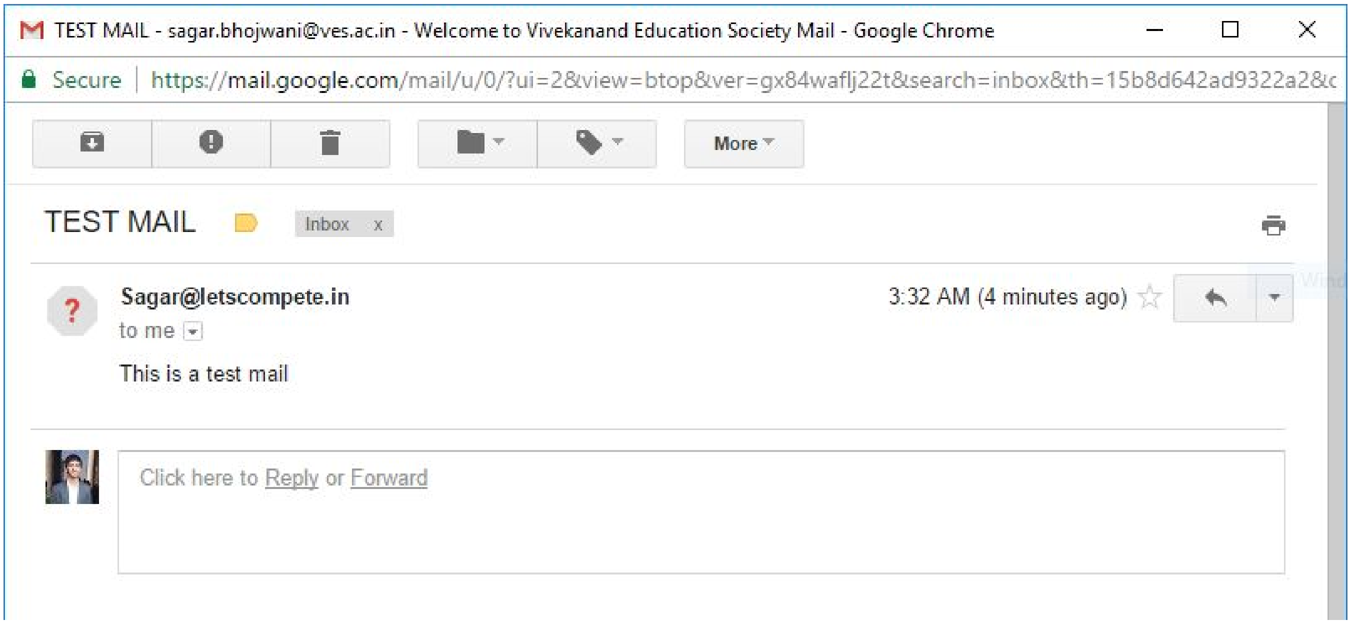
**Sagar@letscompete.in**

to me

3:32 AM (4 minutes ago)

This is a test mail

Click here to Reply or Forward



TEST MAIL - sagar.bhojwani@ves.ac.in - Welcome to Vivekanand Education Society Mail - Google Chrome

Secure | https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=gx84waflj22t&search=inbox&th=15b8d642ad9322a2&c

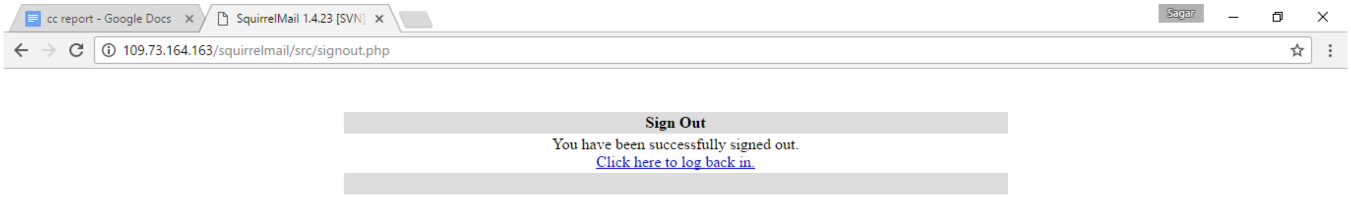
TEST MAIL

Sagar@letscompete.in
to me

3:32 AM (4 minutes ago)

This is a test mail

Click here to Reply or Forward



109.73.164.163/squirrelmail/src/signout.php

Sign Out

You have been successfully signed out.
Click here to log back in.

**Conclusion:** Thus a simple mail server has been setup on Ubuntu using SquirrelMail with functions like attaching files, signature, receipt, etc.

**References:** http://arstechnica.com

http://workaround.org