A · P · U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Individual Assignment

112024-MOD

System Network Administration

APD2F2411CS(CYB)

HAND OUT DATE: December 2025

HAND IN DATE: January 2025

Thaneswaran	TP070624

Table of Contents

Introduction 4

Requirements for email server 5

Install Postfix 7

Update and Upgrade your Rocky Linux by using this command: 7

What is Postfix and function of it? 8

Configuration for main.cf file 9

What is the Inet interface and how does it work? 10

What are Inet protocols? And why is it important to Linux email server? 10

What is the MAILDIR? Why do we need to configure it in our Postfix MAIN.CF file? 11

What is SMTPD certification and the difference between cert file and key file? 12

Configuration for master.cf file 13

What is the difference between master file and main file? Why do we require to configure SSL in master file? 13

Install dovecot 14

Install dovecot by using (**Sudo DNF install dovecot -y**) command. 14

- (**Sudo nano /etc/dovecot/conf.d/10-mail.conf**) 14
- (Sudo nano /etc/dovecot/conf.d/10-ssl.conf) 15
- (**Sudo nano /etc/dovecot/conf.d/10-master.conf**) 16
- **(Sudo nano /etc/dovecot/dovecot.main**) 17
- (**Sudo nano /etc/dovecot/conf.d/10-auth.conf**) 18

Enable, Restart, Start Dovecot and Postfix 19

Installing OpenSSL and creating the key and certificate 20

Create the keys and certificate for our SSL 21

Assigning permissions to key and certificate 22

Adding ports 23

Adding users 24

Testing email locally 24

Verify the ports and configurations 25

Dovecot read user 25

Update and Upgrade Ubuntu 26

Connecting the port 465 and 993 on Ubuntu 27

Install Thunderbird in Ubuntu client 28

Testing Email send and receive 32

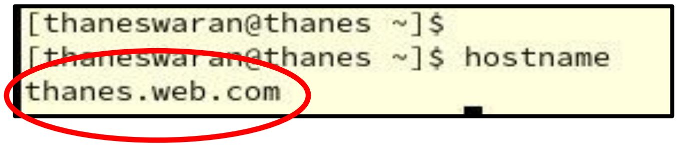
Conclusion 33
Troubleshooting 33

Introduction

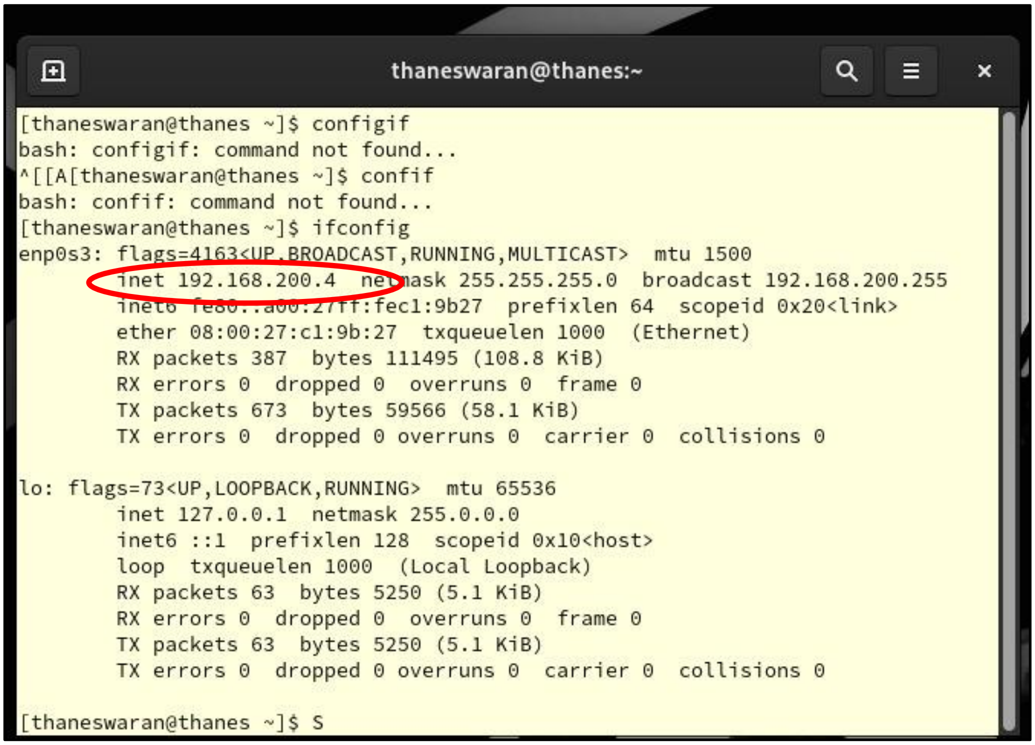
In this modern era, in IT industries most organizations or companies prefer to use Linux operating systems to keep their system and data securely. Moreover, Linux OS also plays a major role in keeping the data and files securely stored because Linux operating systems are not a user-friendly OS. Hereby, only Linux administrators or the people who used to Linux command only know the specific commands to do the configuration in Linux respectively. Furthermore, in this documentation I assigned to create one new email server for my ubuntu client. This is because Linux Email servers can be used for small organizations and can use a lot of storage without any significant reconfiguration because Linux OS can be used for scale to support any organization. In conclusion, people will get to know about how to create their own email server by using Linux OS step by step.

Requirements for email server

For creating a successful email server, we should have two important machines which is Ubuntu and Rocky. Ubuntu will work as our client meanwhile Rocky will work as our server. Hereby, we must have the correct hostname and DNS to create the email server without any interruption. Furthermore, our Ubuntu must connect with our Rocky server, and we should ping the Rocky server's Ip address successfully in our Ubuntu client. By there, we can confirm that our Rocky and Ubuntu were connected to each other.

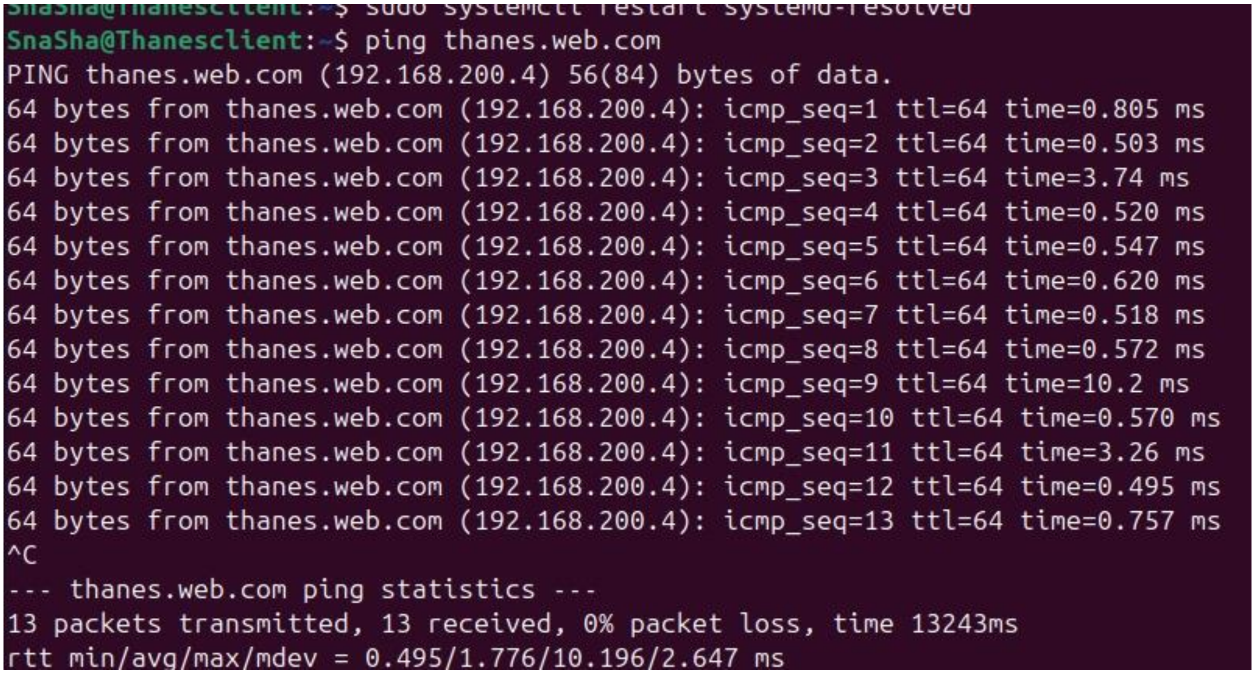


```
[thaneswaran@thanes ~]$
[thaneswaran@thanes ~]$ hostname
thanes.web.com
```



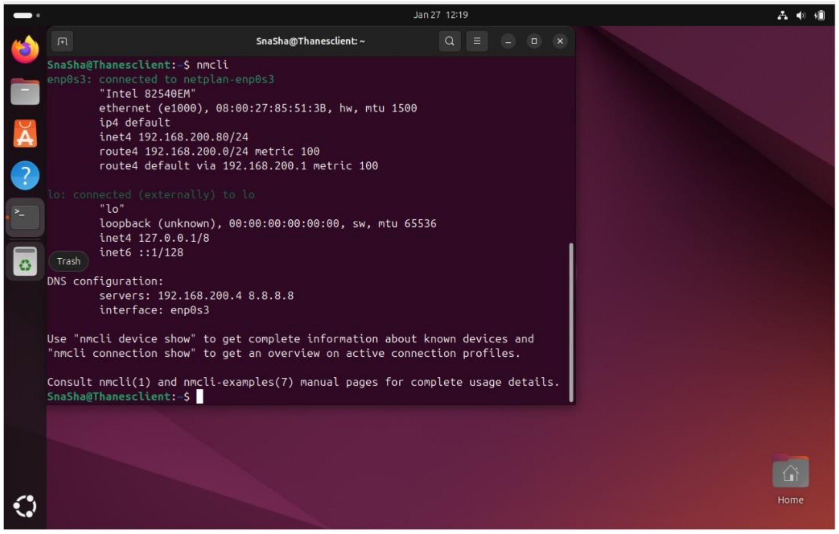
```
[thaneswaran@thanes ~]$ configif
bash: configif: command not found...
^[[A[thaneswaran@thanes ~]$ confif
bash: confif: command not found...
[thaneswaran@thanes ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.4  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::a00:27ff:fec1:9b27  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c1:9b:27  txqueuelen 1000  (Ethernet)
        RX packets 387  bytes 111495 (108.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 673  bytes 59566 (58.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 63  bytes 5250 (5.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 63  bytes 5250 (5.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[thaneswaran@thanes ~]$ S
```

- **Ping Rocky server in ubuntu client by use (ping thanes.web.com) command in Ubuntu Client.**



```
SnaSha@Thanesclient:~$ sudo systemctl restart systemd-resolved
SnaSha@Thanesclient:~$ ping thanes.web.com
PING thanes.web.com (192.168.200.4) 56(84) bytes of data.
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=1 ttl=64 time=0.805 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=2 ttl=64 time=0.503 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=3 ttl=64 time=3.74 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=4 ttl=64 time=0.520 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=5 ttl=64 time=0.547 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=6 ttl=64 time=0.620 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=7 ttl=64 time=0.518 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=8 ttl=64 time=0.572 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=9 ttl=64 time=10.2 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=10 ttl=64 time=0.570 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=11 ttl=64 time=3.26 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=12 ttl=64 time=0.495 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=13 ttl=64 time=0.757 ms
^C
--- thanes.web.com ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 13243ms
rtt min/avg/max/mdev = 0.495/1.776/10.196/2.647 ms
```

- **Check DNS by using (NMCLI) command to confirm the Ip address that we use currently.**

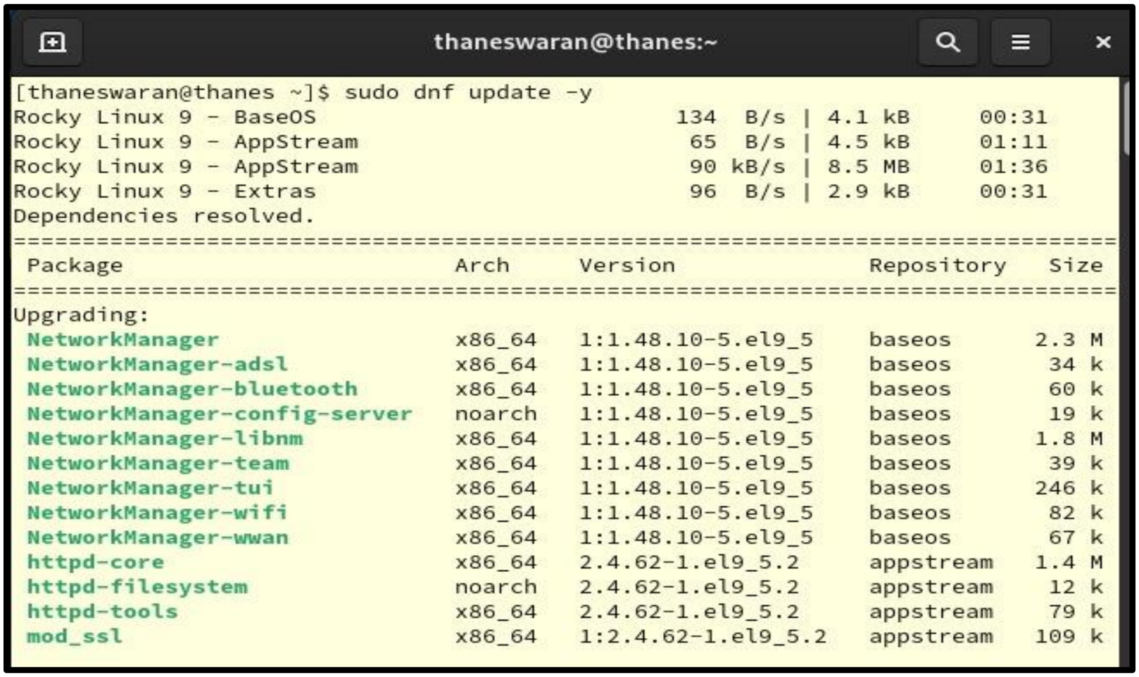


```
SnaSha@Thanesclient:~$ nmcli
enp0s3: connected to netplan-enp0s3
        "Intel 82540EM"
        ethernet (e1000), 08:00:27:85:51:3B, hw, mtu 1500
        ip4 default
        inet4 192.168.200.80/24
        route4 192.168.200.0/24 metric 100
        route4 default via 192.168.200.1 metric 100

lo: connected (externally) to lo
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
        inet4 127.0.0.1/8
        inet6 ::1/128

DNS configuration:
        servers: 192.168.200.4 8.8.8.8
        interface: enp0s3

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(7) manual pages for complete usage details.
SnaSha@Thanesclient:~$
```

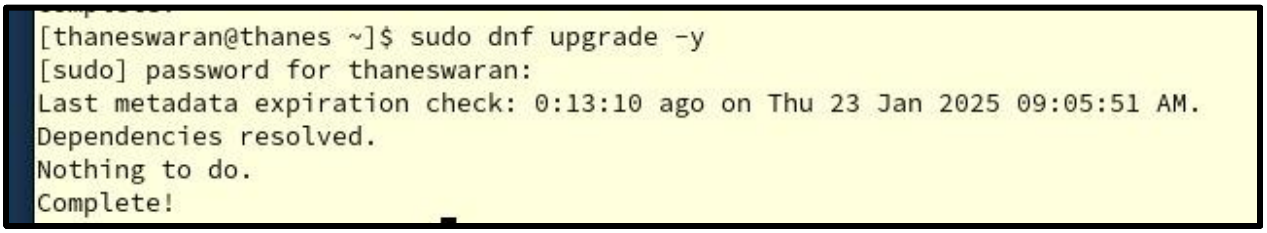
Install Postfix

Update and Upgrade your Rocky Linux by using this command:

- **Sudo dnf update -y**
- **Sudo dnf upgrade -y**



```
[thaneswaran@thanes ~]$ sudo dnf update -y
Rocky Linux 9 - BaseOS                          134  B/s | 4.1 kB     00:31
Rocky Linux 9 - AppStream                        65  B/s | 4.5 kB     01:11
Rocky Linux 9 - AppStream                        90 kB/s | 8.5 MB     01:36
Rocky Linux 9 - Extras                           96  B/s | 2.9 kB     00:31
Dependencies resolved.
================================================================================
 Package                       Arch     Version              Repository   Size
================================================================================
Upgrading:
 NetworkManager                x86_64   1:1.48.10-5.el9_5    baseos      2.3 M
 NetworkManager-adsl           x86_64   1:1.48.10-5.el9_5    baseos       34 k
 NetworkManager-bluetooth      x86_64   1:1.48.10-5.el9_5    baseos       60 k
 NetworkManager-config-server  noarch   1:1.48.10-5.el9_5    baseos       19 k
 NetworkManager-libnm          x86_64   1:1.48.10-5.el9_5    baseos      1.8 M
 NetworkManager-team           x86_64   1:1.48.10-5.el9_5    baseos       39 k
 NetworkManager-tui            x86_64   1:1.48.10-5.el9_5    baseos      246 k
 NetworkManager-wifi           x86_64   1:1.48.10-5.el9_5    baseos       82 k
 NetworkManager-wwan           x86_64   1:1.48.10-5.el9_5    baseos       67 k
 httpd-core                    x86_64   2.4.62-1.el9_5.2     appstream   1.4 M
 httpd-filesystem              noarch   2.4.62-1.el9_5.2     appstream    12 k
 httpd-tools                   x86_64   2.4.62-1.el9_5.2     appstream    79 k
 mod_ssl                       x86_64   1:2.4.62-1.el9_5.2   appstream   109 k
```

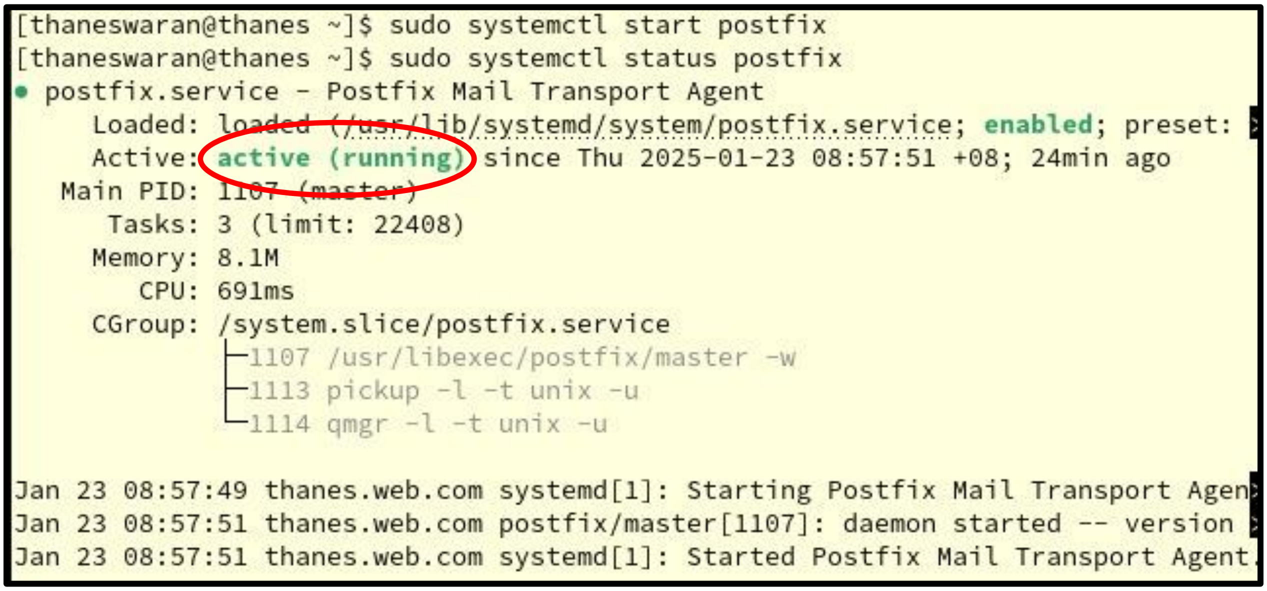


```
[thaneswaran@thanes ~]$ sudo dnf upgrade -y
[sudo] password for thaneswaran:
Last metadata expiration check: 0:13:10 ago on Thu 23 Jan 2025 09:05:51 AM.
Dependencies resolved.
Nothing to do.
Complete!
```

- **Sudo dnf install postfix.**

What is Postfix and function of it?

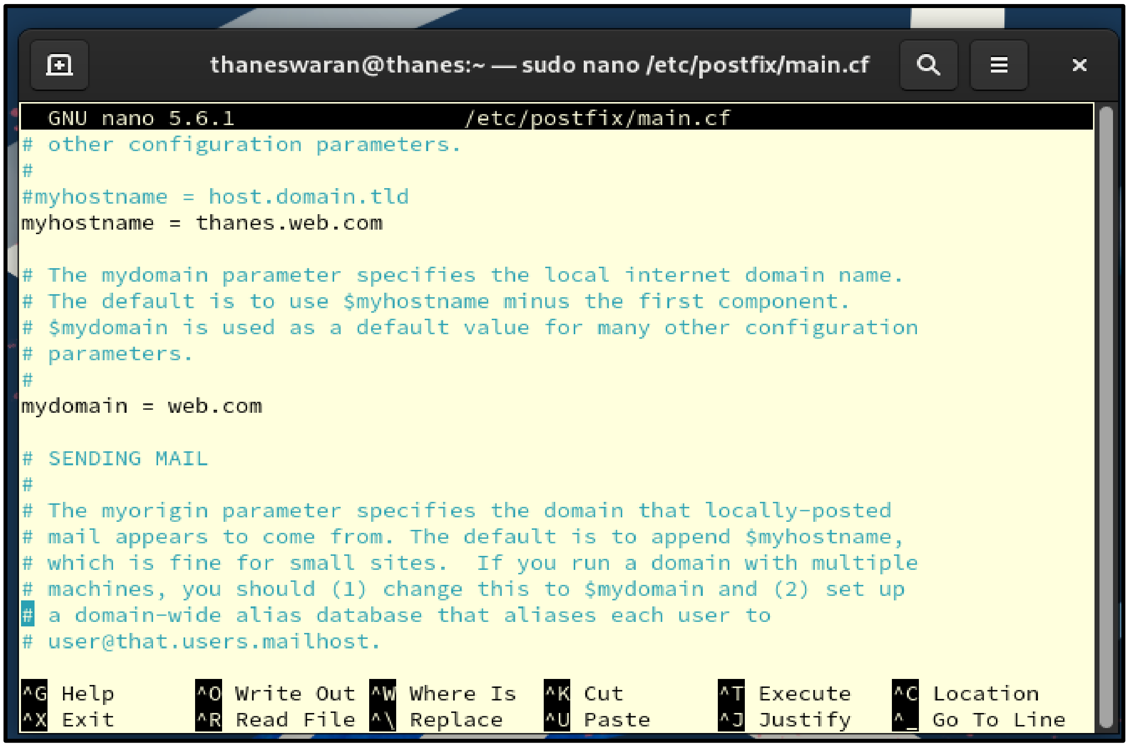
Postfix is a mail transfer agent (MTA), and it is used by Linux and Unix operating system to send and receive mail from servers and clients. Most of the organizations do their email server in this type of operating system to keep their email data and information securely. Moreover, the people like Linux administrators will easily configure the email server and it can help to send high compatible mails to others. For fully setup the email server we must configure the main.cf and master.cf files for setup our hostname and domain correctly. Moreover, we must set up my networks in simple words we have to set our static Ip address which is server Ip address for sending and receiving the mail in correct destination. Other than that, we must configure our SMTP feature for our email server. In short, what is the function of SMTP in email server is sending and relaying email from one to another server or client. On other hand, in Master.Conf file, we must configure the SMTPD.



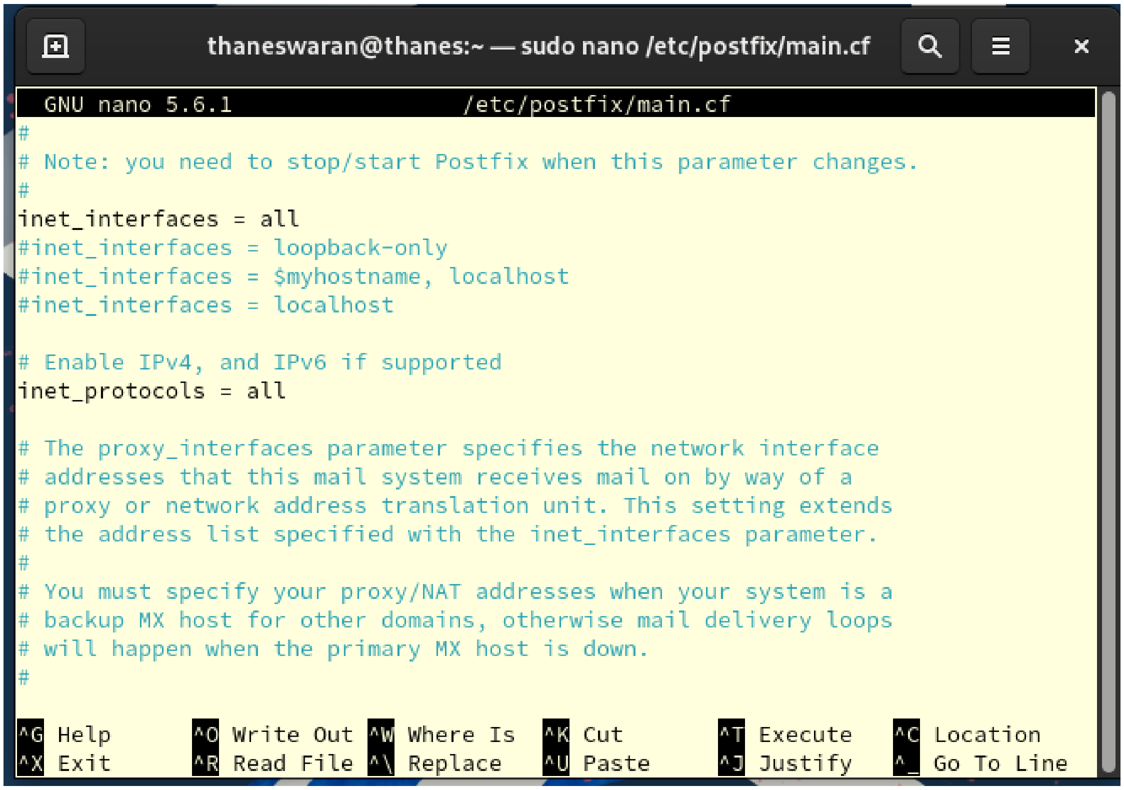
```
[thaneswaran@thanes ~]$ sudo systemctl start postfix
[thaneswaran@thanes ~]$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset:
     Active: active (running) since Thu 2025-01-23 08:57:51 +08; 24min ago
   Main PID: 1107 (master)
      Tasks: 3 (limit: 22408)
     Memory: 8.1M
        CPU: 691ms
     CGroup: /system.slice/postfix.service
             ├─1107 /usr/libexec/postfix/master -w
             ├─1113 pickup -l -t unix -u
             └─1114 qmgr -l -t unix -u

Jan 23 08:57:49 thanes.web.com systemd[1]: Starting Postfix Mail Transport Agen
Jan 23 08:57:51 thanes.web.com postfix/master[1107]: daemon started -- version
Jan 23 08:57:51 thanes.web.com systemd[1]: Started Postfix Mail Transport Agent.
```

Configuration for main.cf file

- **Sudo nano /etc/postfix/main.cf**



```
  GNU nano 5.6.1                  /etc/postfix/main.cf
# other configuration parameters.
#
#myhostname = host.domain.tld
myhostname = thanes.web.com

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = web.com

# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.

^G Help       ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit       ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```



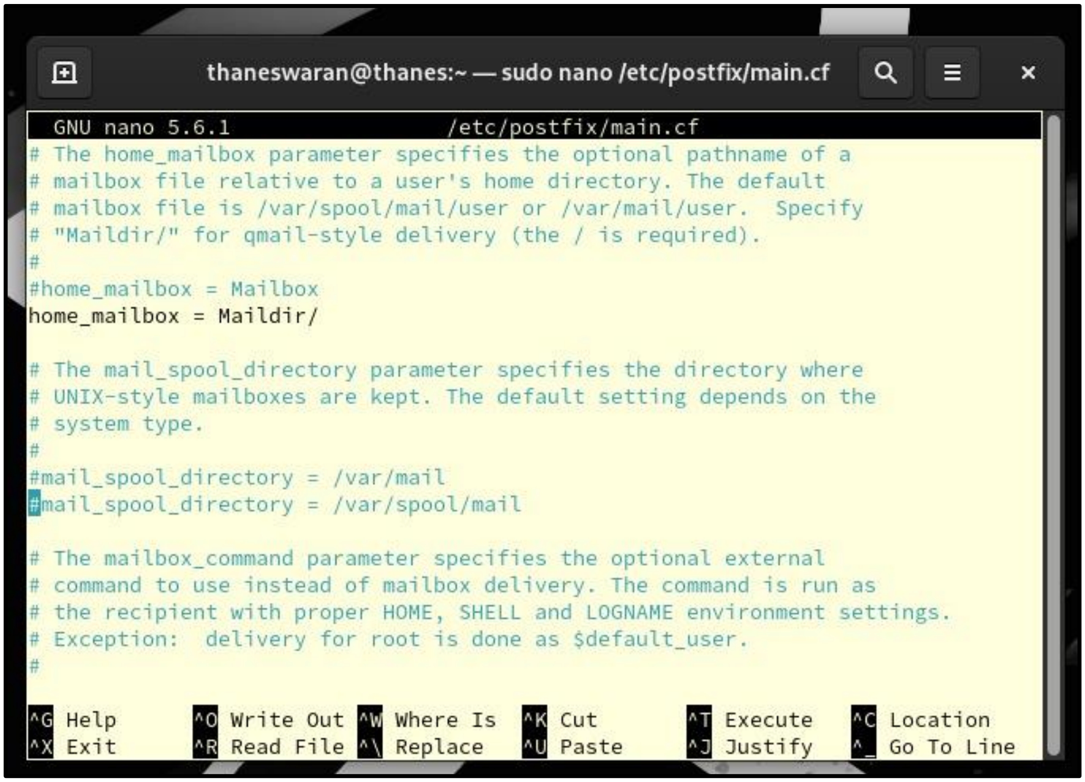
```
  GNU nano 5.6.1                  /etc/postfix/main.cf
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all
#inet_interfaces = loopback-only
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost

# Enable IPv4, and IPv6 if supported
inet_protocols = all

# The proxy_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on by way of a
# proxy or network address translation unit. This setting extends
# the address list specified with the inet_interfaces parameter.
#
# You must specify your proxy/NAT addresses when your system is a
# backup MX host for other domains, otherwise mail delivery loops
# will happen when the primary MX host is down.
#

^G Help       ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit       ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

What is the Inet interface and how does it work?

Why must we assign Inet Interface to all available networks? This is because, if we assign the interface to only one network for example, if we open the interface for only our localhost (127.0.0.1) it will send the email to only our server, in more detail the postfix only can send and receive the mail from its own server but if we assign the interface for all it can access all available networks and can send or receive the email from multiple servers or clients.

What are Inet protocols? And why is it important to Linux email server?

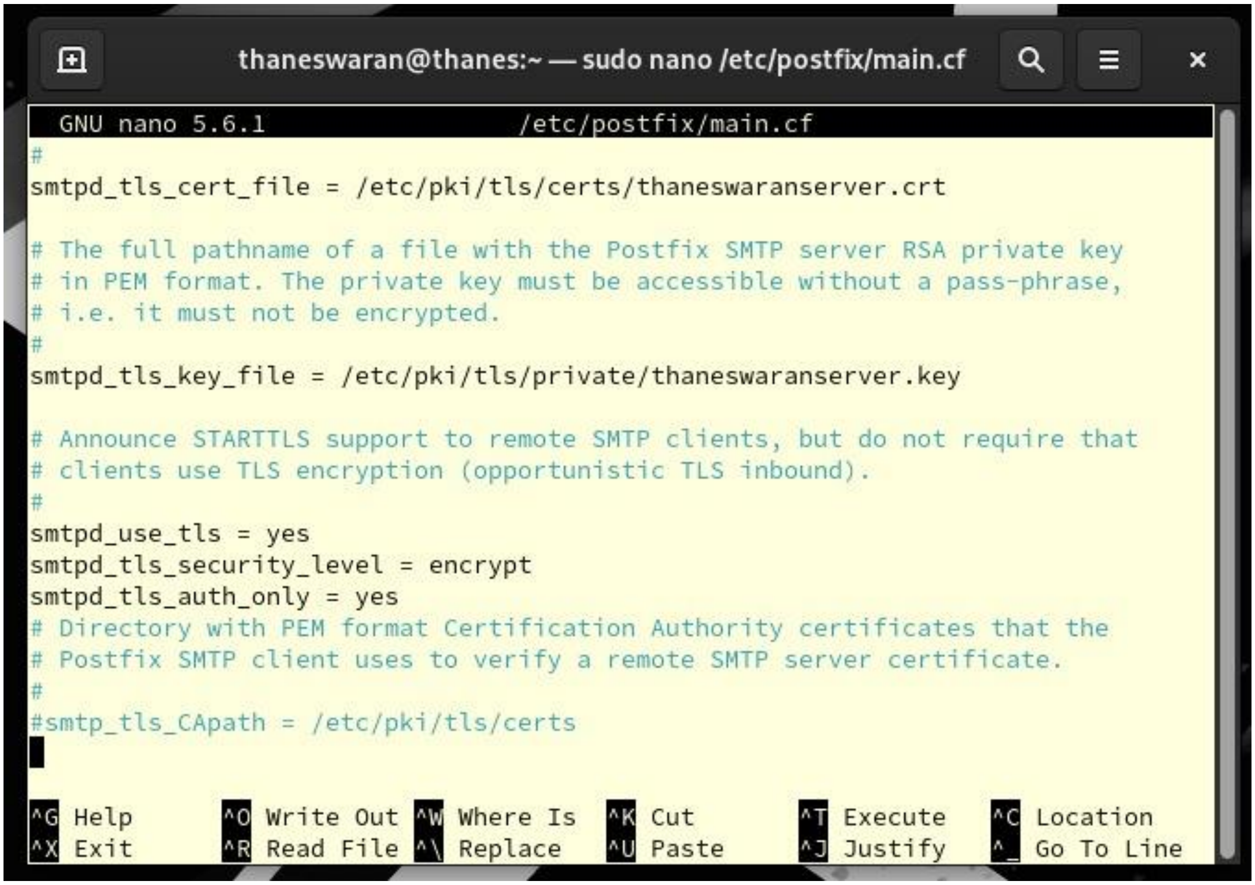
Inet protocols are a feature that assign Postfix to support both IPV4 and IPV6 for sending and receiving emails. Why its important? This is because, nowadays networks do not use the IP class for their organization, some will use IPV6, and the rest will rely on IPV4. Hereby, these Inet protocols will allow the Postfix to configure and access both IP classes for sending and receiving emails.



```
  GNU nano 5.6.1                 /etc/postfix/main.cf
# The home_mailbox parameter specifies the optional pathname of a
# mailbox file relative to a user's home directory. The default
# mailbox file is /var/spool/mail/user or /var/mail/user.  Specify
# "Maildir/" for qmail-style delivery (the / is required).
#
#home_mailbox = Mailbox
home_mailbox = Maildir/

# The mail_spool_directory parameter specifies the directory where
# UNIX-style mailboxes are kept. The default setting depends on the
# system type.
#
#mail_spool_directory = /var/mail
#mail_spool_directory = /var/spool/mail

# The mailbox_command parameter specifies the optional external
# command to use instead of mailbox delivery. The command is run as
# the recipient with proper HOME, SHELL and LOGNAME environment settings.
# Exception:  delivery for root is done as $default_user.
#

^G Help        ^O Write Out  ^W Where Is   ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File  ^\ Replace    ^U Paste       ^J Justify     ^_ Go To Line
```

What is the MAILDIR? Why do we need to configure it in our Postfix MAIN.CF file?

- MAILDIR stands for Mail directory or in a more understandable way is its email storage. Furthermore, Mail directory will store the email data, and it will automatically separate the emails into three components which is (TMP/) Temporary storage for incoming emails that have been delivered yet, (NEW/) the emails that have not been read by any users and (CUR/) is a storage for saved the emails that read and seen by the users. Hereby, most of the organizations that use email servers in Linux operating systems will be configuring Mail directory to manage their emails efficiently. . Control X and press Y to save the configuration.

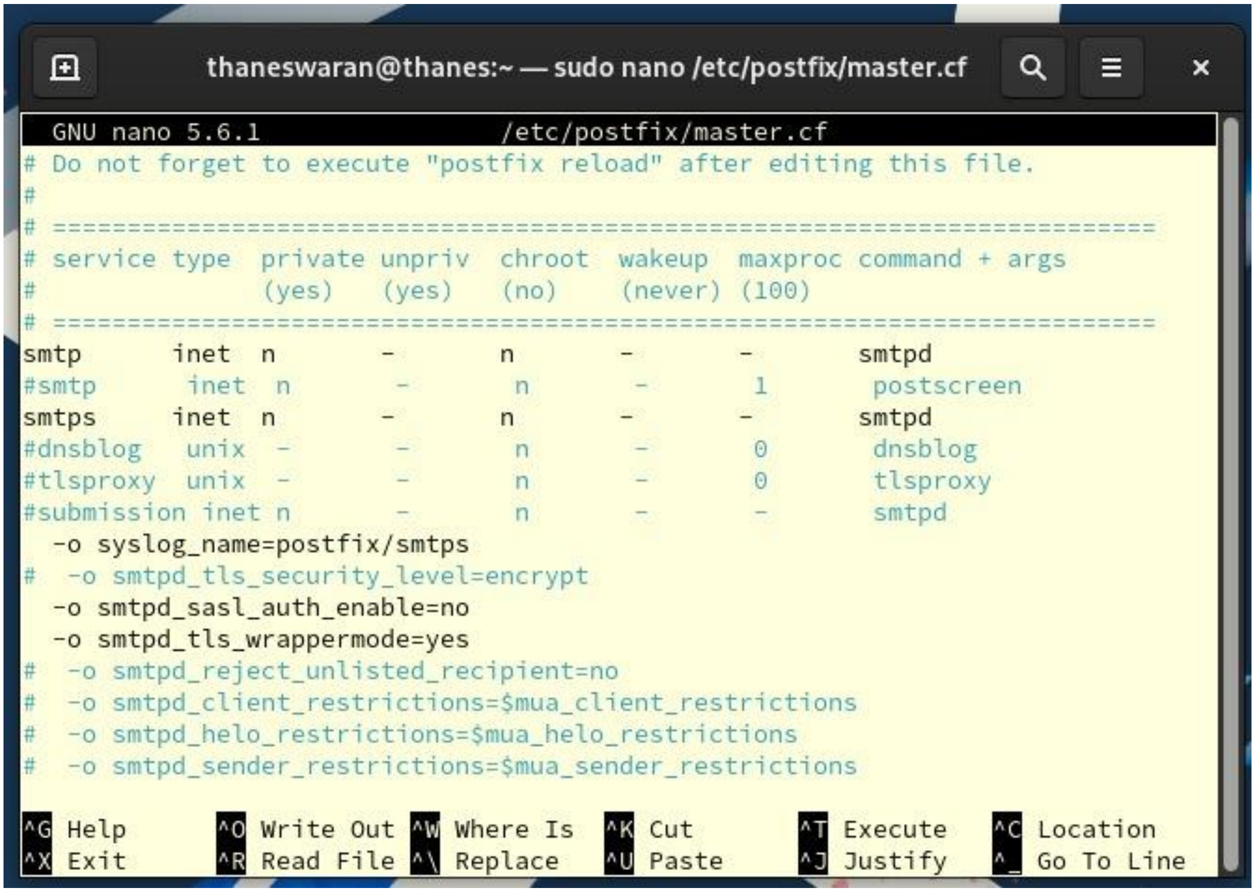


```
  GNU nano 5.6.1                  /etc/postfix/main.cf
#
smtpd_tls_cert_file = /etc/pki/tls/certs/thaneswaranserver.crt

# The full pathname of a file with the Postfix SMTP server RSA private key
# in PEM format. The private key must be accessible without a pass-phrase,
# i.e. it must not be encrypted.
#
smtpd_tls_key_file = /etc/pki/tls/private/thaneswaranserver.key

# Announce STARTTLS support to remote SMTP clients, but do not require that
# clients use TLS encryption (opportunistic TLS inbound).
#
smtpd_use_tls = yes
smtpd_tls_security_level = encrypt
smtpd_tls_auth_only = yes
# Directory with PEM format Certification Authority certificates that the
# Postfix SMTP client uses to verify a remote SMTP server certificate.
#
#smtp_tls_CApath = /etc/pki/tls/certs


^G Help       ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit       ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

What is SMTPD certification and the difference between cert file and key file?

- SMTPD certification is a digital certificate for email purposes like receiving and sending messages or information to other clients or server to give a secure connection by TLS (Transport Layer Security). It can help to encrypt the conservation or data between servers and clients securely, because of this unauthorized people cannot get or read their organization’s data easily. Moreover, we must save that file in two locations which is certs and private folder. In more detail, the function for the Certs folder is used for testing or normal troubleshooting and it can be accessed by unauthorized people too but the cert in private folder is encrypted by it for safety purposes. . Control X and press Y to save the configuration.

Configuration for master.cf file



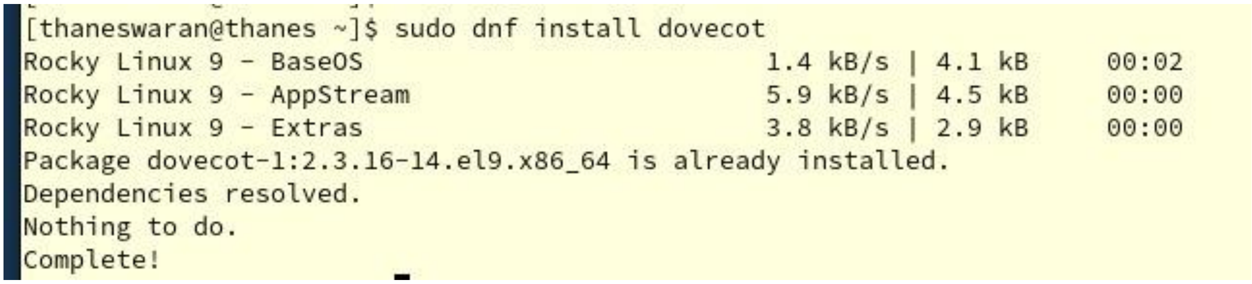
```
  GNU nano 5.6.1                  /etc/postfix/master.cf
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
#smtp      inet  n       -       n       -       1       postscreen
smtps     inet  n       -       n       -       -       smtpd
#dnsblog   unix  -       -       n       -       0       dnsblog
#tlsproxy  unix  -       -       n       -       0       tlsproxy
#submission inet n       -       n       -       -       smtpd
  -o syslog_name=postfix/smtps
#  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=no
  -o smtpd_tls_wrappermode=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

What is the difference between master file and main file? Why do we require to configure SSL in master file?

As we said SSL is a security protocol that ensures to protect the data between Client (Ubuntu) and Server (Rocky). Hereby, it can block the email connection from unauthorized access and can prevent the “man in the middle” attacks. Furthermore, with an SSL certificate we can build trust among the users because most of the users in this modern era trust the HTTPS websites in their browser. Moreover, we must enable TLS for specific ports such as 456 and 993 ports. This is the primary reason why we should configure SSL in master.cf file. In the MAIN.CF file we only can-do general TLS default settings and it will apply to overall postfix process but if we configure it MASTER.CF, it will work in specific process.

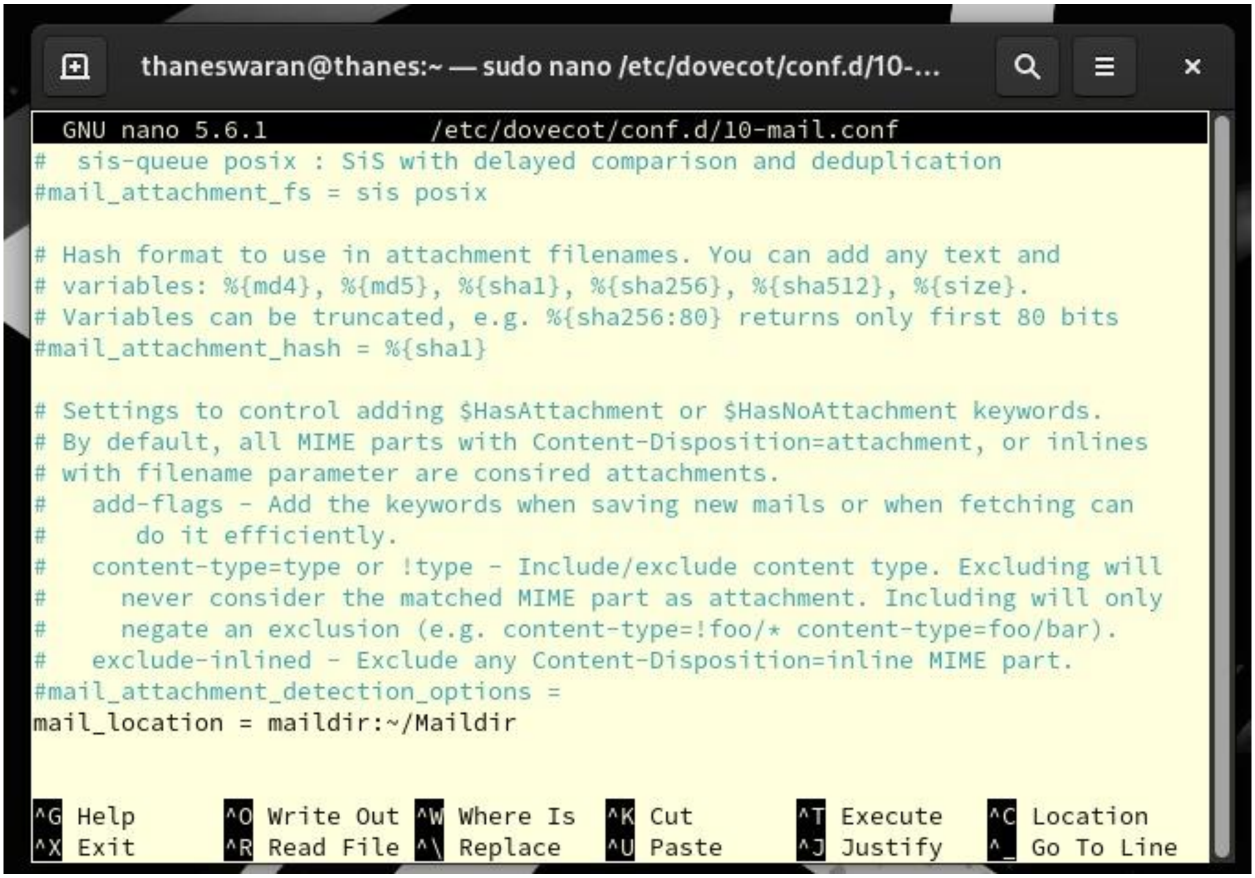
Install dovecot

Install dovecot by using (**Sudo DNF install dovecot -y**) command.



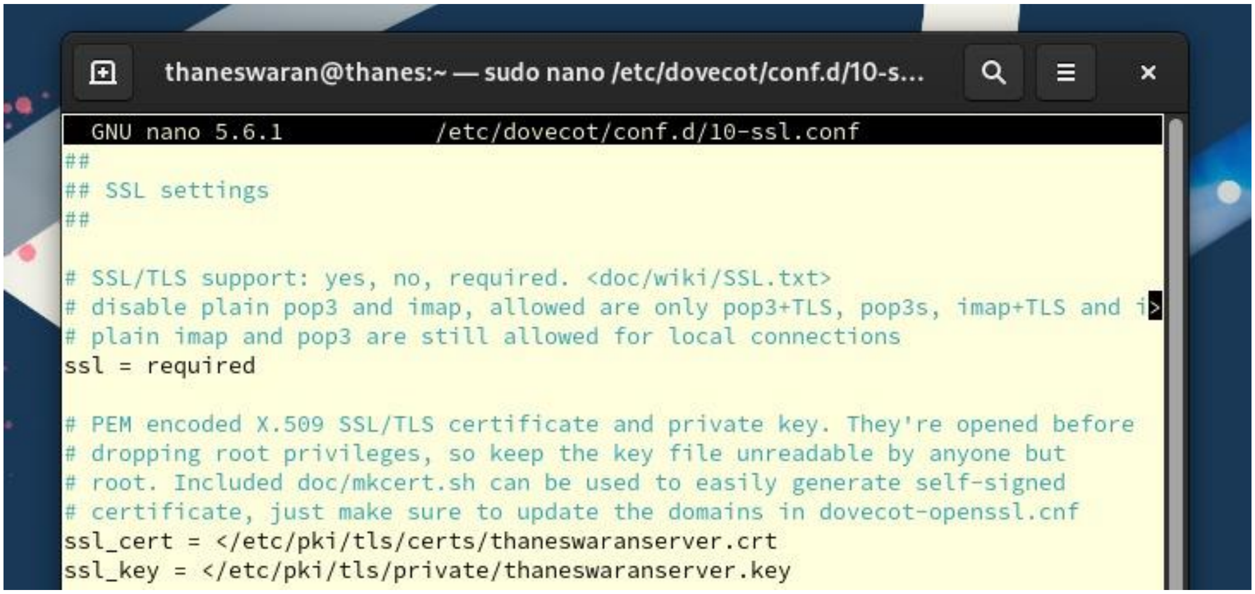
```
[thaneswaran@thanes ~]$ sudo dnf install dovecot
Rocky Linux 9 - BaseOS                          1.4 kB/s | 4.1 kB     00:02
Rocky Linux 9 - AppStream                       5.9 kB/s | 4.5 kB     00:00
Rocky Linux 9 - Extras                          3.8 kB/s | 2.9 kB     00:00
Package dovecot-1:2.3.16-14.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

- We must configure 4 types of files which are 10-mail.conf, 10-ssl.conf, dovecot.conf, 10-auth.conf and 10-master.conf.
- (**Sudo nano /etc/dovecot/conf.d/10-mail.conf**) command for access 10-mail.conf. In this file we must configure the mail location to Mail directory and the function remains the same as we state in postfix configuration.



```
  GNU nano 5.6.1            /etc/dovecot/conf.d/10-mail.conf
#  sis-queue posix : SiS with delayed comparison and deduplication
#mail_attachment_fs = sis posix

# Hash format to use in attachment filenames. You can add any text and
# variables: %{md4}, %{md5}, %{sha1}, %{sha256}, %{sha512}, %{size}.
# Variables can be truncated, e.g. %{sha256:80} returns only first 80 bits
#mail_attachment_hash = %{sha1}

# Settings to control adding $HasAttachment or $HasNoAttachment keywords.
# By default, all MIME parts with Content-Disposition=attachment, or inlines
# with filename parameter are consired attachments.
#   add-flags - Add the keywords when saving new mails or when fetching can
#      do it efficiently.
#   content-type=type or !type - Include/exclude content type. Excluding will
#     never consider the matched MIME part as attachment. Including will only
#     negate an exclusion (e.g. content-type=!foo/* content-type=foo/bar).
#   exclude-inlined - Exclude any Content-Disposition=inline MIME part.
#mail_attachment_detection_options =
mail_location = maildir:~/Maildir

^G Help       ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit       ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- (**Sudo nano /etc/dovecot/conf.d/10-ssl.conf**) command for access the SSL file in dovecot.

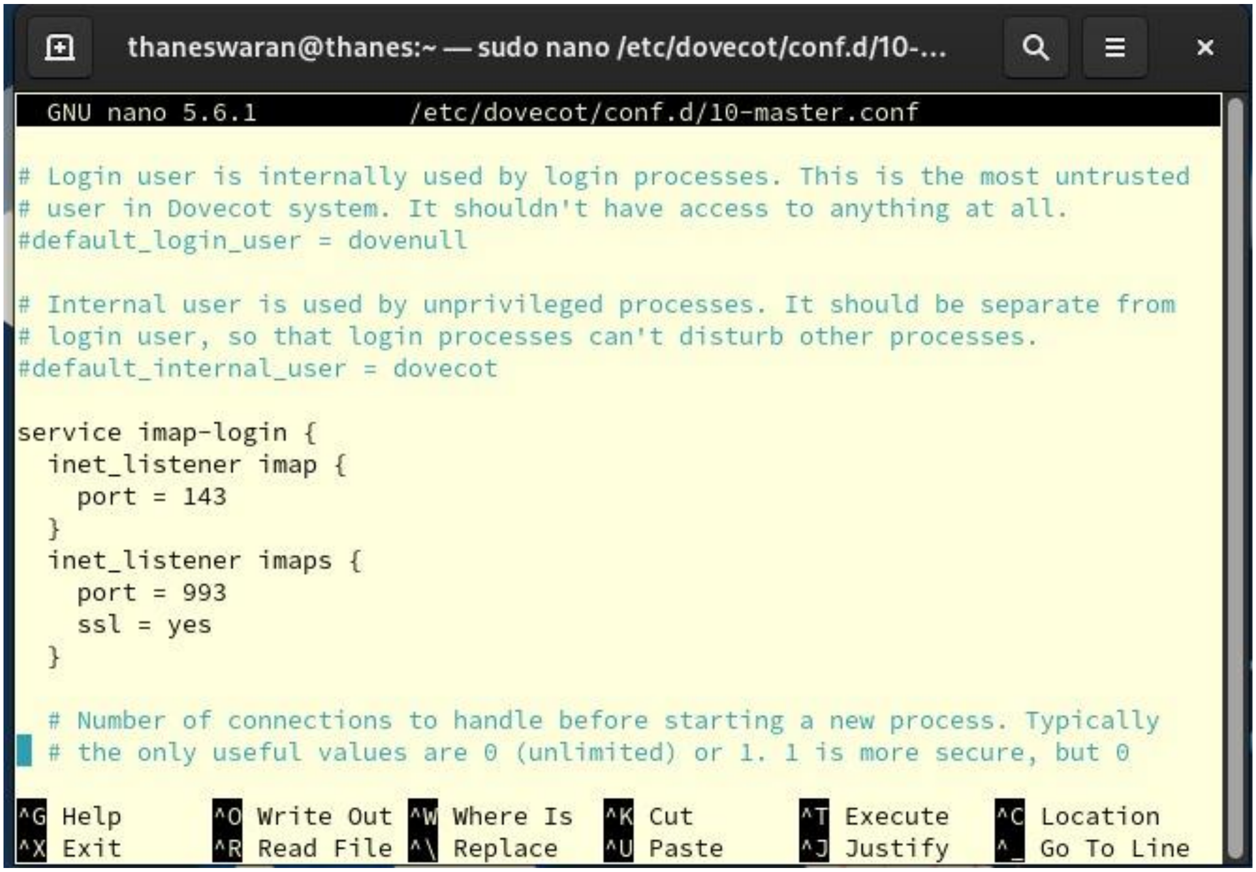


thaneswaran@thanes:~ — sudo nano /etc/dovecot/conf.d/10-s...

```
  GNU nano 5.6.1            /etc/dovecot/conf.d/10-ssl.conf
##
## SSL settings
##

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
# disable plain pop3 and imap, allowed are only pop3+TLS, pop3s, imap+TLS and i>
# plain imap and pop3 are still allowed for local connections
ssl = required

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/pki/tls/certs/thaneswaranserver.crt
ssl_key = </etc/pki/tls/private/thaneswaranserver.key
```

- In this file we have opened the SSL as required, and we must mention our SSL certificate that we are going to create in a few minutes. We must create a two folder for that SSL certificate. One is for certs files and another for private. The difference between both files is in the certificate folder we can use the certificate anytime for any purpose but in the private folder SSL ensures the authentication from authorized people. So, we cannot use any file or data that we saved in private folder through SSL configuration. . Control X and press Y to save the configuration.

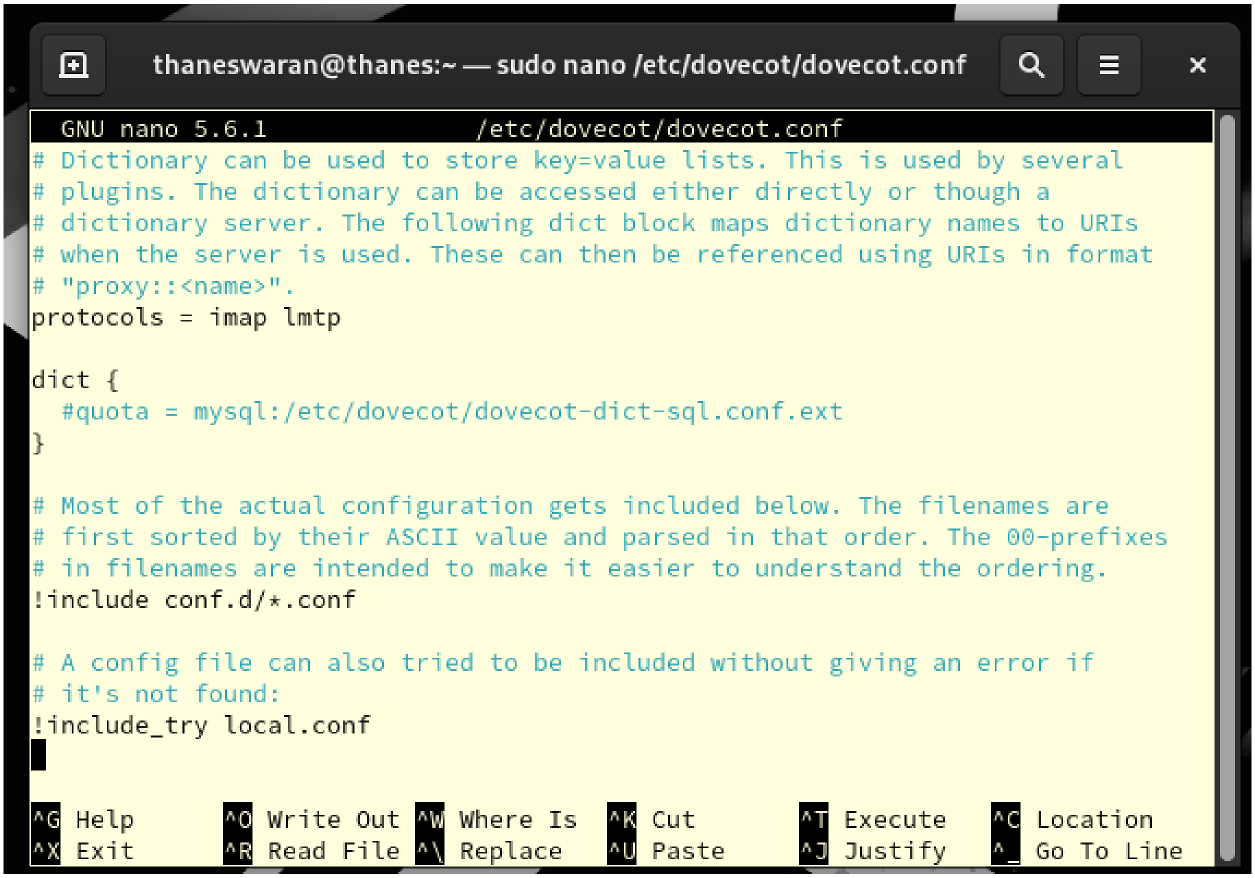
- (**Sudo nano /etc/dovecot/conf.d/10-master.conf**) command for access the master file in dovecot.



```
 GNU nano 5.6.1           /etc/dovecot/conf.d/10-master.conf

# Login user is internally used by login processes. This is the most untrusted
# user in Dovecot system. It shouldn't have access to anything at all.
#default_login_user = dovenull

# Internal user is used by unprivileged processes. It should be separate from
# login user, so that login processes can't disturb other processes.
#default_internal_user = dovecot

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

  # Number of connections to handle before starting a new process. Typically
  # the only useful values are 0 (unlimited) or 1. 1 is more secure, but 0

^G Help        ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit        ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

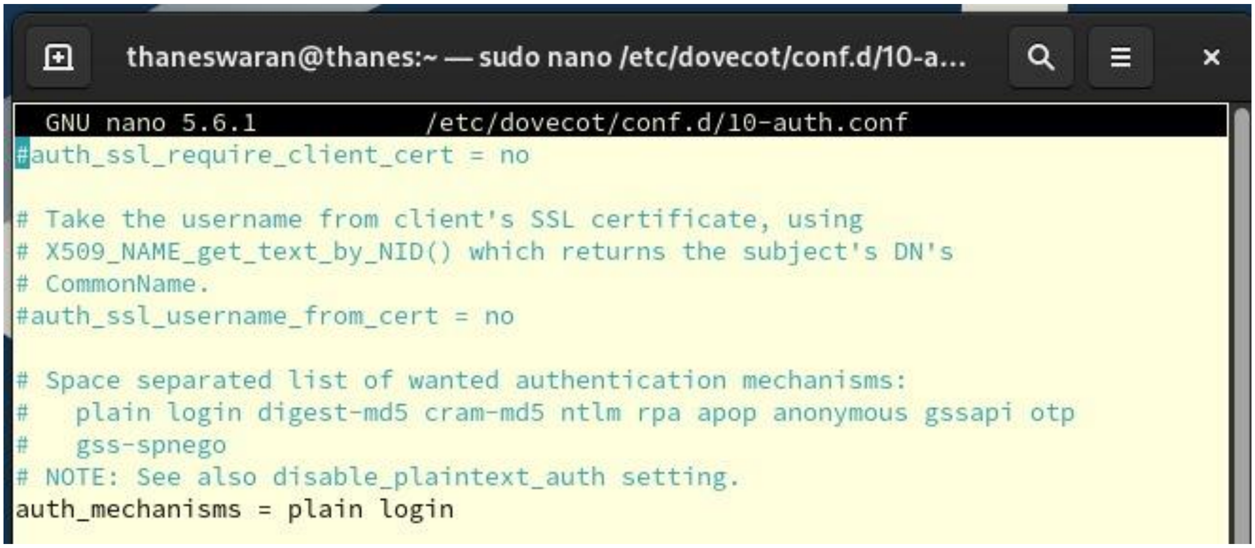
- In this master file we should give access to specific ports that we are going to use later to create users in thunderbird. As I said before in Postfix configuration, the purpose of the master file is we should configure specifically such as SSL or ports. Control X and press Y to save the configuration.

- **(Sudo nano /etc/dovecot/dovecot.main**) this command for access to the dovecot main file is configure the protocols to IMAP port. The function of IMAP is it can centralize the email storage and protect it, hereby we can lose our email data even though the device will totally damage. Control X and press Y to save the configuration.



```
  GNU nano 5.6.1              /etc/dovecot/dovecot.conf
# Dictionary can be used to store key=value lists. This is used by several
# plugins. The dictionary can be accessed either directly or though a
# dictionary server. The following dict block maps dictionary names to URIs
# when the server is used. These can then be referenced using URIs in format
# "proxy::<name>".
protocols = imap lmtp

dict {
  #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
}

# Most of the actual configuration gets included below. The filenames are
# first sorted by their ASCII value and parsed in that order. The 00-prefixes
# in filenames are intended to make it easier to understand the ordering.
!include conf.d/*.conf

# A config file can also tried to be included without giving an error if
# it's not found:
!include_try local.conf


^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

- (**Sudo nano /etc/dovecot/conf.d/10-auth.conf**) command for access to the auth file in dovecot.

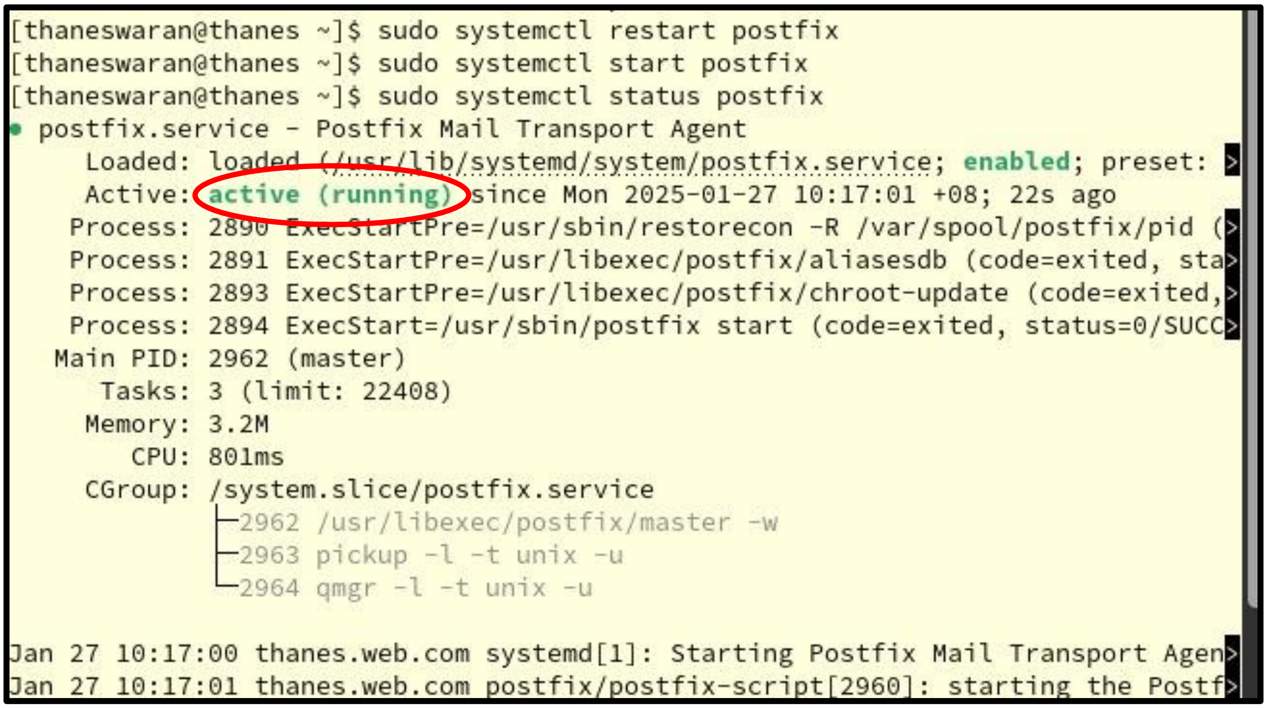


thaneswaran@thanes:~ — sudo nano /etc/dovecot/conf.d/10-a...

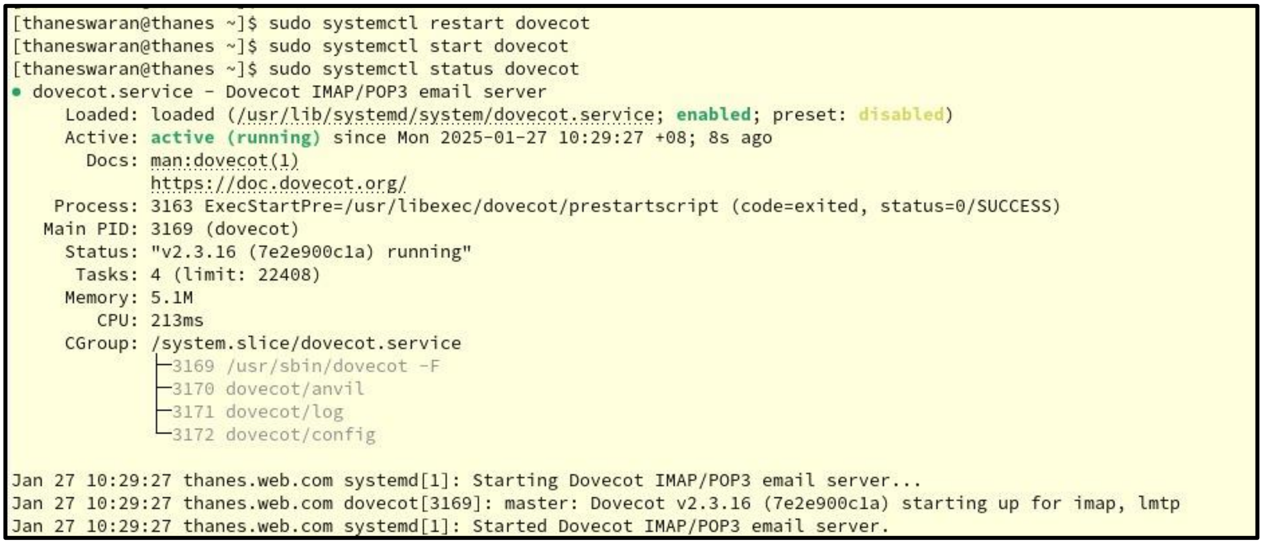
```
  GNU nano 5.6.1           /etc/dovecot/conf.d/10-auth.conf
#auth_ssl_require_client_cert = no

# Take the username from client's SSL certificate, using
# X509_NAME_get_text_by_NID() which returns the subject's DN's
# CommonName.
#auth_ssl_username_from_cert = no

# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login
```

Auth_mechanism refers to authentication methods that are used in our email server like SMTP, IMAP or POP3. The client will send the username and password in two methods which is Plain and Login. In Plain, the client will not encrypt the username and password in one single string and then send it to the Rocky server. On other hand, Login will do this process differently from the Plain method. It will send the username and password in two files, and it will be encoded by base64. Hereby, it can prevent the password cracking attack all from cyber-crimes.

Enable, Restart, Start Dovecot and Postfix



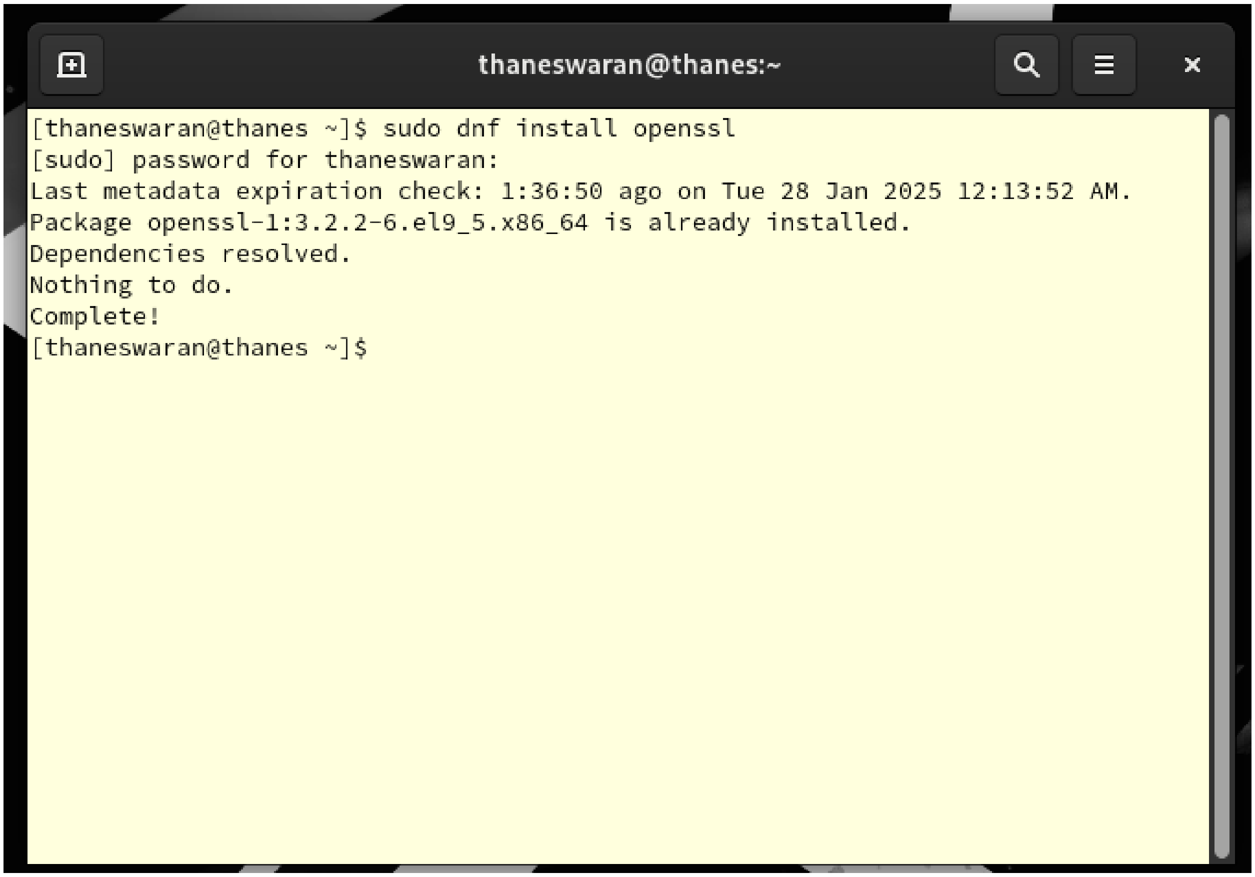
```
[thaneswaran@thanes ~]$ sudo systemctl restart postfix
[thaneswaran@thanes ~]$ sudo systemctl start postfix
[thaneswaran@thanes ~]$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: >
     Active: active (running) since Mon 2025-01-27 10:17:01 +08; 22s ago
    Process: 2890 ExecStartPre=/usr/sbin/restorecon -R /var/spool/postfix/pid (>
    Process: 2891 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, sta>
    Process: 2893 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited,>
    Process: 2894 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCC>
   Main PID: 2962 (master)
      Tasks: 3 (limit: 22408)
     Memory: 3.2M
        CPU: 801ms
     CGroup: /system.slice/postfix.service
             ├─2962 /usr/libexec/postfix/master -w
             ├─2963 pickup -l -t unix -u
             └─2964 qmgr -l -t unix -u

Jan 27 10:17:00 thanes.web.com systemd[1]: Starting Postfix Mail Transport Agen>
Jan 27 10:17:01 thanes.web.com postfix/postfix-script[2960]: starting the Postf>
```



```
[thaneswaran@thanes ~]$ sudo systemctl restart dovecot
[thaneswaran@thanes ~]$ sudo systemctl start dovecot
[thaneswaran@thanes ~]$ sudo systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
     Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled; preset: disabled)
     Active: active (running) since Mon 2025-01-27 10:29:27 +08; 8s ago
       Docs: man:dovecot(1)
             https://doc.dovecot.org/
    Process: 3163 ExecStartPre=/usr/libexec/dovecot/prestartscript (code=exited, status=0/SUCCESS)
   Main PID: 3169 (dovecot)
     Status: "v2.3.16 (7e2e900c1a) running"
      Tasks: 4 (limit: 22408)
     Memory: 5.1M
        CPU: 213ms
     CGroup: /system.slice/dovecot.service
             ├─3169 /usr/sbin/dovecot -F
             ├─3170 dovecot/anvil
             ├─3171 dovecot/log
             └─3172 dovecot/config

Jan 27 10:29:27 thanes.web.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
Jan 27 10:29:27 thanes.web.com dovecot[3169]: master: Dovecot v2.3.16 (7e2e900c1a) starting up for imap, lmtp
Jan 27 10:29:27 thanes.web.com systemd[1]: Started Dovecot IMAP/POP3 email server.
```

Installing OpenSSL and creating the key and certificate

(Sudo dnf install openssl) command for downloading SSL.

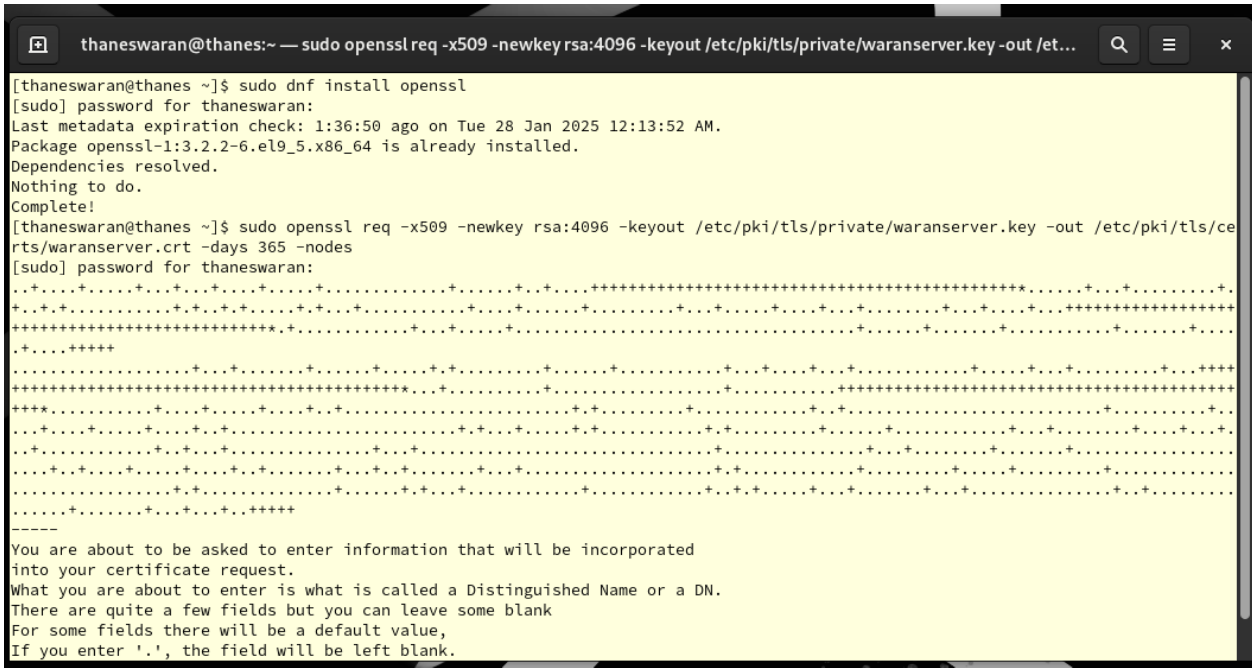


```
[thaneswaran@thanes ~]$ sudo dnf install openssl
[sudo] password for thaneswaran:
Last metadata expiration check: 1:36:50 ago on Tue 28 Jan 2025 12:13:52 AM.
Package openssl-1:3.2.2-6.el9_5.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[thaneswaran@thanes ~]$
```

- After you download the OpenSSL, it will show like this, if the installation was successful.

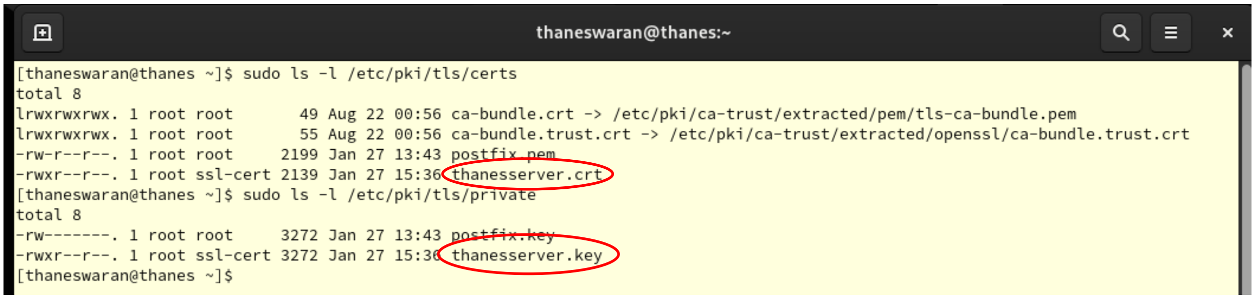
Create the keys and certificate for our SSL.

- **(Sudo openssl req -x509 -newkey rsa:4096 -keyout /etc/pki/tls/private/thanesserver.key -out /etc/pki/tls/certs/thanesserver.crt -days 365 -nodes)** command for opening the blog for creating the certificate.


thaneswaran@thanes:~ — sudo openssl req -x509 -newkey rsa:4096 -keyout /etc/pki/tls/private/waranserver.key -out /et...

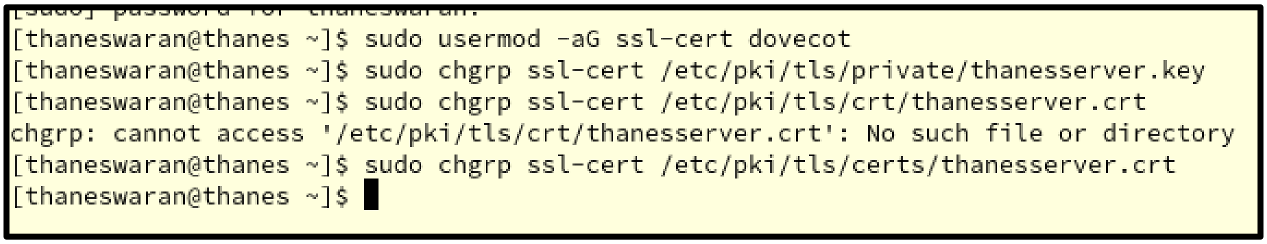
```
[thaneswaran@thanes ~]$ sudo dnf install openssl
[sudo] password for thaneswaran:
Last metadata expiration check: 1:36:50 ago on Tue 28 Jan 2025 12:13:52 AM.
Package openssl-1:3.2.2-6.el9_5.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[thaneswaran@thanes ~]$ sudo openssl req -x509 -newkey rsa:4096 -keyout /etc/pki/tls/private/waranserver.key -out /etc/pki/tls/ce
rts/waranserver.crt -days 365 -nodes
[sudo] password for thaneswaran:
..+....+.....+...+...+....+.....+............+......+..+....++++++++++++++++++++++++++++++++++++++++++++++*......+...+.........+.
+..+.+..........+.+..+.+.....+.+...+..........+....+......+.........+...+.....+....+...+........+...+....+...+++++++++++++++++
++++++++++++++++++++++++++*.+...........+...+.....+................................+......+.......+..........+.......+....
.+....+++++
..................+...+.......+......+.....+.+.........+......+..........+...+....+...+...........+.....+...+.........+...++++
+++++++++++++++++++++++++++++++++++++++++*...+.........+................+..........++++++++++++++++++++++++++++++++++++++++++
++++*..........+....+.....+....+..+.......................+.+.........+...........+..+..........................+.........+..
...+....+.....+....+..+.......................+.+...+.....+.+..........+.+.........+......+..........+....+......+...+...+.
..+...........+..+...+..............+...+............................+...............+...+........+......+...................
....+..+....+.....+....+..+.......+...+..+.......+...+..........................+.+..........+.........+.....+........+..........
................+.+.............+......+.+...+...........+...........+..+.+.....+...+.......+...+...............+..+.........
......+.......+...+...+..+++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

Here you will create the SSL certificate by inputting all their requirements to create the certificate as self-signed.



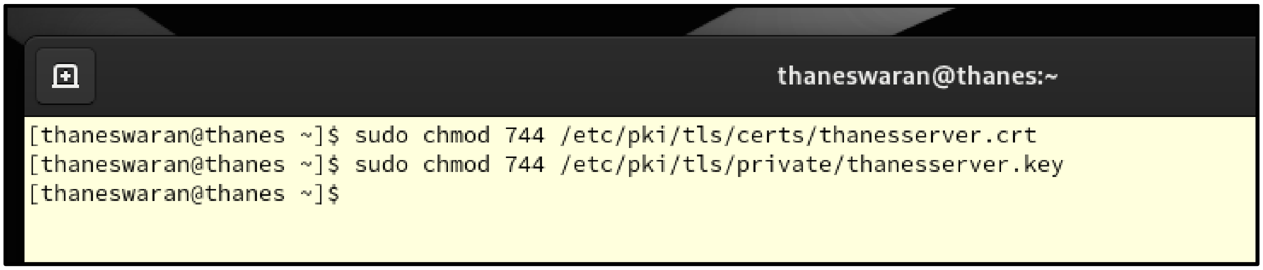
```
[thaneswaran@thanes ~]$ sudo ls -l /etc/pki/tls/certs
total 8
lrwxrwxrwx. 1 root root       49 Aug 22 00:56 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
lrwxrwxrwx. 1 root root       55 Aug 22 00:56 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracted/openssl/ca-bundle.trust.crt
-rw-r--r--. 1 root root     2199 Jan 27 13:43 postfix.pem
-rwxr--r--. 1 root ssl-cert 2139 Jan 27 15:36 thanesserver.crt
[thaneswaran@thanes ~]$ sudo ls -l /etc/pki/tls/private
total 8
-rw-------. 1 root root     3272 Jan 27 13:43 postfix.key
-rwxr--r--. 1 root ssl-cert 3272 Jan 27 15:36 thanesserver.key
[thaneswaran@thanes ~]$
```

Assigning permissions to key and certificate



```
[sudo] password for thaneswaran:
[thaneswaran@thanes ~]$ sudo usermod -aG ssl-cert dovecot
[thaneswaran@thanes ~]$ sudo chgrp ssl-cert /etc/pki/tls/private/thanesserver.key
[thaneswaran@thanes ~]$ sudo chgrp ssl-cert /etc/pki/tls/crt/thanesserver.crt
chgrp: cannot access '/etc/pki/tls/crt/thanesserver.crt': No such file or directory
[thaneswaran@thanes ~]$ sudo chgrp ssl-cert /etc/pki/tls/certs/thanesserver.crt
[thaneswaran@thanes ~]$ 
```

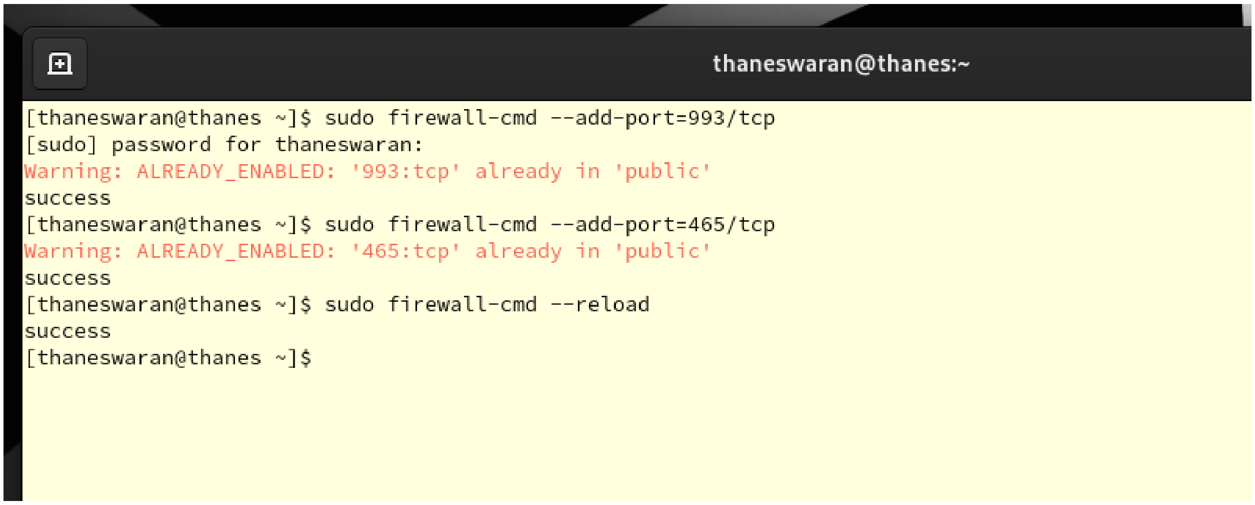
- Assigning the users in one group for postfix and dovecot and adding the key and certificate into the group



```
[thaneswaran@thanes ~]$ sudo chmod 744 /etc/pki/tls/certs/thanesserver.crt
[thaneswaran@thanes ~]$ sudo chmod 744 /etc/pki/tls/private/thanesserver.key
[thaneswaran@thanes ~]$
```

- Assign the permission for the files and 744 contain their permission respectively.
- 7 = Permission for the owner (First digit)
- 4 = Permission for the group (Second digit)
- 4 = Permission for others (Third digit)

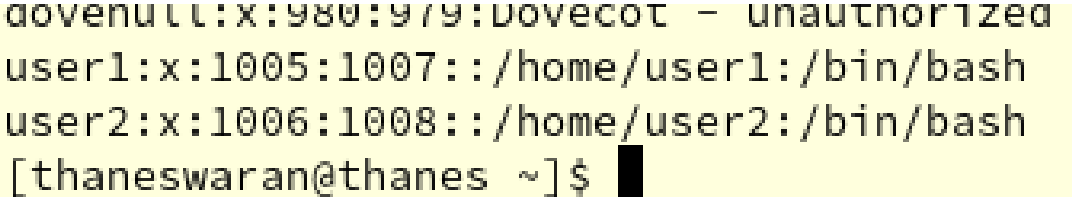
Adding ports



```
[thaneswaran@thanes ~]$ sudo firewall-cmd --add-port=993/tcp
[sudo] password for thaneswaran:
Warning: ALREADY_ENABLED: '993:tcp' already in 'public'
success
[thaneswaran@thanes ~]$ sudo firewall-cmd --add-port=465/tcp
Warning: ALREADY_ENABLED: '465:tcp' already in 'public'
success
[thaneswaran@thanes ~]$ sudo firewall-cmd --reload
success
[thaneswaran@thanes ~]$
```

- I already enable all the ports that’s why it shows the WARNING error.

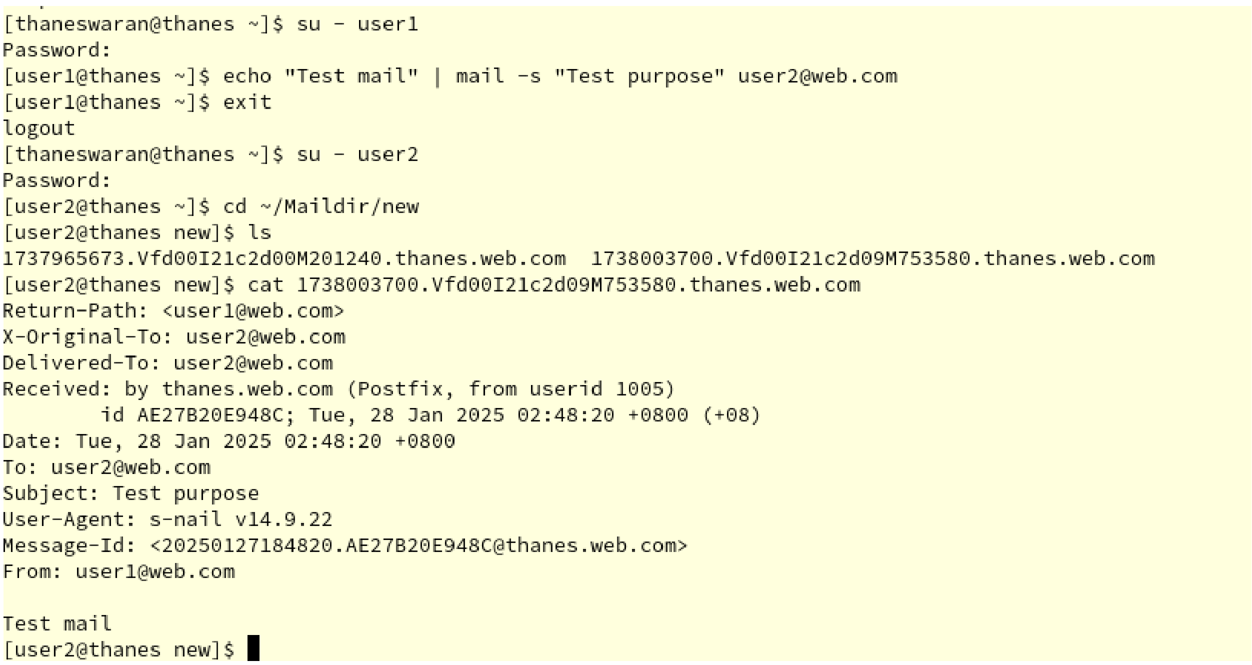
Adding users



```
dovenull:x:980:979:Dovecot - unauthorized
user1:x:1005:1007::/home/user1:/bin/bash
user2:x:1006:1008::/home/user2:/bin/bash
[thaneswaran@thanes ~]$ 
```

- I already created my user1 and user2 by using (**Sudo useradd user1 -m -s /bin/bash**) command and password too.

Testing email locally

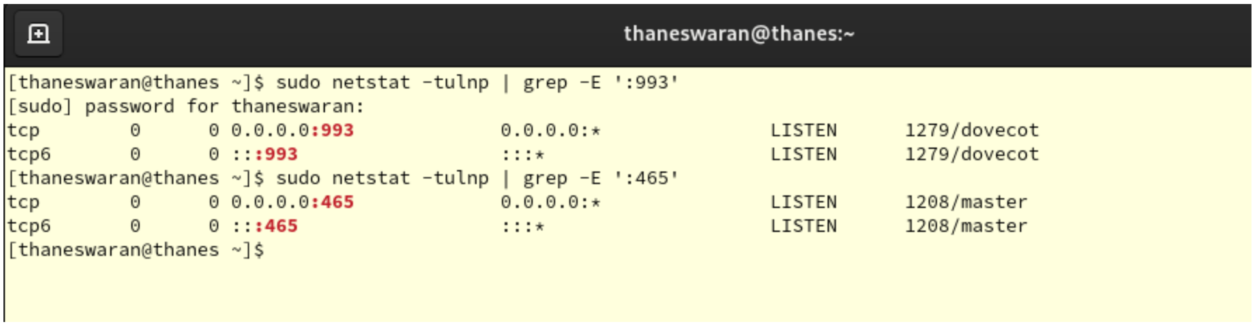


```
[thaneswaran@thanes ~]$ su - user1
Password:
[user1@thanes ~]$ echo "Test mail" | mail -s "Test purpose" user2@web.com
[user1@thanes ~]$ exit
logout
[thaneswaran@thanes ~]$ su - user2
Password:
[user2@thanes ~]$ cd ~/Maildir/new
[user2@thanes new]$ ls
1737965673.Vfd00I21c2d00M201240.thanes.web.com  1738003700.Vfd00I21c2d09M753580.thanes.web.com
[user2@thanes new]$ cat 1738003700.Vfd00I21c2d09M753580.thanes.web.com
Return-Path: <user1@web.com>
X-Original-To: user2@web.com
Delivered-To: user2@web.com
Received: by thanes.web.com (Postfix, from userid 1005)
        id AE27B20E948C; Tue, 28 Jan 2025 02:48:20 +0800 (+08)
Date: Tue, 28 Jan 2025 02:48:20 +0800
To: user2@web.com
Subject: Test purpose
User-Agent: s-nail v14.9.22
Message-Id: <20250127184820.AE27B20E948C@thanes.web.com>
From: user1@web.com

Test mail
[user2@thanes new]$ 
```

- As we see here, the user 2 will communicate and receive the mail from user 1.

Verify the ports and configurations

- (**Sudo netstat -tulnp | grep -E :993’)**
- (**Sudo netstat -tulnp | grep -E :465’)**

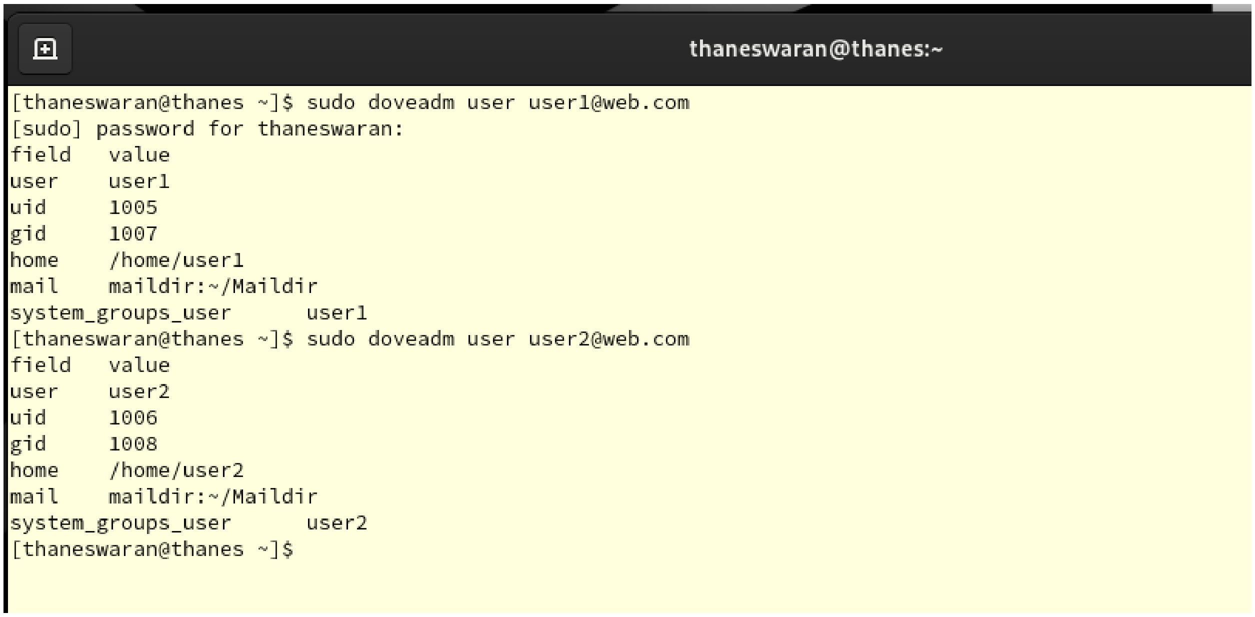


```
[thaneswaran@thanes ~]$ sudo netstat -tulnp | grep -E ':993'
[sudo] password for thaneswaran:
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      1279/dovecot
tcp6       0      0 :::993                  :::*                    LISTEN      1279/dovecot
[thaneswaran@thanes ~]$ sudo netstat -tulnp | grep -E ':465'
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      1208/master
tcp6       0      0 :::465                  :::*                    LISTEN      1208/master
[thaneswaran@thanes ~]$
```

This output should be the same with each other, by using this command we can ensure that port 993 connects with port 465. After it connected it will show the self-signed certificate created successfully.

Dovecot read user

(Sudo doveadm user user1@web.com)



```
[thaneswaran@thanes ~]$ sudo doveadm user user1@web.com
[sudo] password for thaneswaran:
field   value
user    user1
uid     1005
gid     1007
home    /home/user1
mail    maildir:~/Maildir
system_groups_user      user1
[thaneswaran@thanes ~]$ sudo doveadm user user2@web.com
field   value
user    user2
uid     1006
gid     1008
home    /home/user2
mail    maildir:~/Maildir
system_groups_user      user2
[thaneswaran@thanes ~]$
```

Update and Upgrade Ubuntu

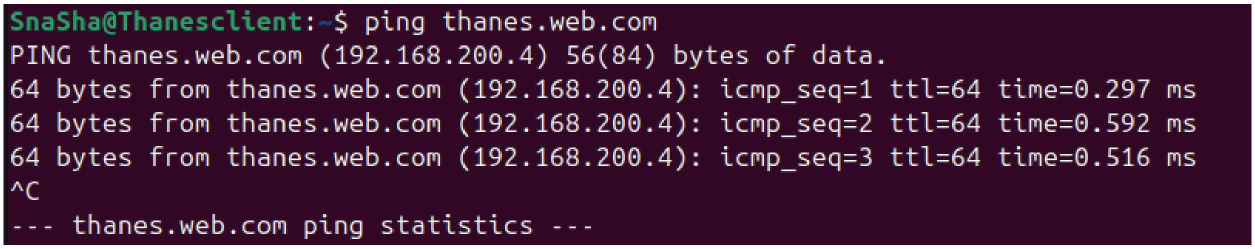
(**Sudo apt-get update & upgrade)**

- To ensure that our Ubuntu (client) is UpToDate, then later we can install any new tool or application without any interruption with it.

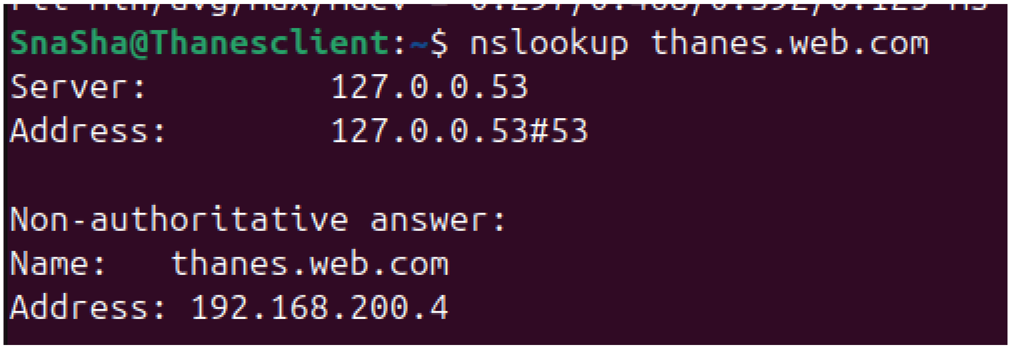
(ping thanes.web.com)

(nslookup thanes.web.com)

- Make sure our client should ping the Rocky server's Ip address to confirm that our client listens to the server every time. Moreover, we make sure that we (NSLOOKUP) for confirmation of the correct Ip address



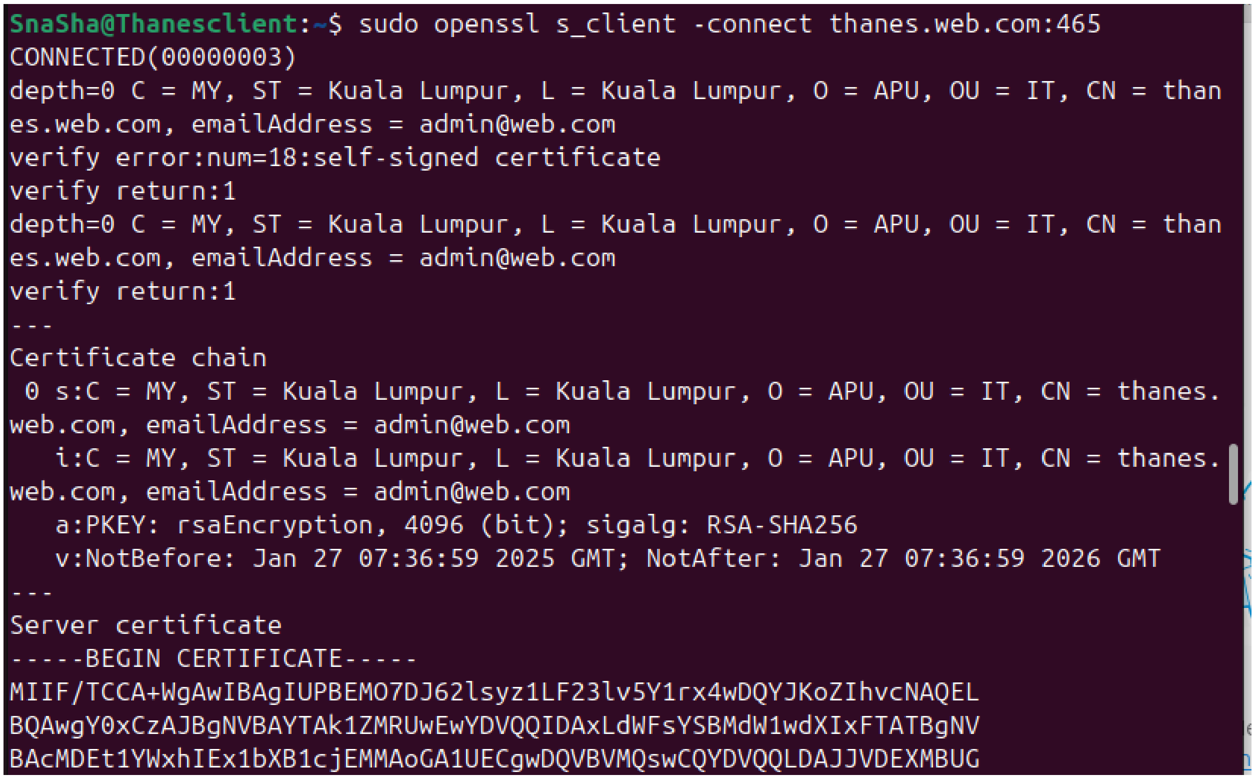
```
SnaSha@Thanesclient:~$ ping thanes.web.com
PING thanes.web.com (192.168.200.4) 56(84) bytes of data.
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=1 ttl=64 time=0.297 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=2 ttl=64 time=0.592 ms
64 bytes from thanes.web.com (192.168.200.4): icmp_seq=3 ttl=64 time=0.516 ms
^C
--- thanes.web.com ping statistics ---
```



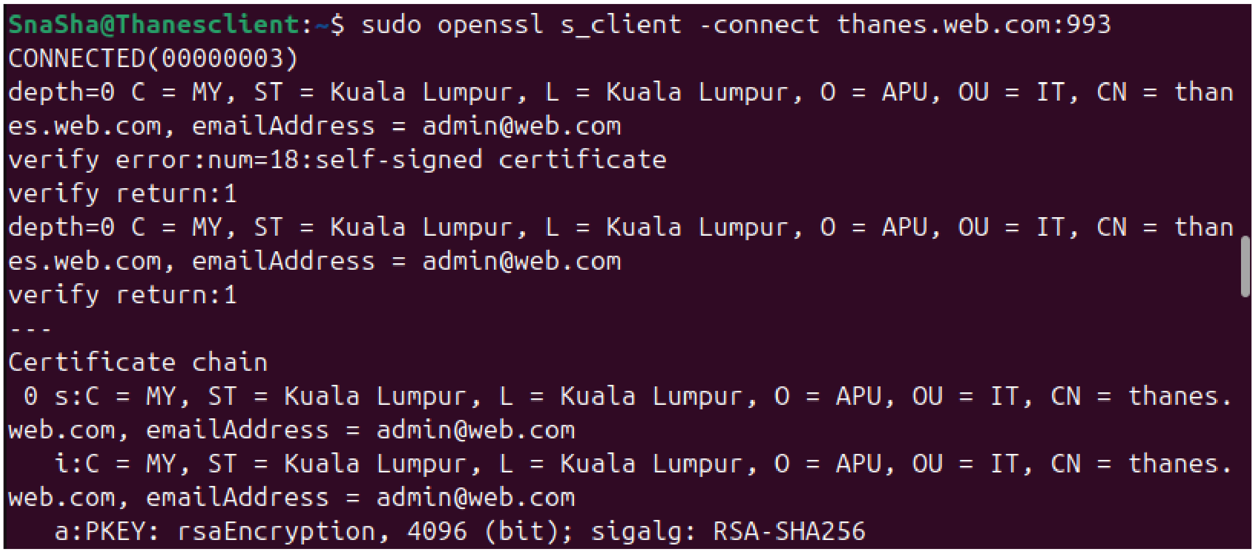
```
SnaSha@Thanesclient:~$ nslookup thanes.web.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   thanes.web.com
Address: 192.168.200.4
```

Connecting the port 465 and 993 on Ubuntu

(Sudo openssl s_client -connect thanesserver.web.com:465) and (Sudo openssl s_client -connect thanesserver.web.com:993) by using these commands.



```
SnaSha@Thanesclient:~$ sudo openssl s_client -connect thanes.web.com:465
CONNECTED(00000003)
depth=0 C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = than
es.web.com, emailAddress = admin@web.com
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = than
es.web.com, emailAddress = admin@web.com
verify return:1
---
Certificate chain
 0 s:C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = thanes.
web.com, emailAddress = admin@web.com
   i:C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = thanes.
web.com, emailAddress = admin@web.com
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jan 27 07:36:59 2025 GMT; NotAfter: Jan 27 07:36:59 2026 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIF/TCCA+WgAwIBAgIUPBEMO7DJ62lsyz1LF23lv5Y1rx4wDQYJKoZIhvcNAQEL
BQAwgY0xCzAJBgNVBAYTAk1ZMRUwEwYDVQQIDAxLdWFsYSBMdW1wdXIxFTATBgNV
BAcMDEt1YWxhIEx1bXB1cjEMMAoGA1UECgwDQVBVMQswCQYDVQQLDAJJVDEXMBUG
```

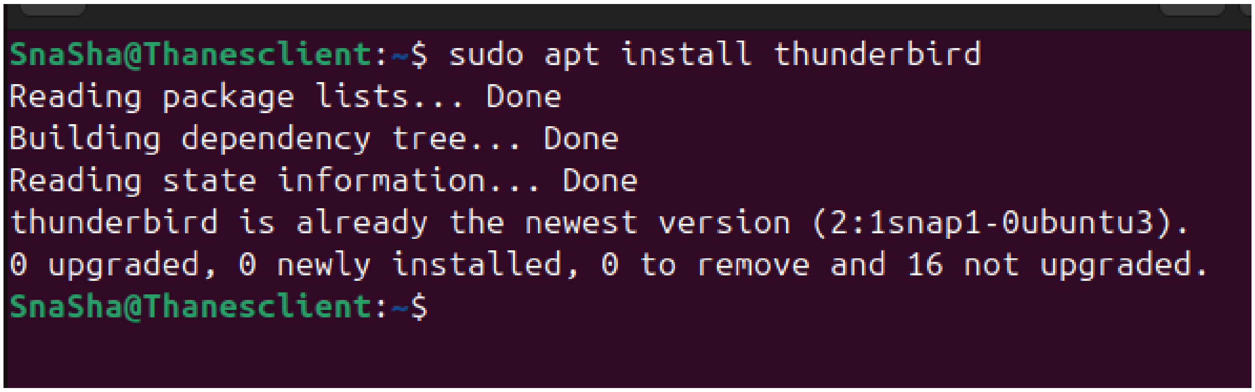


```
SnaSha@Thanesclient:~$ sudo openssl s_client -connect thanes.web.com:993
CONNECTED(00000003)
depth=0 C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = than
es.web.com, emailAddress = admin@web.com
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = than
es.web.com, emailAddress = admin@web.com
verify return:1
---
Certificate chain
 0 s:C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = thanes.
web.com, emailAddress = admin@web.com
   i:C = MY, ST = Kuala Lumpur, L = Kuala Lumpur, O = APU, OU = IT, CN = thanes.
web.com, emailAddress = admin@web.com
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
```

Install Thunderbird in Ubuntu client

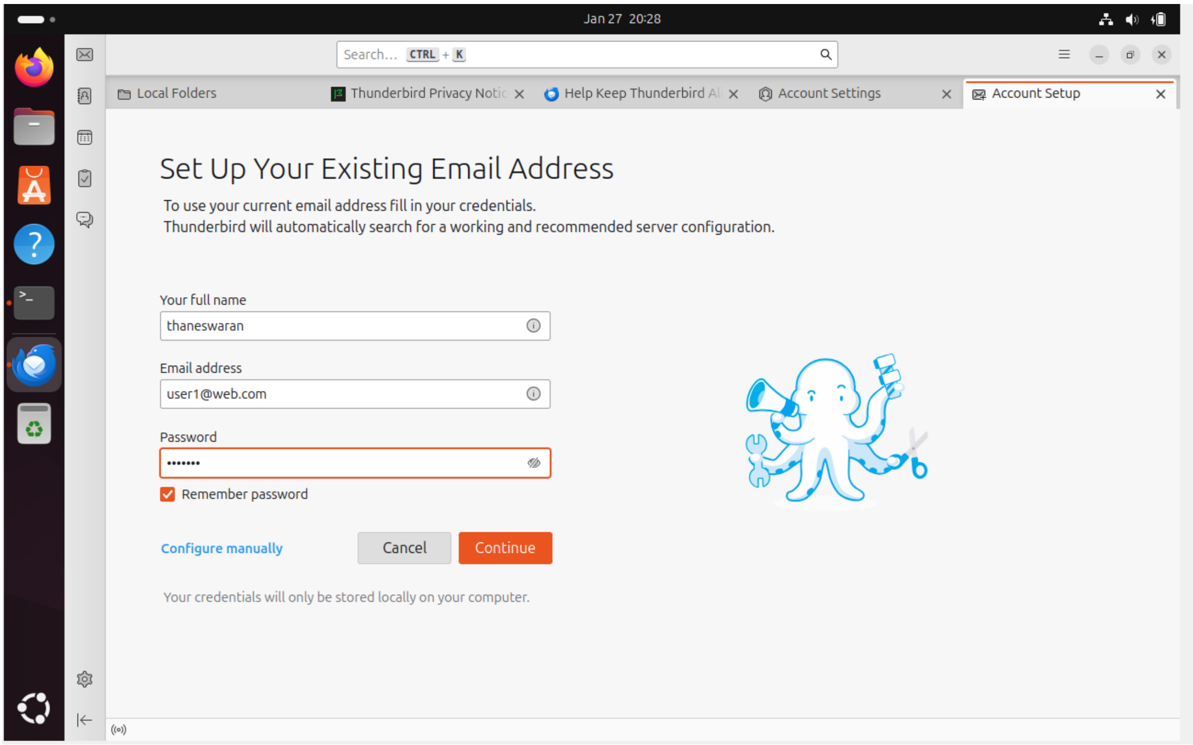
(Sudo apt install thunderbird) use this command to install thunderbird

(thunderbird &) this command for opening the thunderbird.



```
SnaSha@Thanesclient:~$ sudo apt install thunderbird
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
thunderbird is already the newest version (2:1snap1-0ubuntu3).
0 upgraded, 0 newly installed, 0 to remove and 16 not upgraded.
SnaSha@Thanesclient:~$
```

- Just click manual configuration to config the ports all manually.



Set Up Your Existing Email Address

To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

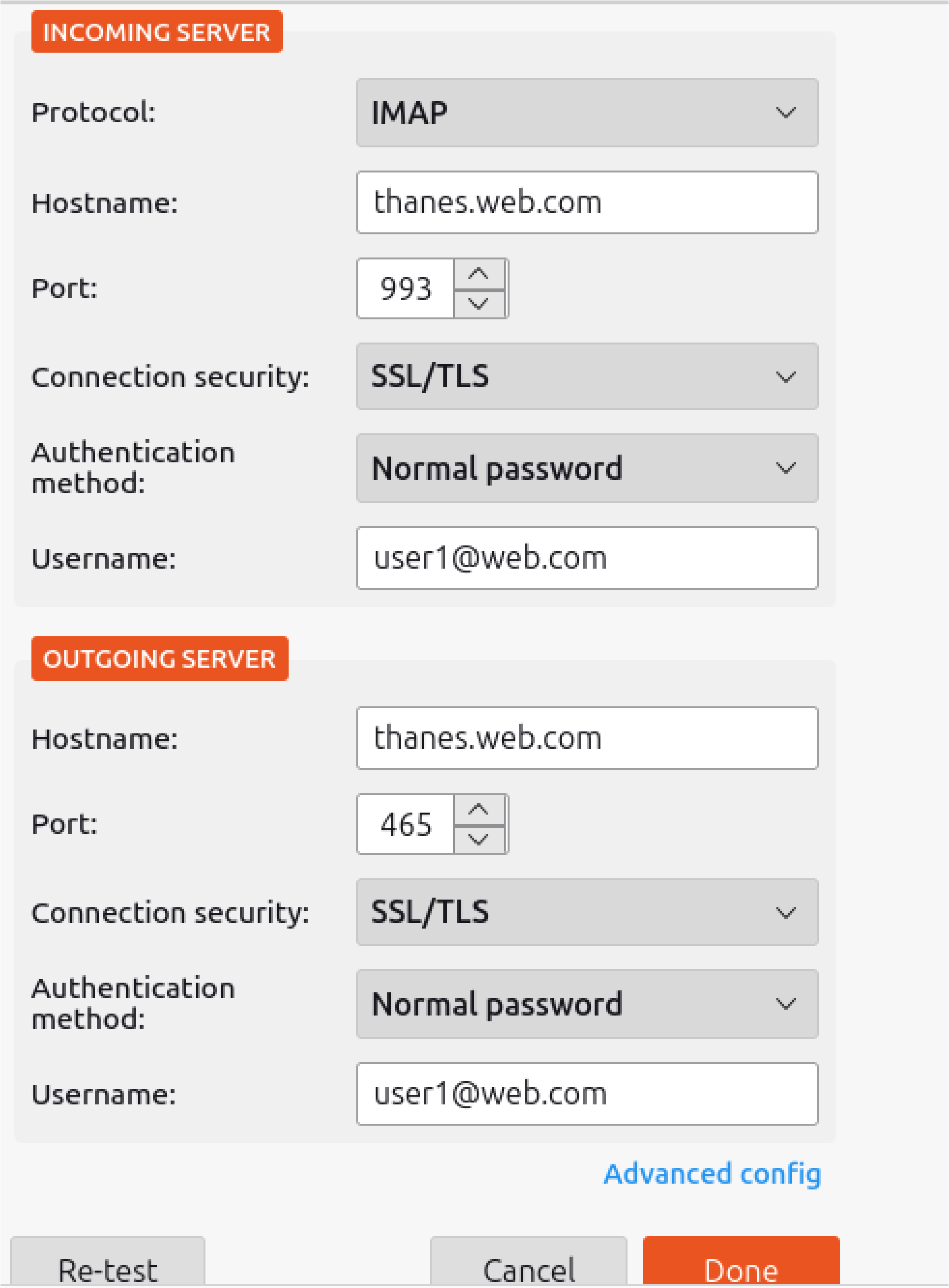
Your full name: thaneswaran

Email address: user1@web.com

Password: •••••••

☑ Remember password

Your credentials will only be stored locally on your computer.



INCOMING SERVER

Protocol: IMAP

Hostname: thanes.web.com

Port: 993

Connection security: SSL/TLS

Authentication method: Normal password

Username: user1@web.com

OUTGOING SERVER

Hostname: thanes.web.com

Port: 465

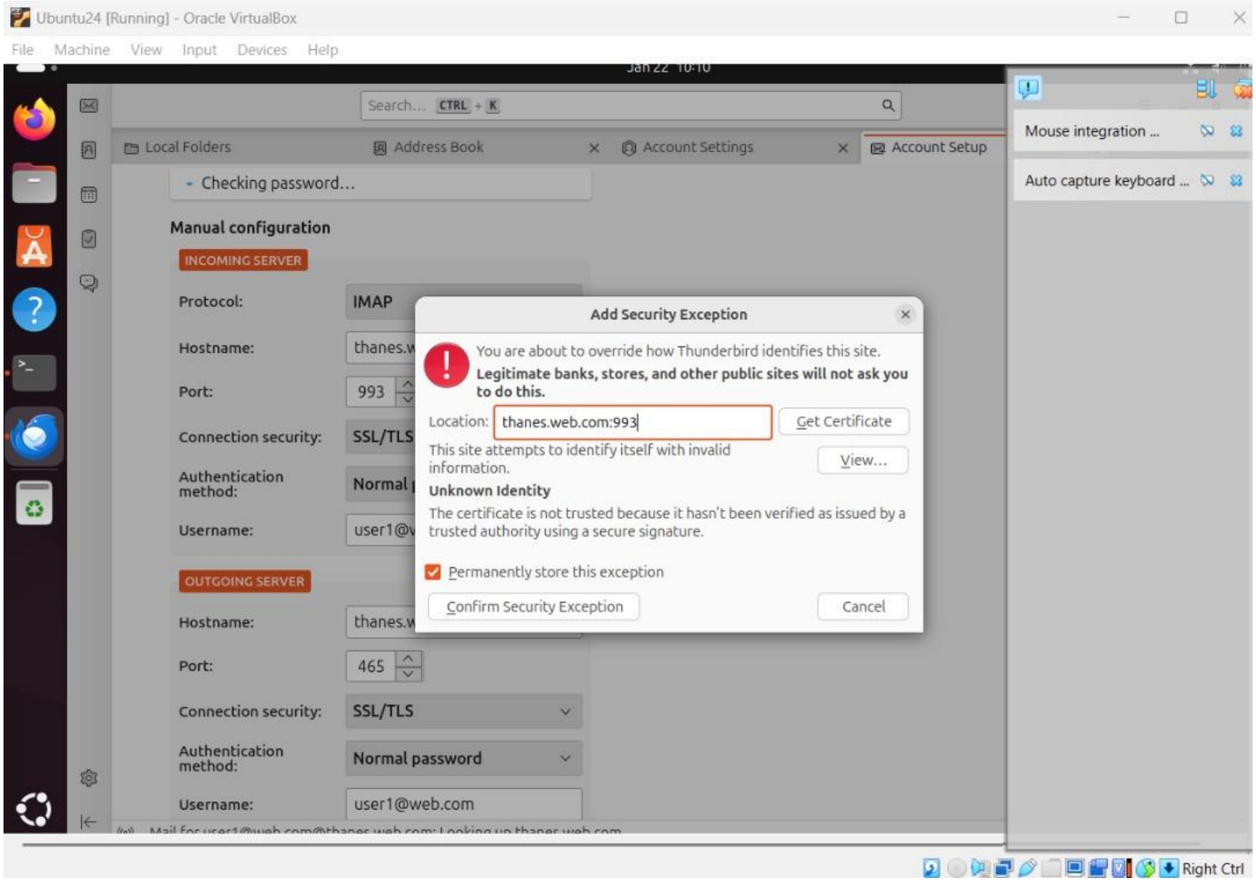
Connection security: SSL/TLS

Authentication method: Normal password

Username: user1@web.com

- Make sure your manual configuration should look like this before you click the DONE button.

- Then you will get notified of the SSL certificate confirmation because we use a self-signed certificate for our email server.



- Checking password...

Manual configuration

INCOMING SERVER

Protocol: IMAP

Hostname: thanes.w

Port: 993

Connection security: SSL/TLS

Authentication method: Normal p

Username: user1@v

OUTGOING SERVER

Hostname: thanes.w

Port: 465

Connection security: SSL/TLS

Authentication method: Normal password

Username: user1@web.com

Mail for user1@web.com@thanes.web.com: Looking up thanes.web.com

Add Security Exception

You are about to override how Thunderbird identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Location: thanes.web.com:993 [Get Certificate]

This site attempts to identify itself with invalid information. [View...]

Unknown Identity

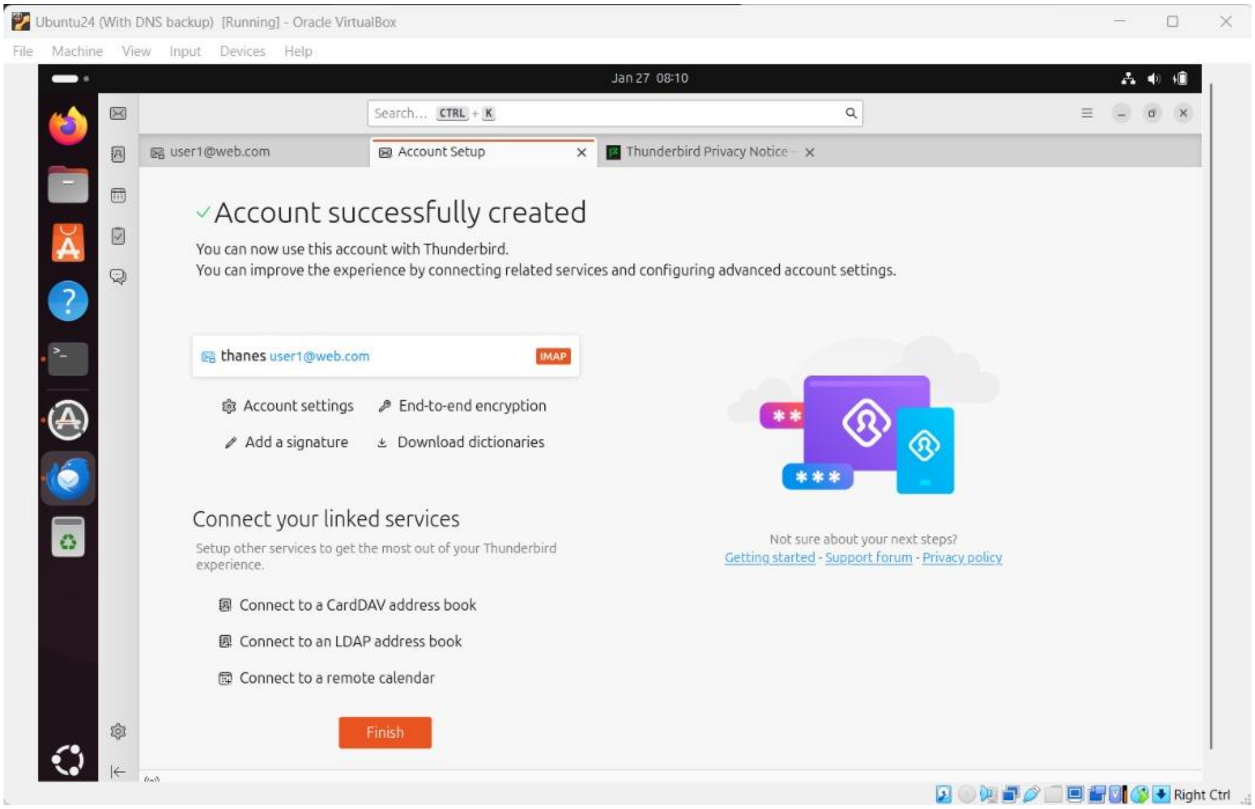
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

[Confirm Security Exception] [Cancel]

- We just have to click on the (Confirm Security Exception) button to sign up for our new user.

- Then we will successfully sign up our user 1 into thunderbird and then we have to do the same manual configuration for user 2 as well. Then only we can test our email whether it can send and receive or not.



Ubuntu24 (With DNS backup) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Jan 27 08:10
Search... CTRL + K
user1@web.com
Account Setup
Thunderbird Privacy Notice
IMAP
Finish
Right Ctrl

Account successfully created

You can now use this account with Thunderbird.
You can improve the experience by connecting related services and configuring advanced account settings.

thanes user1@web.com

Account settings
End-to-end encryption
Add a signature
Download dictionaries

Connect your linked services

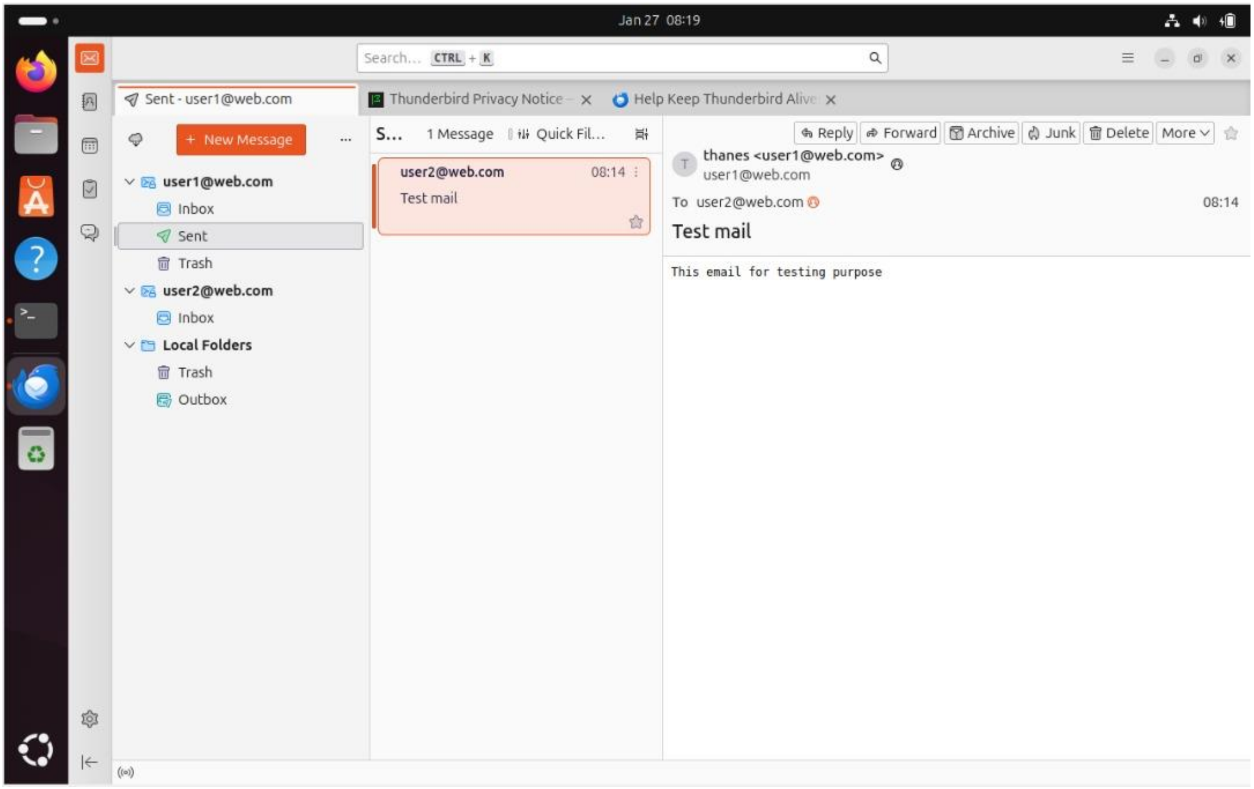
Setup other services to get the most out of your Thunderbird experience.

Connect to a CardDAV address book
Connect to an LDAP address book
Connect to a remote calendar

Not sure about your next steps?
Getting started - Support forum - Privacy policy

Testing Email send and receive

- If you did the configuration all right from the beginning now, we should be able to send and receive the email like I had shown here.
- I try to send Test mail from user 1 to user 2 and it is done successfully without any error.
- You able to see your new mail inside user 2 inbox.



user2@web.com 08:14
Test mail

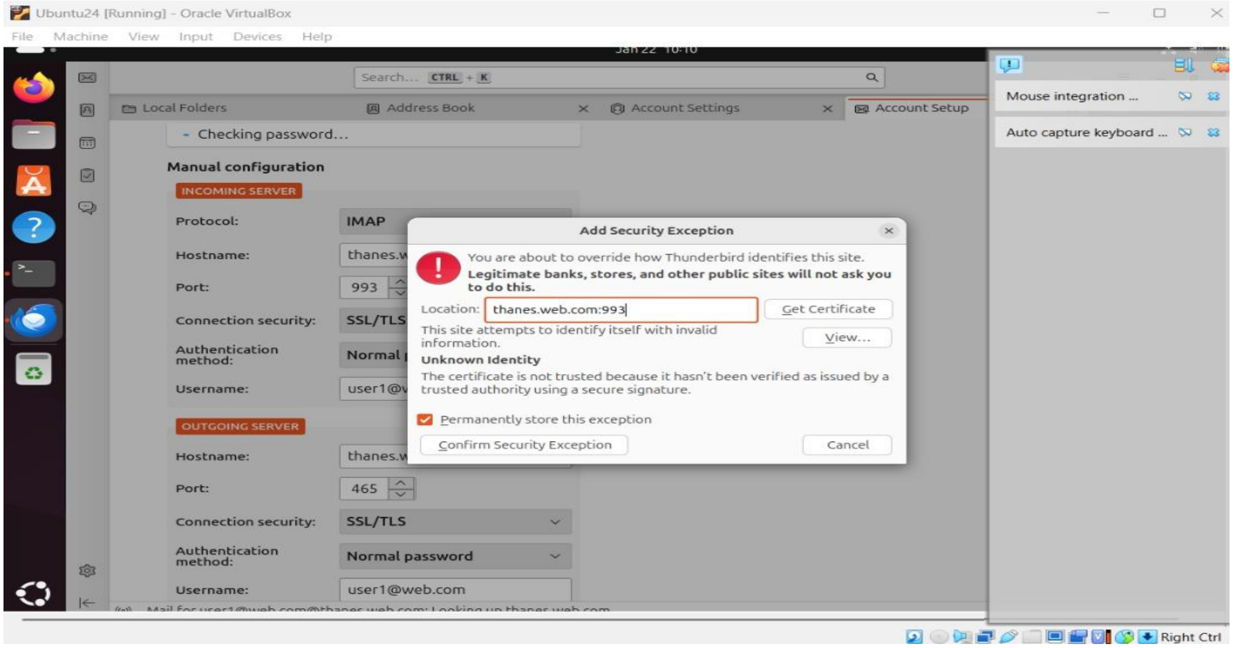
thanes <user1@web.com>
user1@web.com
To user2@web.com 08:14
Test mail

```
This email for testing purpose
```

Conclusion

I completed all the configuration and setup the email server successfully, by using Postfix, Dovecot, Thunderbird, TLS and many more tools that I used to create complete email server in my own. Moreover, we can surely say that this email server is completely safe and secure to use by any organization because we already configure SSL, Plain and Login protocols to encrypt our Username and password.

Troubleshooting



Checking password…

Manual configuration

INCOMING SERVER

Protocol: IMAP

Hostname: thanes.w

Port: 993

Connection security: SSL/TLS

Authentication method: Normal p

Username: user1@v

OUTGOING SERVER

Hostname: thanes.w

Port: 465

Connection security: SSL/TLS

Authentication method: Normal password

Username: user1@web.com

Add Security Exception

You are about to override how Thunderbird identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Location: thanes.web.com:993

This site attempts to identify itself with invalid information.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

I faced only one problem in this progress which is after I sign up to the new user this notification will appear by then after I clicked the Confirm Security exception it keeps showing me the message repeatedly. This is because I accidentally created two certs' files during my SSL certificate configuration. Hereby this warning message was overriding that cert and kept repeating the same notification to me. So, I just went to that specific folder and removed the redundant certificate from it by use

- (Sudo **/etc/pki/tls/certs/)**
- **(ls -l)**

- **rm thanesserver.crt**

So, this command will remove the file from the path. Furthermore, I just went to Ubuntu again to reboot it. Then open thunderbird to sign up with the user that time I can pursue with my next step.