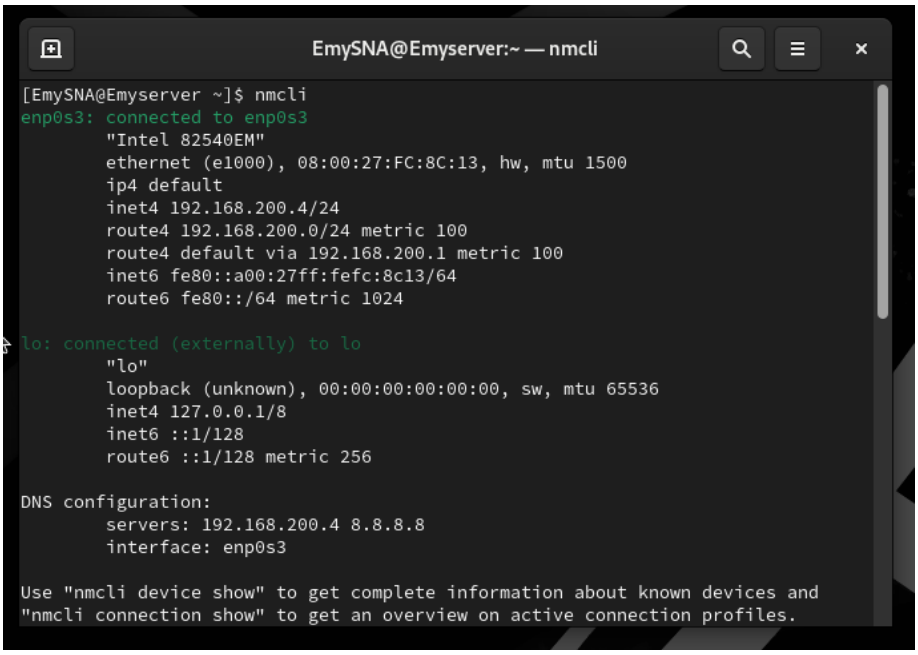
Contents

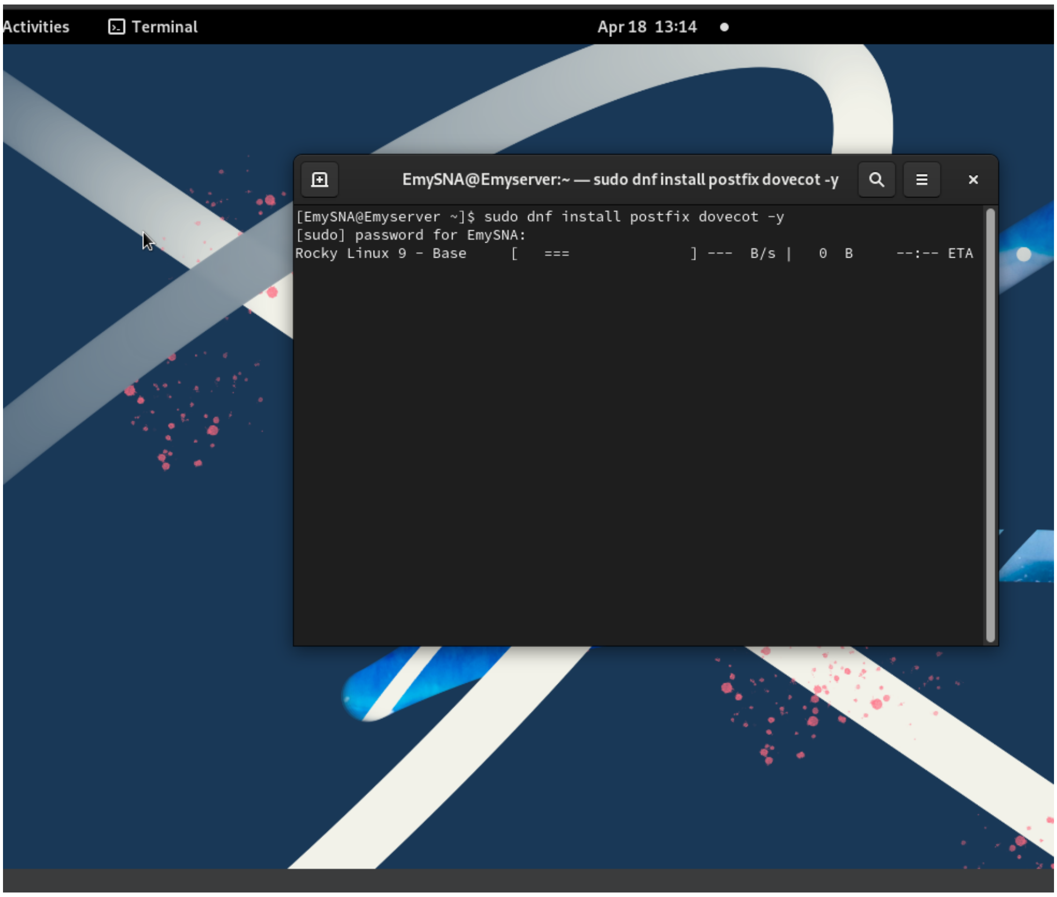
Configure SSL:

First step is to use nmcli to Identify and list out our server configuration:



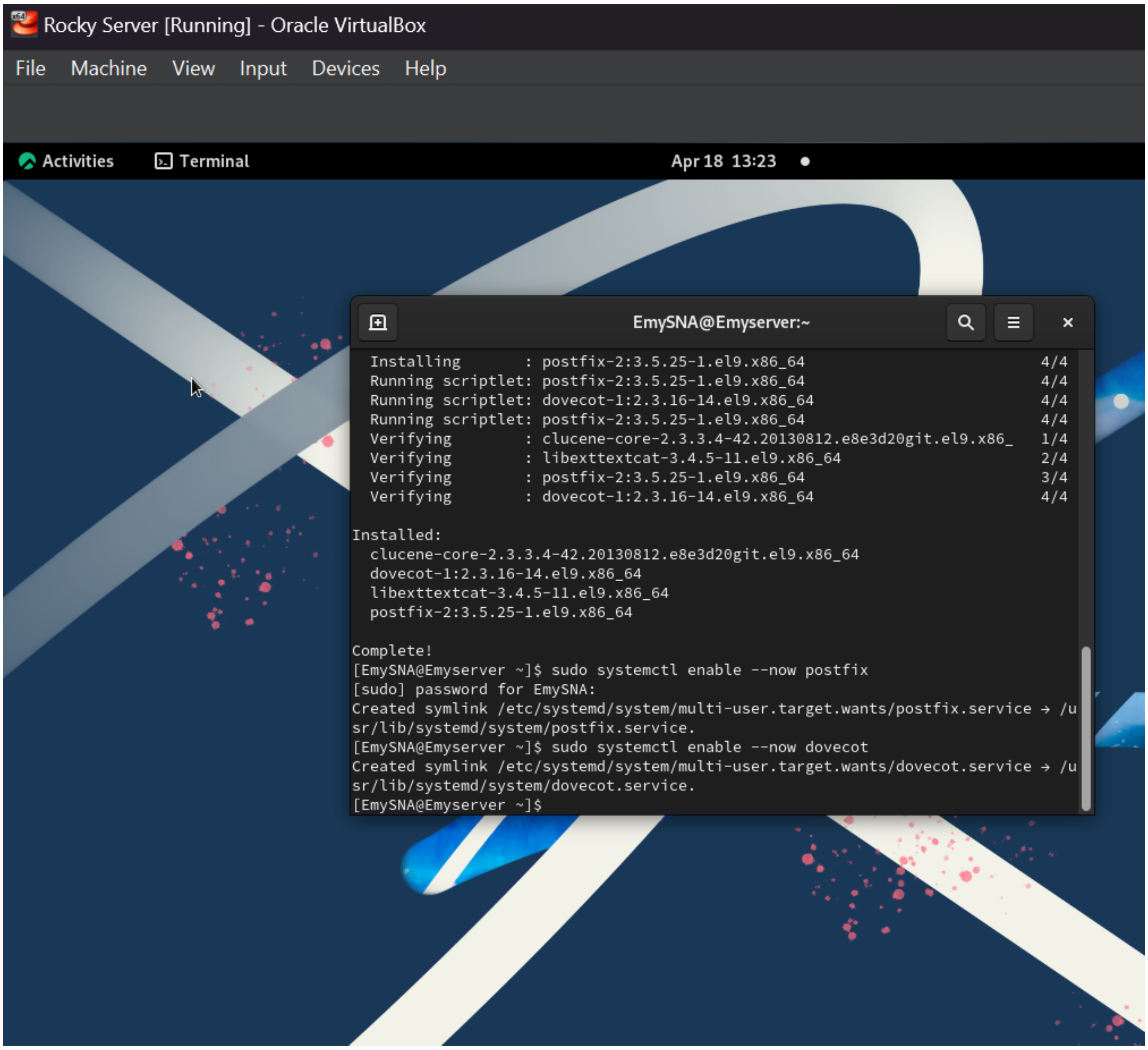
```
[EmySNA@Emyserver ~]$ nmcli
enp0s3: connected to enp0s3
        "Intel 82540EM"
        ethernet (e1000), 08:00:27:FC:8C:13, hw, mtu 1500
        ip4 default
        inet4 192.168.200.4/24
        route4 192.168.200.0/24 metric 100
        route4 default via 192.168.200.1 metric 100
        inet6 fe80::a00:27ff:fefc:8c13/64
        route6 fe80::/64 metric 1024

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
        route6 ::1/128 metric 256

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.
```

First thing, ensure the system is updated:



```
[EmySNA@Emyserver ~]$ sudo dnf install postfix dovecot -y
[sudo] password for EmySNA:
Rocky Linux 9 - Base     [   ===               ] ---  B/s |   0  B     --:-- ETA
```

Using “sudo dnf install postfix dovecot -y” we’re Install postfix to use as a MTA (Mail Transfer Agent) to send and receive emails using SMTP (simple mail transfer protocol) as well as Install dovecot as our mail delivery agent (MDA) software to handle IMAP for sending messages as a message transferring protocol to enable user to access mail on various d and the message transferring protocol POP3 to download message to our machine when connected to the internet and delete it from server since it’s a message transferring protocol in case of unstable internet connection.

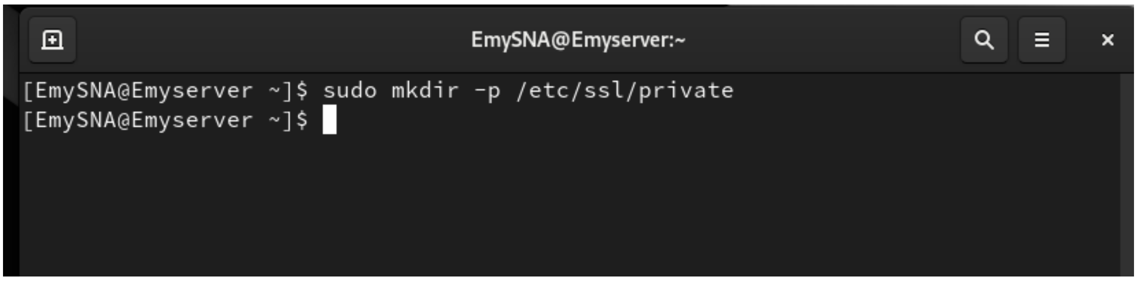


```
  Installing       : postfix-2:3.5.25-1.el9.x86_64                          4/4
  Running scriptlet: postfix-2:3.5.25-1.el9.x86_64                          4/4
  Running scriptlet: dovecot-1:2.3.16-14.el9.x86_64                         4/4
  Running scriptlet: postfix-2:3.5.25-1.el9.x86_64                          4/4
  Verifying        : clucene-core-2.3.3.4-42.20130812.e8e3d20git.el9.x86_   1/4
  Verifying        : libexttextcat-3.4.5-11.el9.x86_64                      2/4
  Verifying        : postfix-2:3.5.25-1.el9.x86_64                          3/4
  Verifying        : dovecot-1:2.3.16-14.el9.x86_64                         4/4

Installed:
  clucene-core-2.3.3.4-42.20130812.e8e3d20git.el9.x86_64
  dovecot-1:2.3.16-14.el9.x86_64
  libexttextcat-3.4.5-11.el9.x86_64
  postfix-2:3.5.25-1.el9.x86_64

Complete!
[EmySNA@Emyserver ~]$ sudo systemctl enable --now postfix
[sudo] password for EmySNA:
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /u
sr/lib/systemd/system/postfix.service.
[EmySNA@Emyserver ~]$ sudo systemctl enable --now dovecot
Created symlink /etc/systemd/system/multi-user.target.wants/dovecot.service → /u
sr/lib/systemd/system/dovecot.service.
[EmySNA@Emyserver ~]$
```

Use “sudo systemctl enable --now postfix

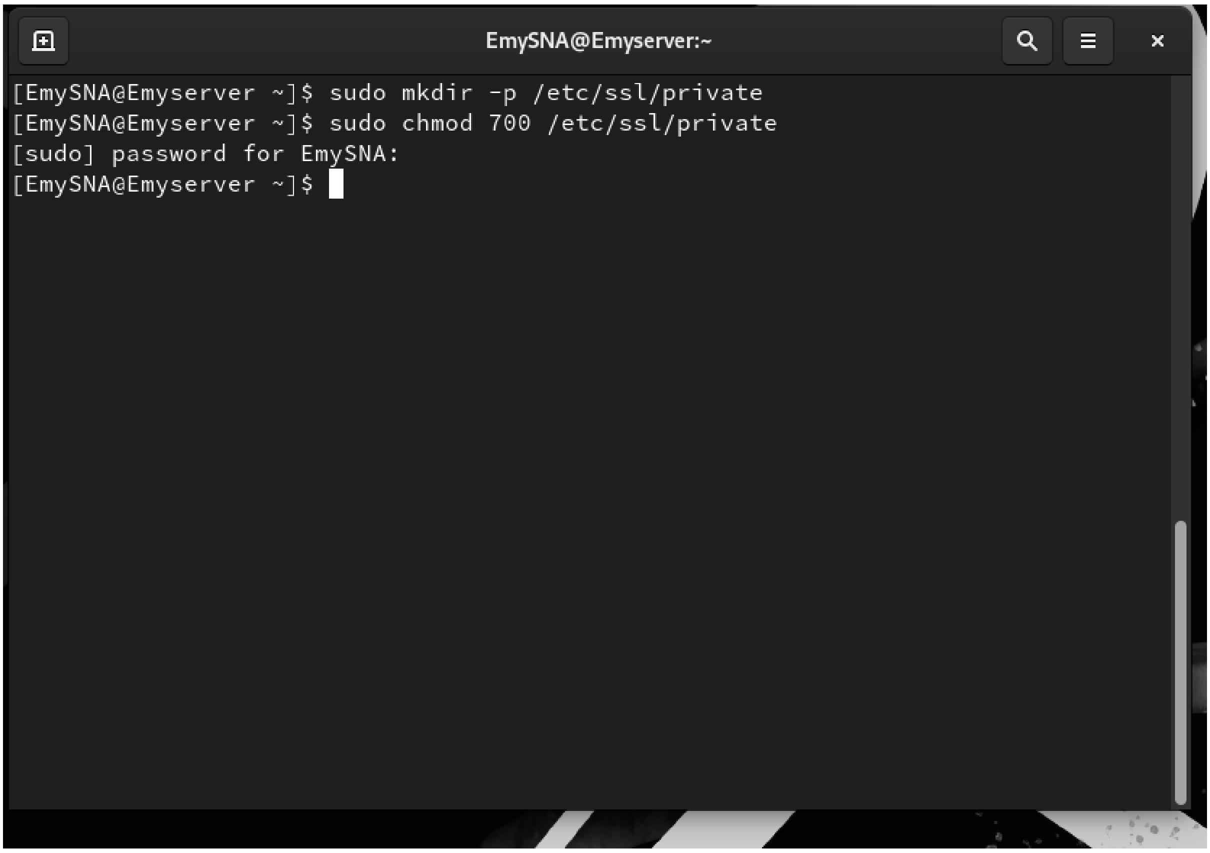
sudo systemctl enable --now dovecot”

to ensure both services start immediately and ensure mail server will be active after reboot next we create a directory to store the private SSL/TLS encryption keys securely in the system:



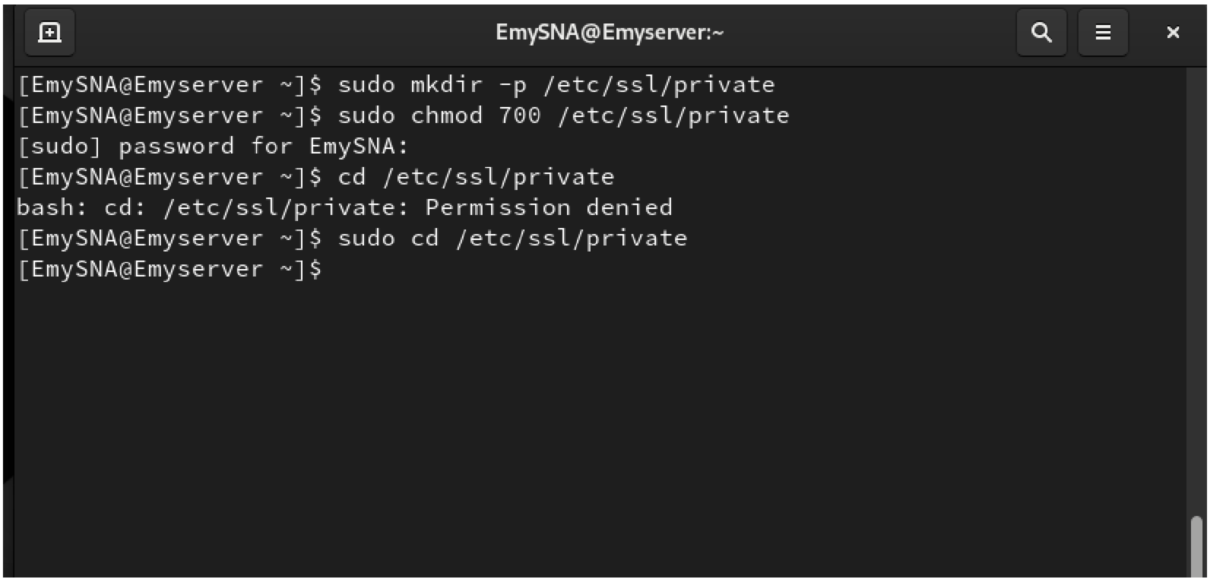
```
[EmySNA@Emyserver ~]$ sudo mkdir -p /etc/ssl/private
[EmySNA@Emyserver ~]$ 
```

We then set permissions int the recently created directory where only the root (owner) can write (4), read(2) and execute(1) hence the 7, whereas group and others can't hence 0s:



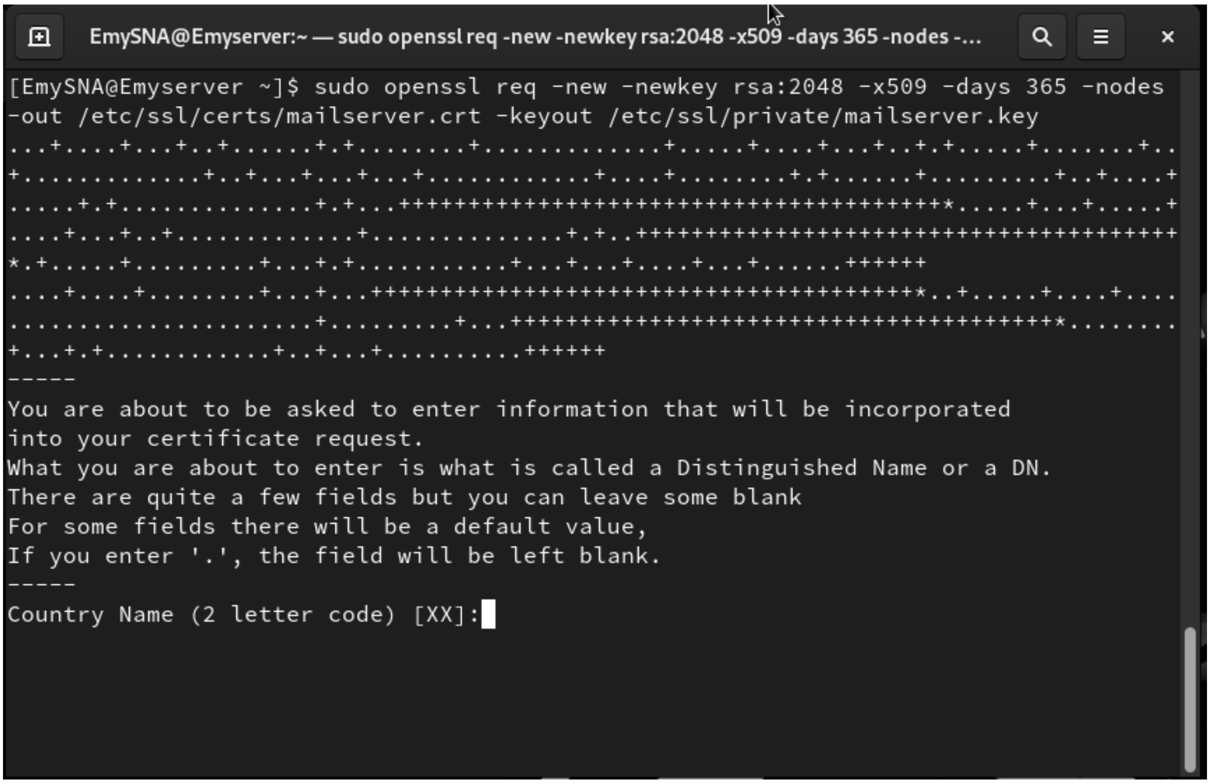
```
[EmySNA@Emyserver ~]$ sudo mkdir -p /etc/ssl/private
[EmySNA@Emyserver ~]$ sudo chmod 700 /etc/ssl/private
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ 
```

We then change directories to the recently created one.



```
[EmySNA@Emyserver ~]$ sudo mkdir -p /etc/ssl/private
[EmySNA@Emyserver ~]$ sudo chmod 700 /etc/ssl/private
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ cd /etc/ssl/private
bash: cd: /etc/ssl/private: Permission denied
[EmySNA@Emyserver ~]$ sudo cd /etc/ssl/private
[EmySNA@Emyserver ~]$
```

Then we generate a self-signed TLS certificate and private key to be used for mail servers like Postfix or Dovecot in testing or private deployments:



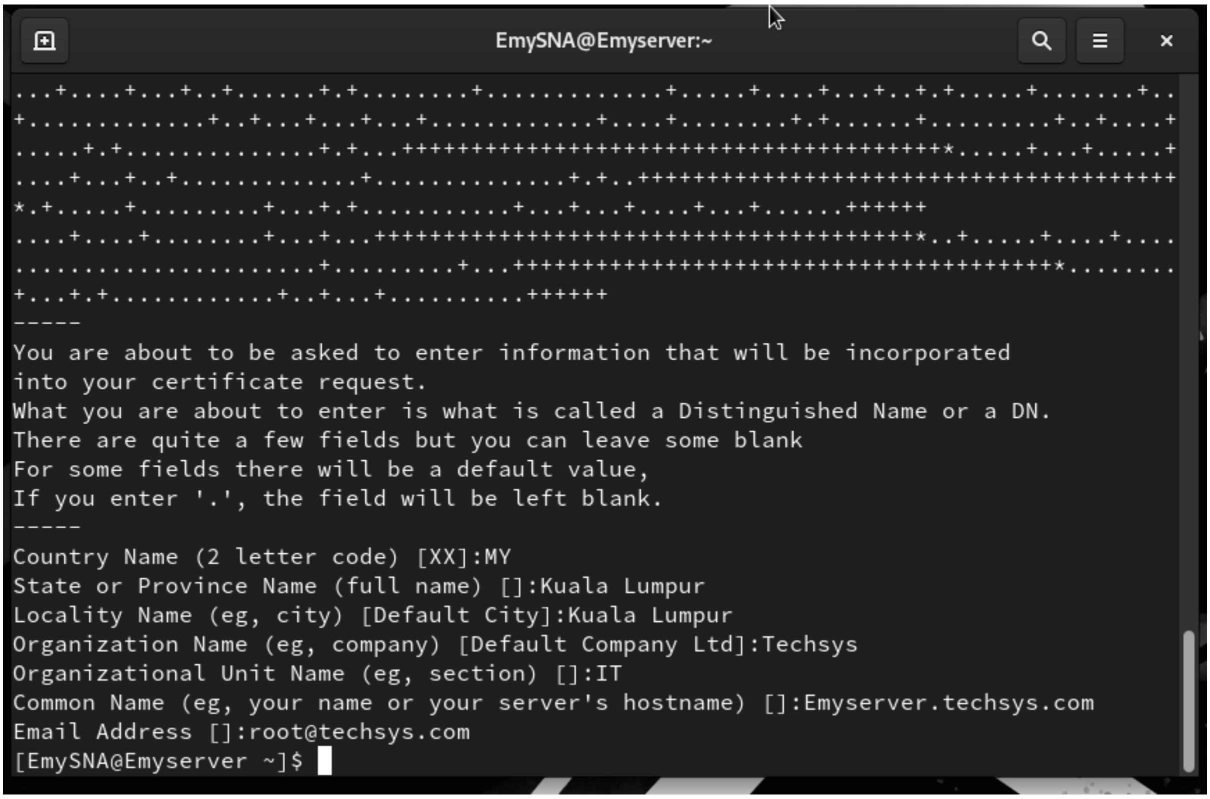
EmySNA@Emyserver:~ — sudo openssl req -new -newkey rsa:2048 -x509 -days 365 -nodes -...

```
[EmySNA@Emyserver ~]$ sudo openssl req -new -newkey rsa:2048 -x509 -days 365 -nodes
-out /etc/ssl/certs/mailserver.crt -keyout /etc/ssl/private/mailserver.key
...+....+...+..+......+.+........+............+.....+....+...+..+.+.....+.......+..
+............+..+...+...+...+...........+....+........+.+......+.........+..+....+
.....+.+.............+.+...+++++++++++++++++++++++++++++++++++++++*.....+...+.....+
....+...+..+............+............+.+..+++++++++++++++++++++++++++++++++++++++
*.+.....+........+...+.+..........+...+...+....+...+......++++++
....+....+.......+...+...+++++++++++++++++++++++++++++++++++++++*..+.....+....+....
....................+........+...+++++++++++++++++++++++++++++++++++++++*.......
+...+.+...........+..+...+.........++++++
-----
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.
-----
Country Name (2 letter code) [XX]:
```

- new : generate a new certificate request
- newkey rsa:2048 : generate a new RSA(Rivest–Shamir–Adleman) 2048-bit key
- x509 : make self-signed certificate instead of CSR (certificate signing request)
- days 365 : sets certificate validity period to 365 days
- nodes : specifies the private key that is not to be encrypted

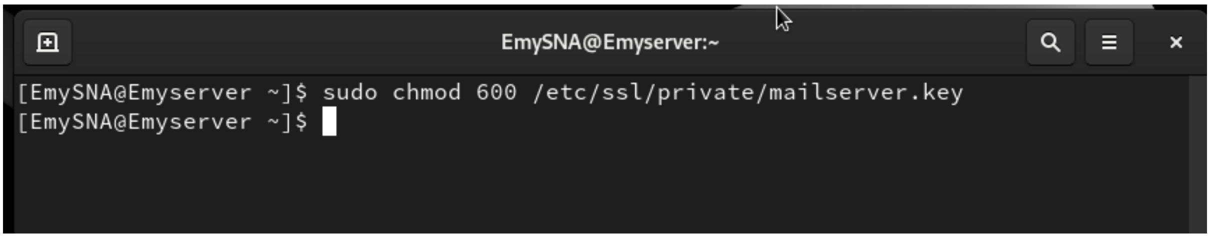
- out : defines the output path for the generated certificate
- keyout :define the output path for the generated private key

then the self-signed certificate information is filled:



```
...+....+...+..+......+.+........+.............+.....+....+...+..+.+.....+.......+..
+.............+..+...+...+...+............+....+........+.+......+.........+..+....+
.....+.+..............+.+...+++++++++++++++++++++++++++++++++++++++*.....+...+.....+
....+...+..+.............+..............+.+..+++++++++++++++++++++++++++++++++++++++
*.+.....+.........+...+.+...........+...+...+....+...+......++++++
....+....+........+...+...+++++++++++++++++++++++++++++++++++++++*..+.....+....+....
......................+.........+...+++++++++++++++++++++++++++++++++++++++*........
+...+.+............+..+...+..........++++++
-----
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.
-----
Country Name (2 letter code) [XX]:MY
State or Province Name (full name) []:Kuala Lumpur
Locality Name (eg, city) [Default City]:Kuala Lumpur
Organization Name (eg, company) [Default Company Ltd]:Techsys
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:Emyserver.techsys.com
Email Address []:root@techsys.com
[EmySNA@Emyserver ~]$ 
```

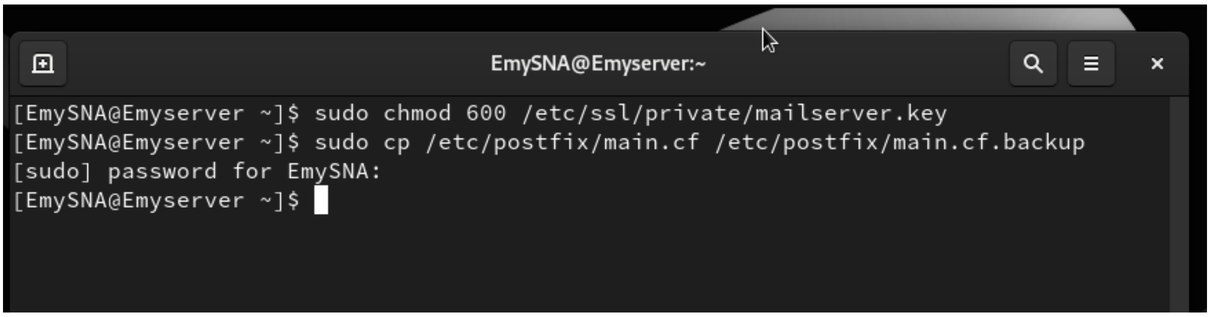
Set permission so only root can read and write the private key:



```
[EmySNA@Emyserver ~]$ sudo chmod 600 /etc/ssl/private/mailserver.key
[EmySNA@Emyserver ~]$ 
```

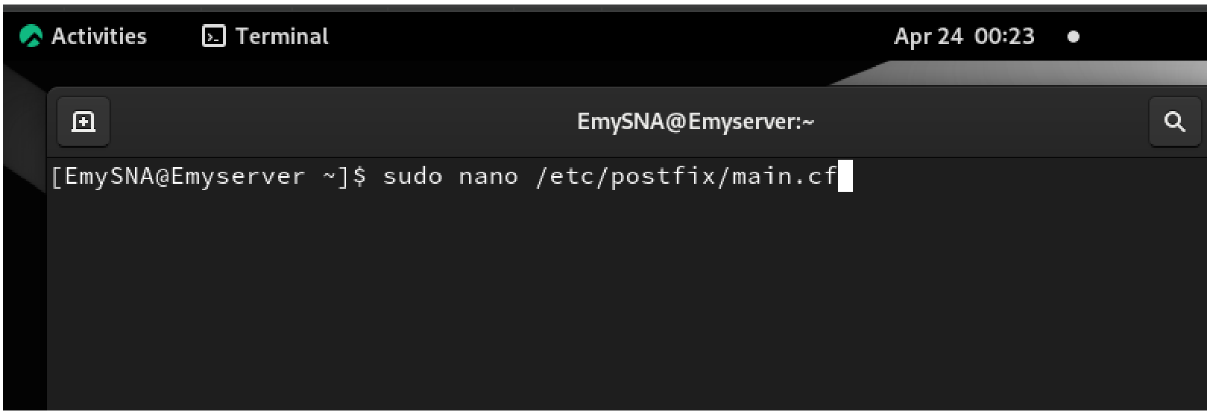
Postfix configuration

We use sudo as the original file Is owned by the root based on previous permissions to make a backup of postfix configuration file and stores it as “main.cf.backup” in the same directory



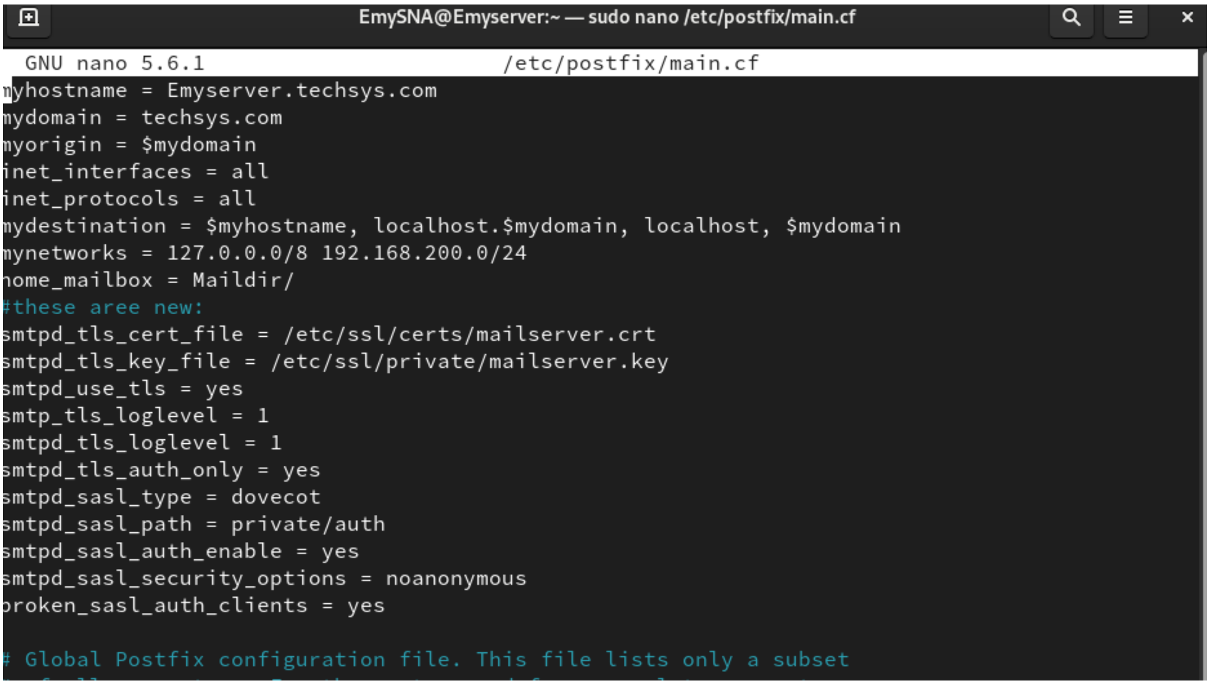
```
[EmySNA@Emyserver ~]$ sudo chmod 600 /etc/ssl/private/mailserver.key
[EmySNA@Emyserver ~]$ sudo cp /etc/postfix/main.cf /etc/postfix/main.cf.backup
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ 
```

we then open a nano text editor with root privileges to edit hostname, TLS, domain…etc.:



```
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/main.cf
```

We then modify the file to the following:



```
 GNU nano 5.6.1                      /etc/postfix/main.cf
myhostname = Emyserver.techsys.com
mydomain = techsys.com
myorigin = $mydomain
inet_interfaces = all
inet_protocols = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mynetworks = 127.0.0.0/8 192.168.200.0/24
home_mailbox = Maildir/
#these aree new:
smtpd_tls_cert_file = /etc/ssl/certs/mailserver.crt
smtpd_tls_key_file = /etc/ssl/private/mailserver.key
smtpd_use_tls = yes
smtp_tls_loglevel = 1
smtpd_tls_loglevel = 1
smtpd_tls_auth_only = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes

# Global Postfix configuration file. This file lists only a subset
```

myhostname =Emyserver.techsys.org (hostname)

mydomain = tech.org (domain name)

myorigin = $mydomain (domain for outgoing emails, will be auto filled with the assigned domain)

inet_interfaces = all,

inet_protocols = all (all network interfaces and both ipv4 and IPv6 will be supports)

mydestination = $myhostname, localhost.$mydomain,localhost, $mydomain(domains this server will accept for mail purposes)

mynetworks = 127.0.0.0/8, 192.168.200.0/24 (IP addresses range allowed to send via server)

home_mailbox = Maildir/ (stores mail in “/Maildir/”) :

smtpd_tls_cert_file = /etc/ssl/certs/mailserver.crt (The location of the SSL certificate used to encrypt connections)

smtpd_tls_key_file = /etc/ssl/private/mailserver.key (private key that matches the certificate above)

smtpd_use_tls = yes (Turns on TLS encryption for incoming mail)

smtp_tls_loglevel = 1 (Log basic info about outgoing TLS connections to smtp)

smtpd_tls_loglevel = 1 (Log basic info about incoming TLS connections to smtpd)

smtpd_tls_auth_only = yes (allow login if the connection is encrypted only)

smtpd_sasl_type = dovecot (Use Dovecot to check login usernames and passwords)

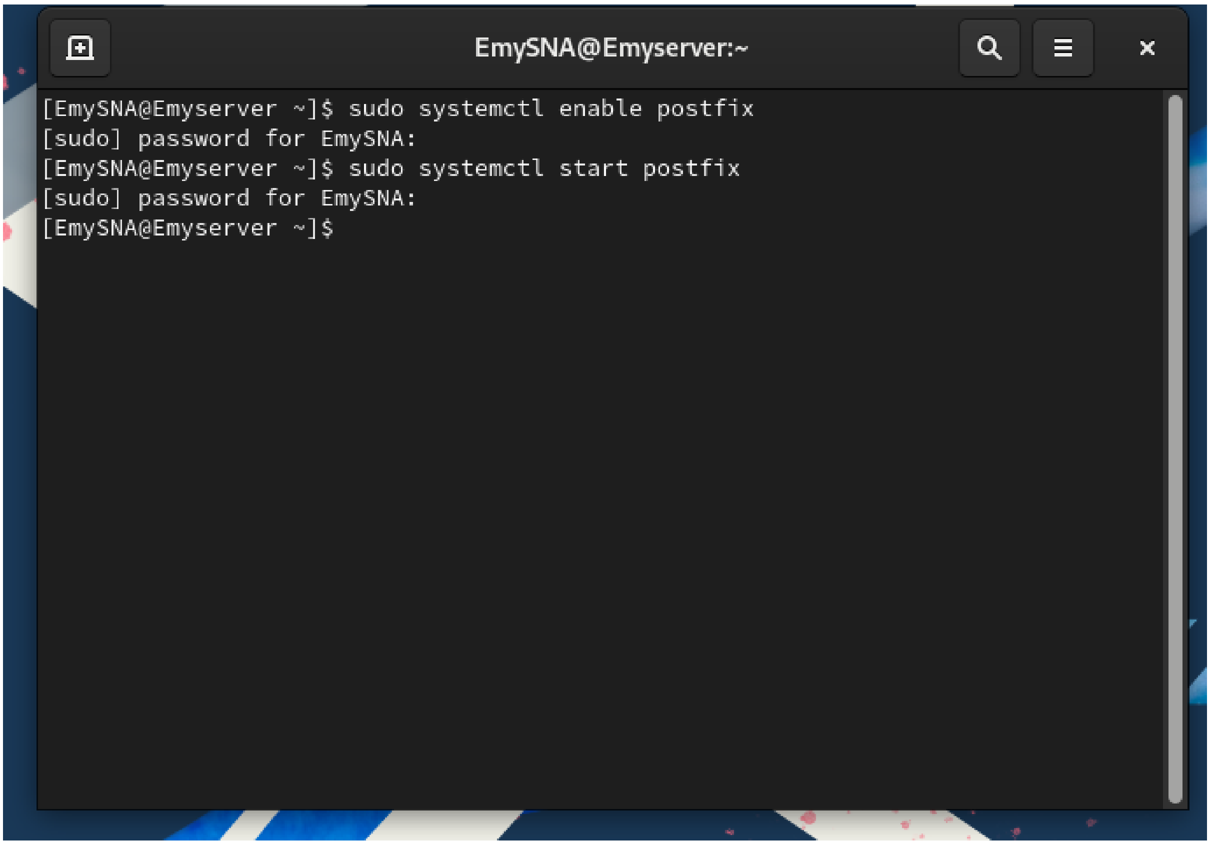
smtpd_sasl_path = private/auth (The internal socket Postfix uses totalks to Dovecot to check logins)

smtpd_sasl_auth_enable = yes (Enable login/authentication for users sending mail)

smtpd_sasl_security_options = noanonymous (reject logging in attempts without a username/password)

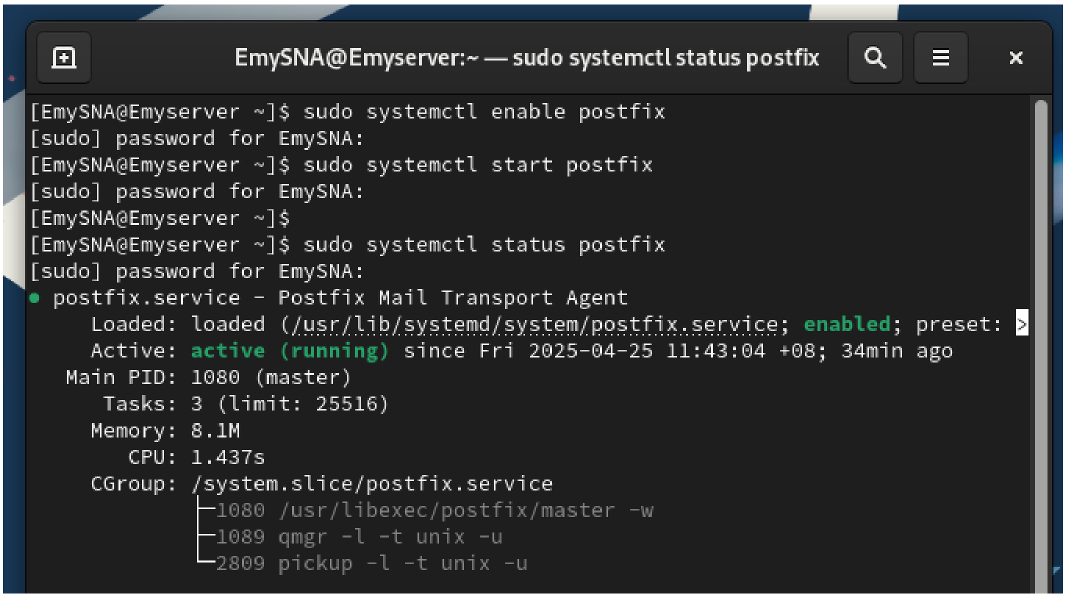
broken_sasl_auth_clients = yes (support old or buggy email apps that don’t follow SASL clients standards)

Enable and start postfix:



```
[EmySNA@Emyserver ~]$ sudo systemctl enable postfix
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo systemctl start postfix
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$
```

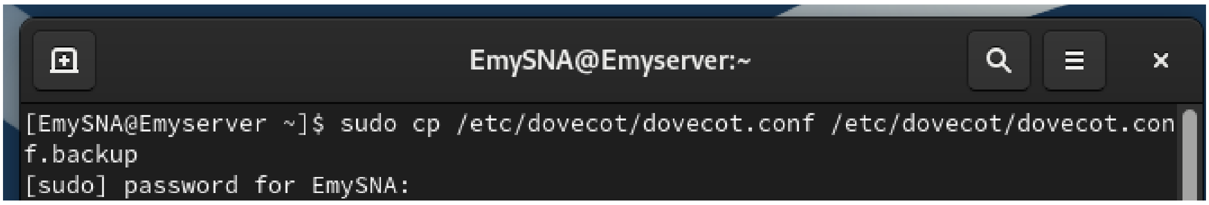
Checking postfix status to ensuer it’s enabled and active:



```
[EmySNA@Emyserver ~]$ sudo systemctl enable postfix
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo systemctl start postfix
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$
[EmySNA@Emyserver ~]$ sudo systemctl status postfix
[sudo] password for EmySNA:
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: >
     Active: active (running) since Fri 2025-04-25 11:43:04 +08; 34min ago
   Main PID: 1080 (master)
      Tasks: 3 (limit: 25516)
     Memory: 8.1M
        CPU: 1.437s
     CGroup: /system.slice/postfix.service
             ├─1080 /usr/libexec/postfix/master -w
             ├─1089 qmgr -l -t unix -u
             └─2809 pickup -l -t unix -u
```

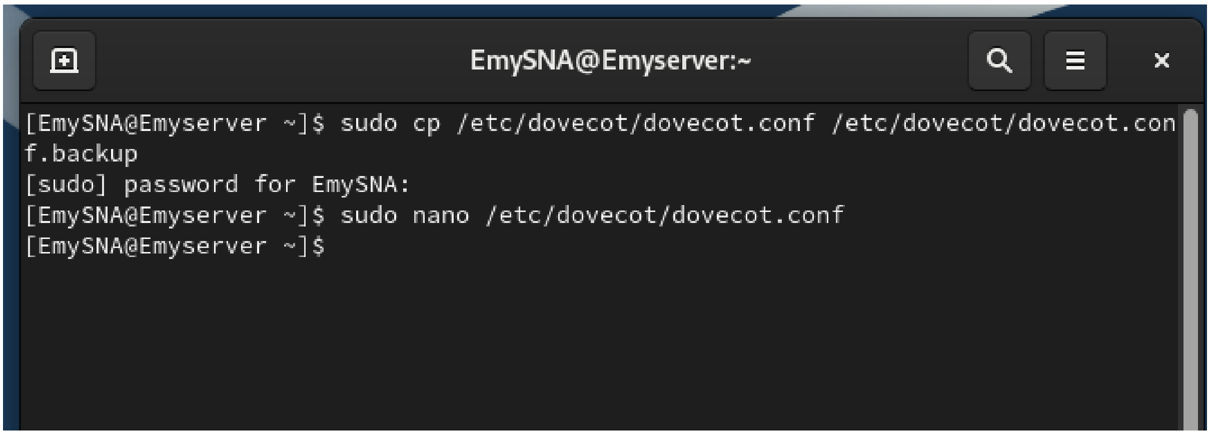
Dovecot configuration

Command to make a backup file of dovecot.conf :



```
[EmySNA@Emyserver ~]$ sudo cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.con
f.backup
[sudo] password for EmySNA:
```

Open a text editor as root to edit dovecot configuration file which manages IMAP/POP3 mail.server:

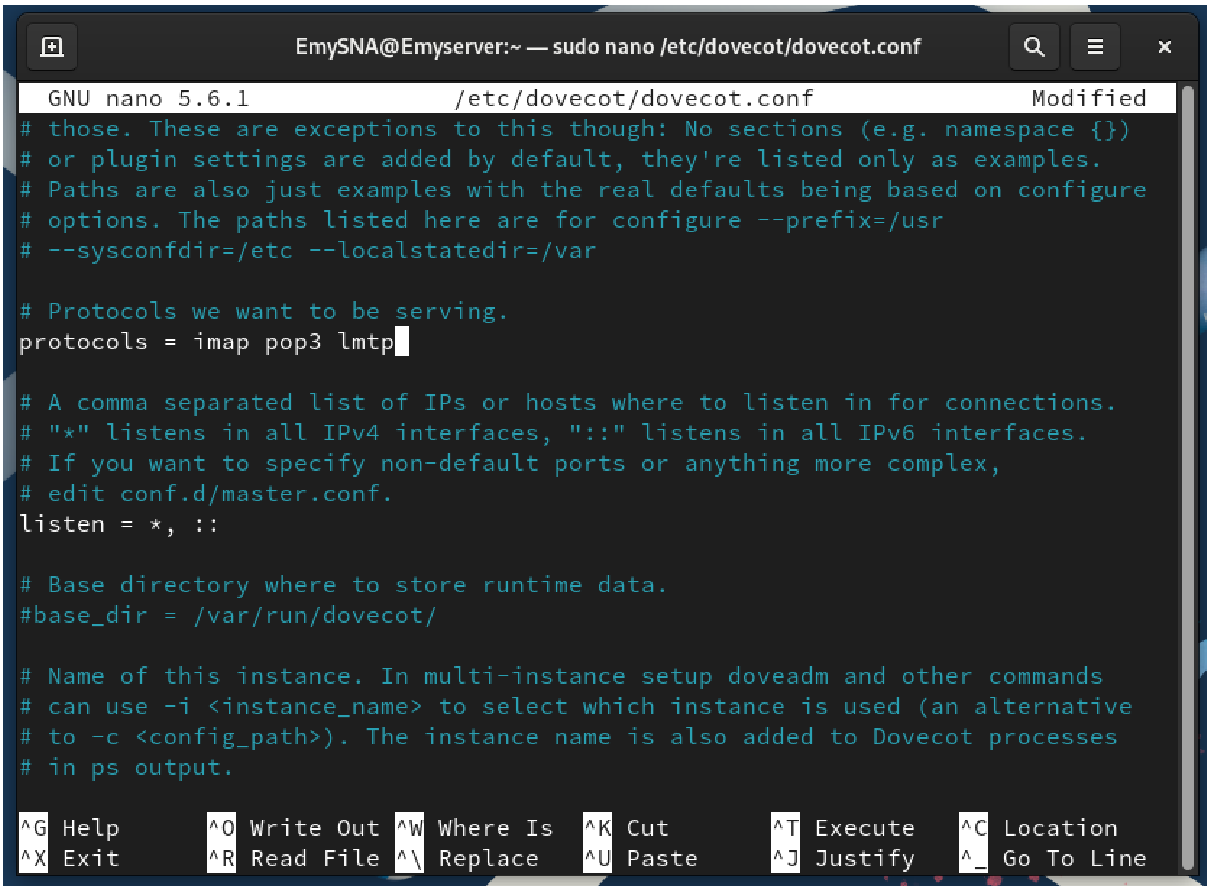


```
[EmySNA@Emyserver ~]$ sudo cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.con
f.backup
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/dovecot.conf
[EmySNA@Emyserver ~]$
```

Uncomment the following lines:

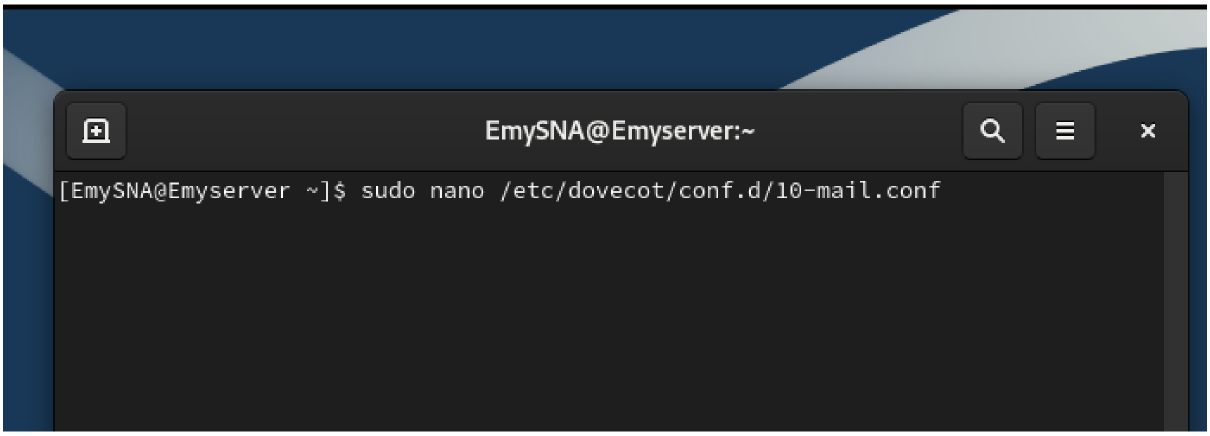
Protocol = imap pop3 lmtp (to enable IMAP, POP3, LMTP)

Listen = *, :: (listens on all IPv4, IPV6 address)



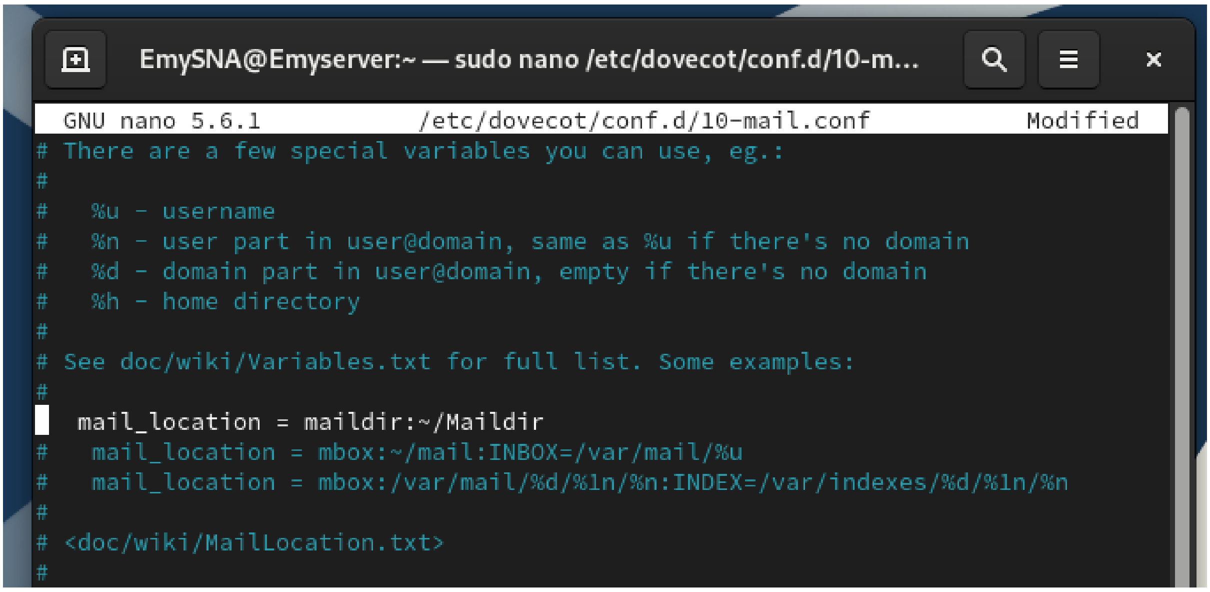
```
  GNU nano 5.6.1                 /etc/dovecot/dovecot.conf                 Modified
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Protocols we want to be serving.
protocols = imap pop3 lmtp

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
listen = *, ::

# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Name of this instance. In multi-instance setup doveadm and other commands
# can use -i <instance_name> to select which instance is used (an alternative
# to -c <config_path>). The instance name is also added to Dovecot processes
# in ps output.

^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
```

Open a text editor as root to Dovecot sub-configuration file for mail storage settings:



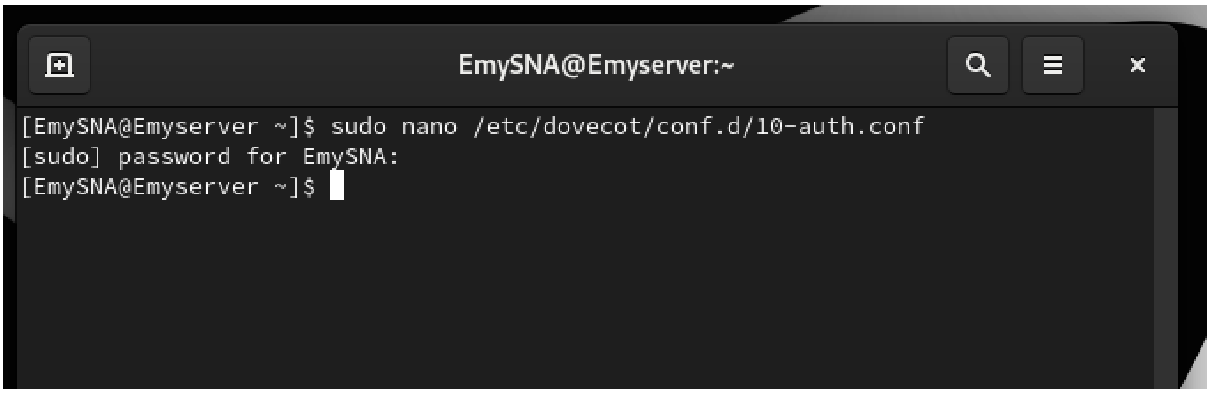
```
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/conf.d/10-mail.conf
```

Uncomment the following the following comment that stores each user’s email in a folder called ‘Maildir’ inside their own home directory:



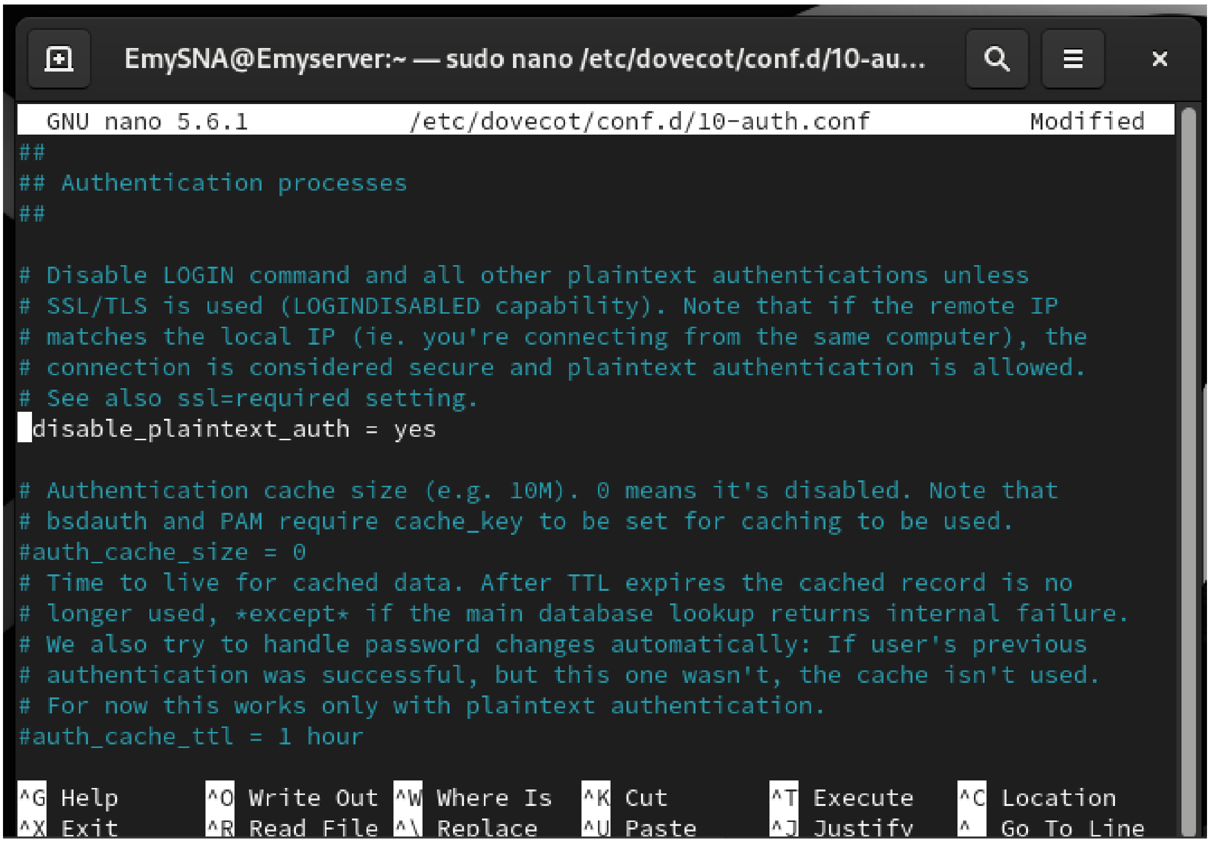
```
 GNU nano 5.6.1           /etc/dovecot/conf.d/10-mail.conf           Modified
# There are a few special variables you can use, eg.:
#
#   %u - username
#   %n - user part in user@domain, same as %u if there's no domain
#   %d - domain part in user@domain, empty if there's no domain
#   %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
  mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
```

The following command uses text editor to open Dovecot text authentication settings file with root privileges:



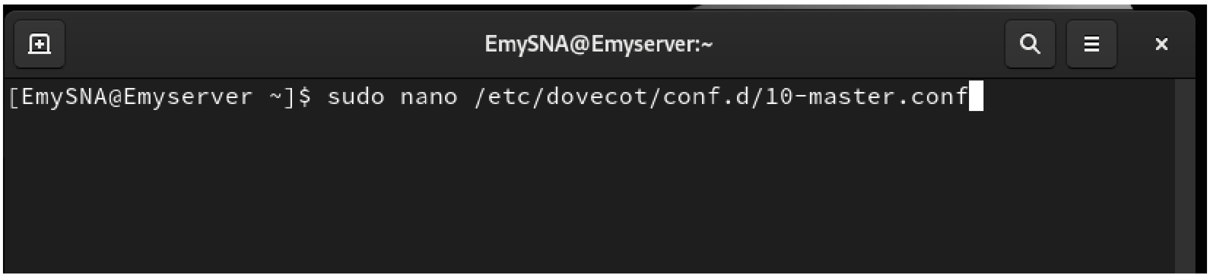
```
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/conf.d/10-auth.conf
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ 
```

Uncomment “disable_plaintext_auth=yes” to ensure passwords are protected unless using SSL as SSL encrypts the connection to ensure security:

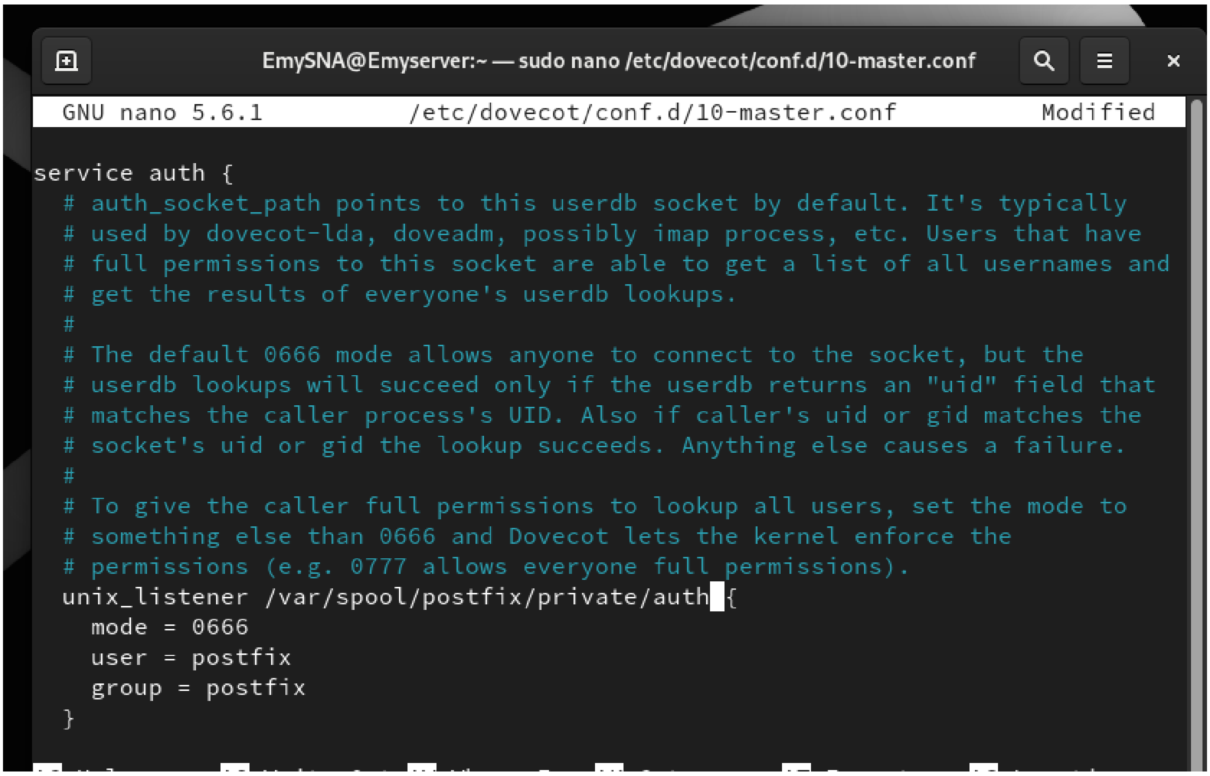


```
  GNU nano 5.6.1             /etc/dovecot/conf.d/10-auth.conf           Modified
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes

# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth and PAM require cache_key to be set for caching to be used.
#auth_cache_size = 0
# Time to live for cached data. After TTL expires the cached record is no
# longer used, *except* if the main database lookup returns internal failure.
# We also try to handle password changes automatically: If user's previous
# authentication was successful, but this one wasn't, the cache isn't used.
# For now this works only with plaintext authentication.
#auth_cache_ttl = 1 hour
```

Using a nano text editor to open a dovecot configuration file that runs authentication and communication with the system:



```
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/conf.d/10-master.conf
```



EmySNA@Emyserver:~ — sudo nano /etc/dovecot/conf.d/10-master.conf

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

service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Users that have
  # full permissions to this socket are able to get a list of all usernames and
  # get the results of everyone's userdb lookups.
  #
  # The default 0666 mode allows anyone to connect to the socket, but the
  # userdb lookups will succeed only if the userdb returns an "uid" field that
  # matches the caller process's UID. Also if caller's uid or gid matches the
  # socket's uid or gid the lookup succeeds. Anything else causes a failure.
  #
  # To give the caller full permissions to lookup all users, set the mode to
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
```

Service auth {} : this states the authentication service in dovecot

Within it the following lines are added,

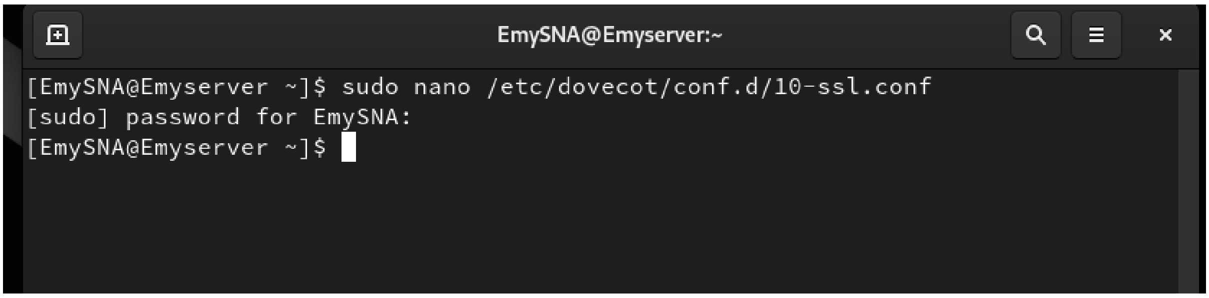
“unix_listener /va/spool/postfix/private/auth”: it creates a UNIX socket so postfix and dovecot can communicate

“mode = 0666”: set permissions so processes can read and write to socket

“User = postfix”: only user can use this socket file

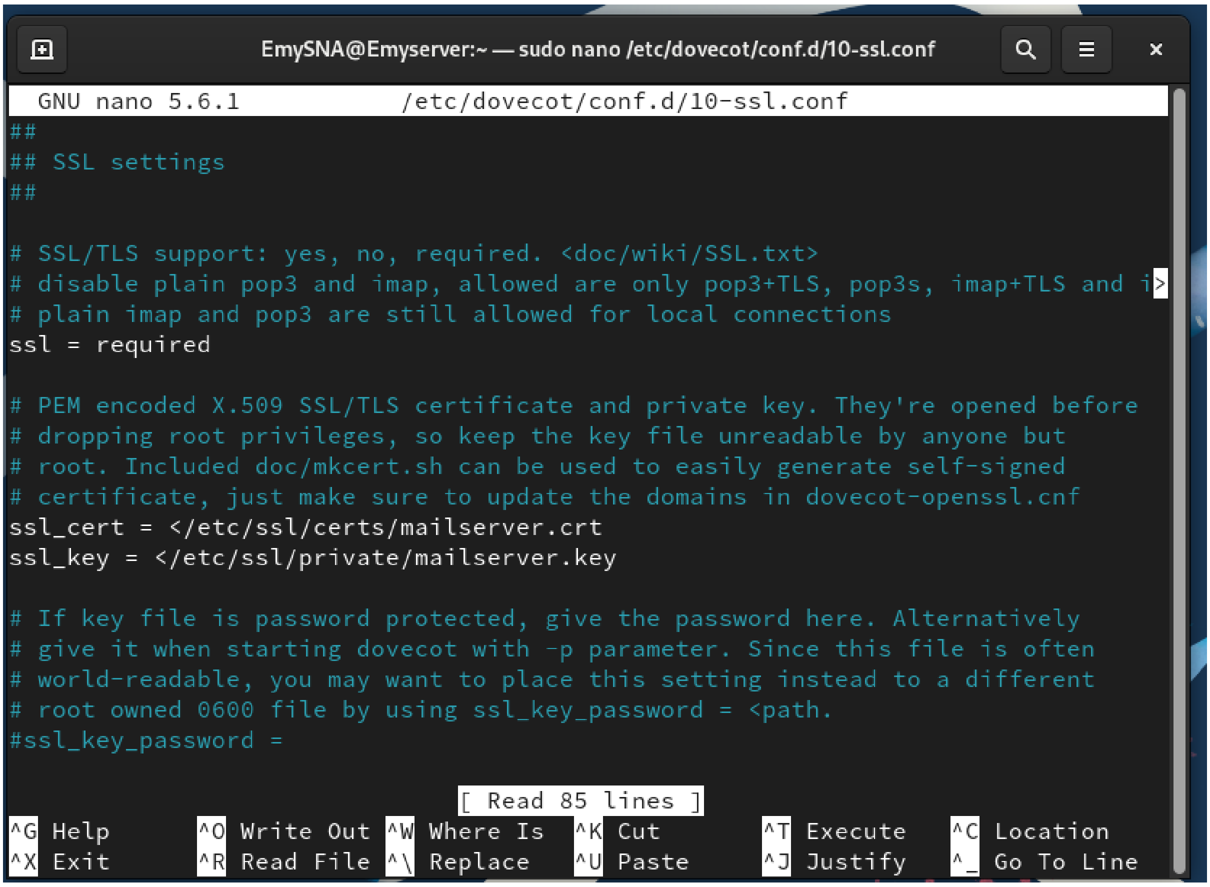
“group = postfix": only group can use this file

Next the SSL/TLS settings file for dovecot is opened as root using nano text editor with root:



```
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/conf.d/10-ssl.conf
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ 
```

We ensure the following lines are uncommented:



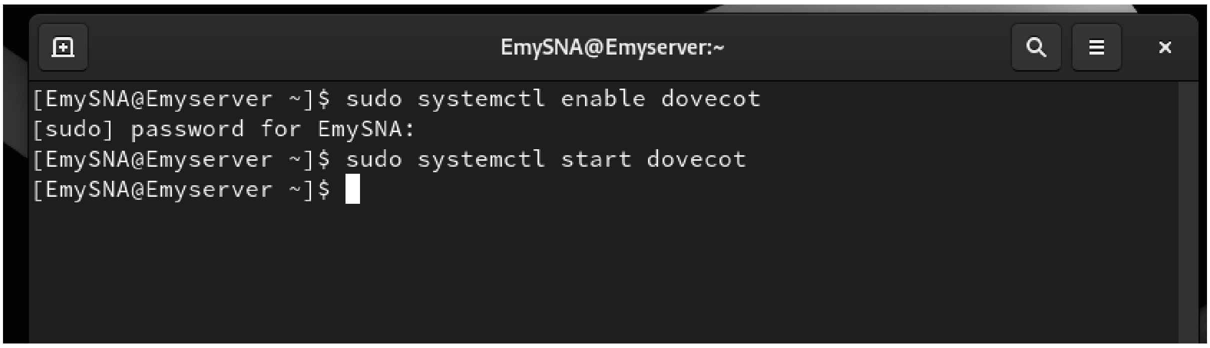
```
##
## SSL settings
##

# 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/ssl/certs/mailserver.crt
ssl_key = </etc/ssl/private/mailserver.key

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path.
#ssl_key_password =

                              [ Read 85 lines ]
```

“ssl = required”: this will make dovecot only allow encrypted (SSL/TSL) connections

"ssl_cert = </etc/pki/dovecot/ssl/certs/dovecot.pem”: the public file, SSL certificate, which clients use to identify the server

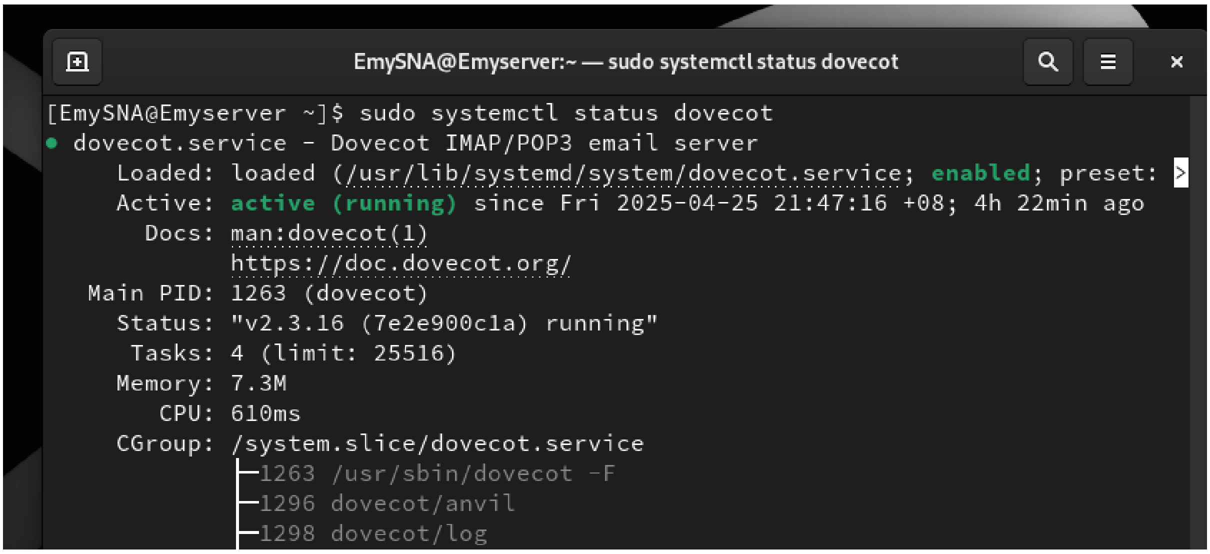
“ssl_key = </etc/pki/dovecot/private/dovecot.key”: the private key, which is used to decrypt secure messages

Then enable and start dovecot services:



```
[EmySNA@Emyserver ~]$ sudo systemctl enable dovecot
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo systemctl start dovecot
[EmySNA@Emyserver ~]$ █
```

Then we ensure everything is running properly through checking the status:

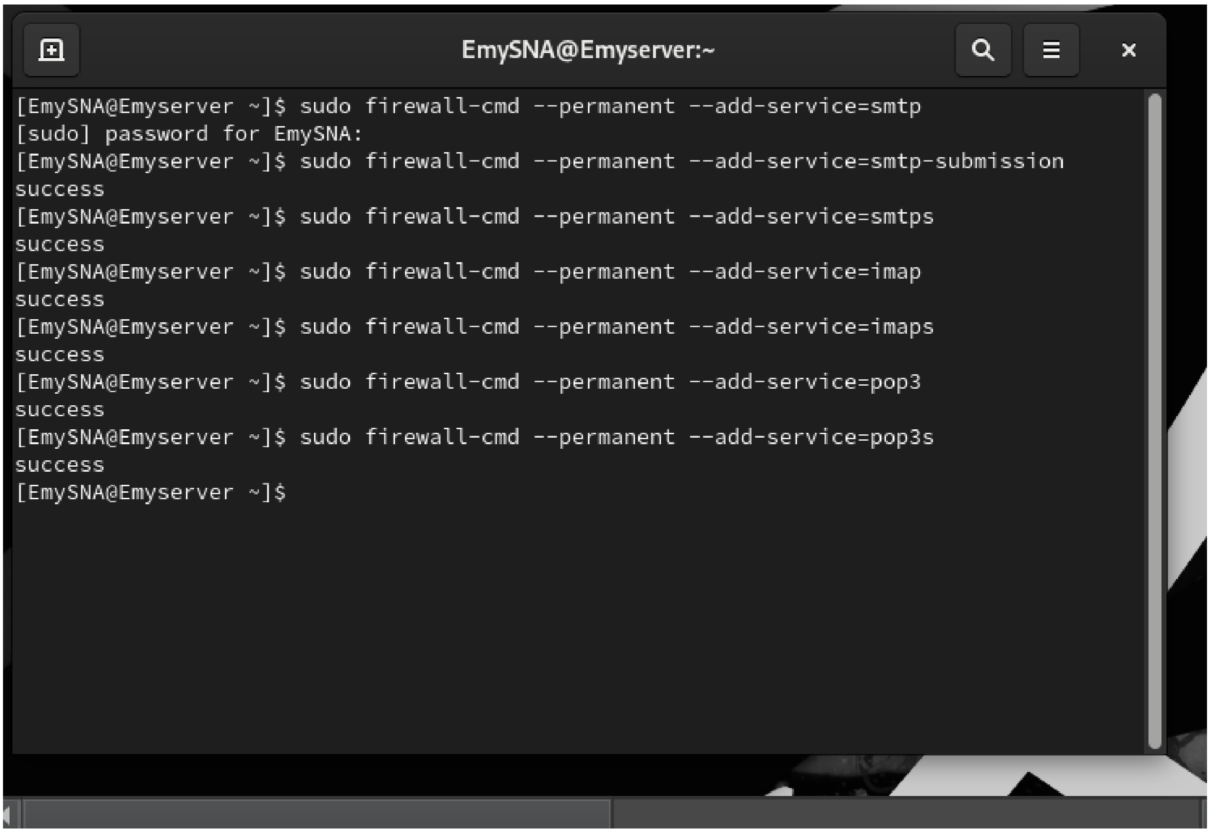


```
[EmySNA@Emyserver ~]$ sudo systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
     Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled; preset: >
     Active: active (running) since Fri 2025-04-25 21:47:16 +08; 4h 22min ago
       Docs: man:dovecot(1)
             https://doc.dovecot.org/
   Main PID: 1263 (dovecot)
     Status: "v2.3.16 (7e2e900c1a) running"
      Tasks: 4 (limit: 25516)
     Memory: 7.3M
        CPU: 610ms
     CGroup: /system.slice/dovecot.service
             ├─1263 /usr/sbin/dovecot -F
             ├─1296 dovecot/anvil
             ├─1298 dovecot/log
```

Firewall/Ports:

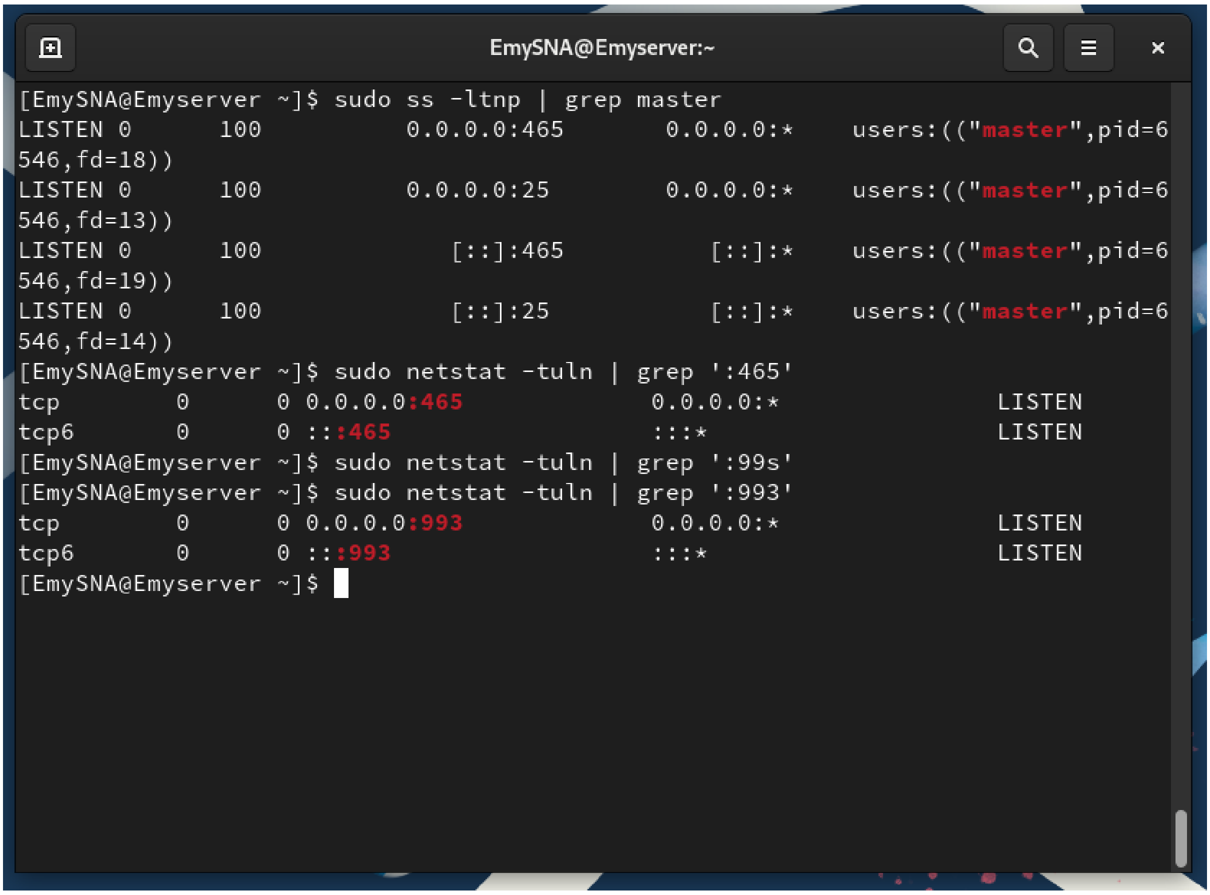
Then all traffic, sent or received through the ports, is ensured to go through the firewall

ports used and their use: SMTP for sending outgoing emails from server, SMTP-submission is to securely send mail from client, SMTPS is for sending mail over a secure and encrypted connection like SSL/TLS, IMAP is used to read mail without the need to downloading them, IMAPS is to read emails without downloading them yet over a secure connection, POP enables users to download emails from server and remove them, and POP3S does the same job but securely, all to keep harmful data from intercepting the network connection.



```
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=smtp
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=smtp-submission
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=smtps
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=imap
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=imaps
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=pop3
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-service=pop3s
success
[EmySNA@Emyserver ~]$
```

We then check all active (listening) ports being used by posfix master process that manages the mail services such as SMTP, submission, etc.:



```
[EmySNA@Emyserver ~]$ sudo ss -ltnp | grep master
LISTEN 0      100          0.0.0.0:465        0.0.0.0:*    users:(("master",pid=6
546,fd=18))
LISTEN 0      100          0.0.0.0:25         0.0.0.0:*    users:(("master",pid=6
546,fd=13))
LISTEN 0      100             [::]:465           [::]:*    users:(("master",pid=6
546,fd=19))
LISTEN 0      100             [::]:25            [::]:*    users:(("master",pid=6
546,fd=14))
[EmySNA@Emyserver ~]$ sudo netstat -tuln | grep ':465'
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN
tcp6       0      0 :::465                  :::*                    LISTEN
[EmySNA@Emyserver ~]$ sudo netstat -tuln | grep ':99s'
[EmySNA@Emyserver ~]$ sudo netstat -tuln | grep ':993'
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp6       0      0 :::993                  :::*                    LISTEN
[EmySNA@Emyserver ~]$
```

Ss: to show all active network sockets

-l: is to show the listening ports AKA the ones waiting for any sort of connection

-t: to show tcp connections only

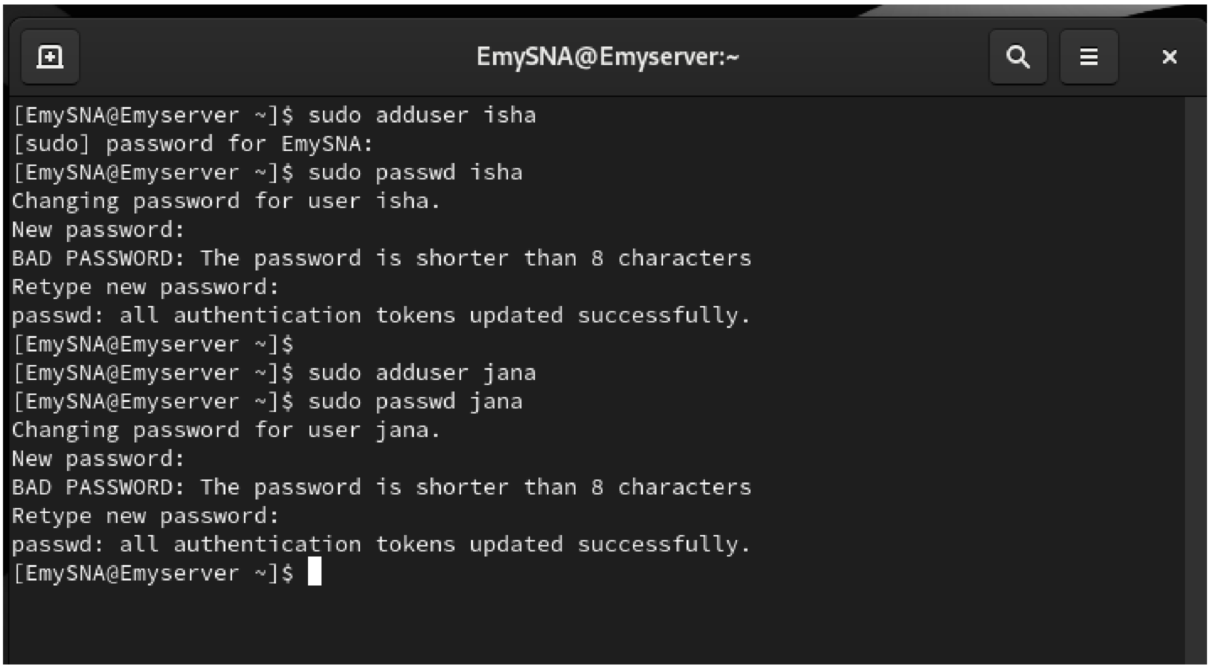
-n: to show addresses and ports not names

-p: to show processes and program using the port

| grep master: this is so only lines that mention ‘master’ (main controller process of postfix) show up.

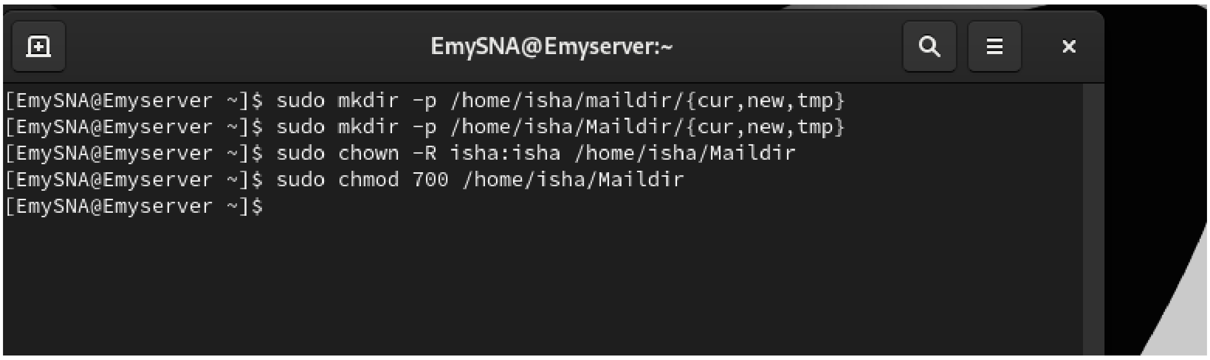
Testing

Then to test it we create users with different names and passwords using the following steps:



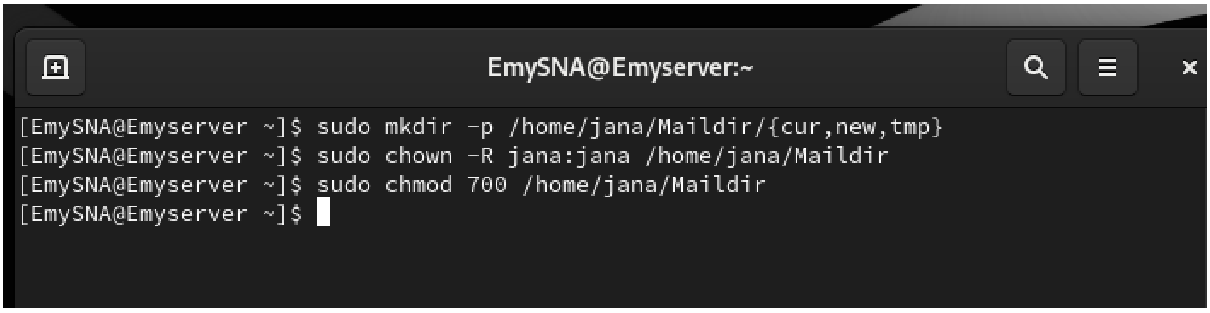
```
[EmySNA@Emyserver ~]$ sudo adduser isha
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo passwd isha
Changing password for user isha.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[EmySNA@Emyserver ~]$
[EmySNA@Emyserver ~]$ sudo adduser jana
[EmySNA@Emyserver ~]$ sudo passwd jana
Changing password for user jana.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[EmySNA@Emyserver ~]$
```

We then create a new directory for each, then change the ownership of the owner and group to the respective mail user, and give each respective user full access to read, write and execute using “chmod 700”:



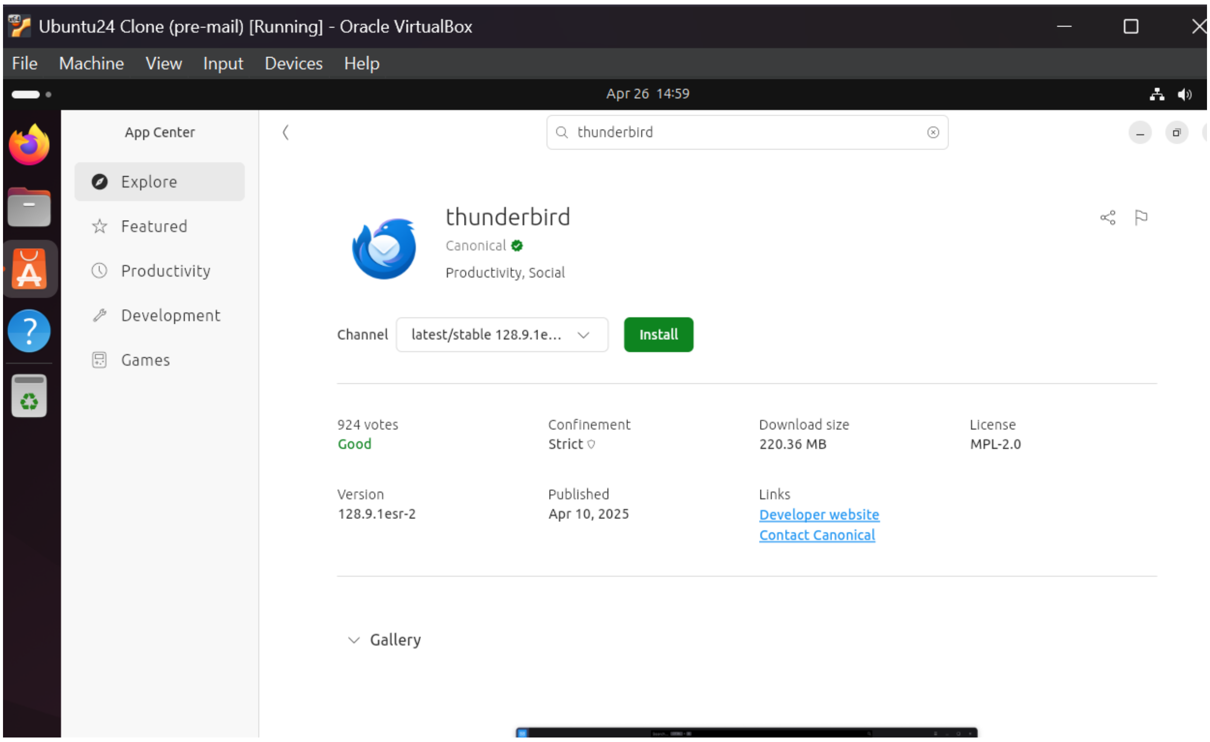
```
[EmySNA@Emyserver ~]$ sudo mkdir -p /home/isha/maildir/{cur,new,tmp}
[EmySNA@Emyserver ~]$ sudo mkdir -p /home/isha/Maildir/{cur,new,tmp}
[EmySNA@Emyserver ~]$ sudo chown -R isha:isha /home/isha/Maildir
[EmySNA@Emyserver ~]$ sudo chmod 700 /home/isha/Maildir
[EmySNA@Emyserver ~]$
```

Then we repeat the previous steps for the 2nd user:



```
[EmySNA@Emyserver ~]$ sudo mkdir -p /home/jana/Maildir/{cur,new,tmp}
[EmySNA@Emyserver ~]$ sudo chown -R jana:jana /home/jana/Maildir
[EmySNA@Emyserver ~]$ sudo chmod 700 /home/jana/Maildir
[EmySNA@Emyserver ~]$
```

Install thunderbird on client machine (ubuntu)


Ubuntu24 Clone (pre-mail) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apr 26 14:59
App Center
Explore
Featured
Productivity
Development
Games
thunderbird
Gallery

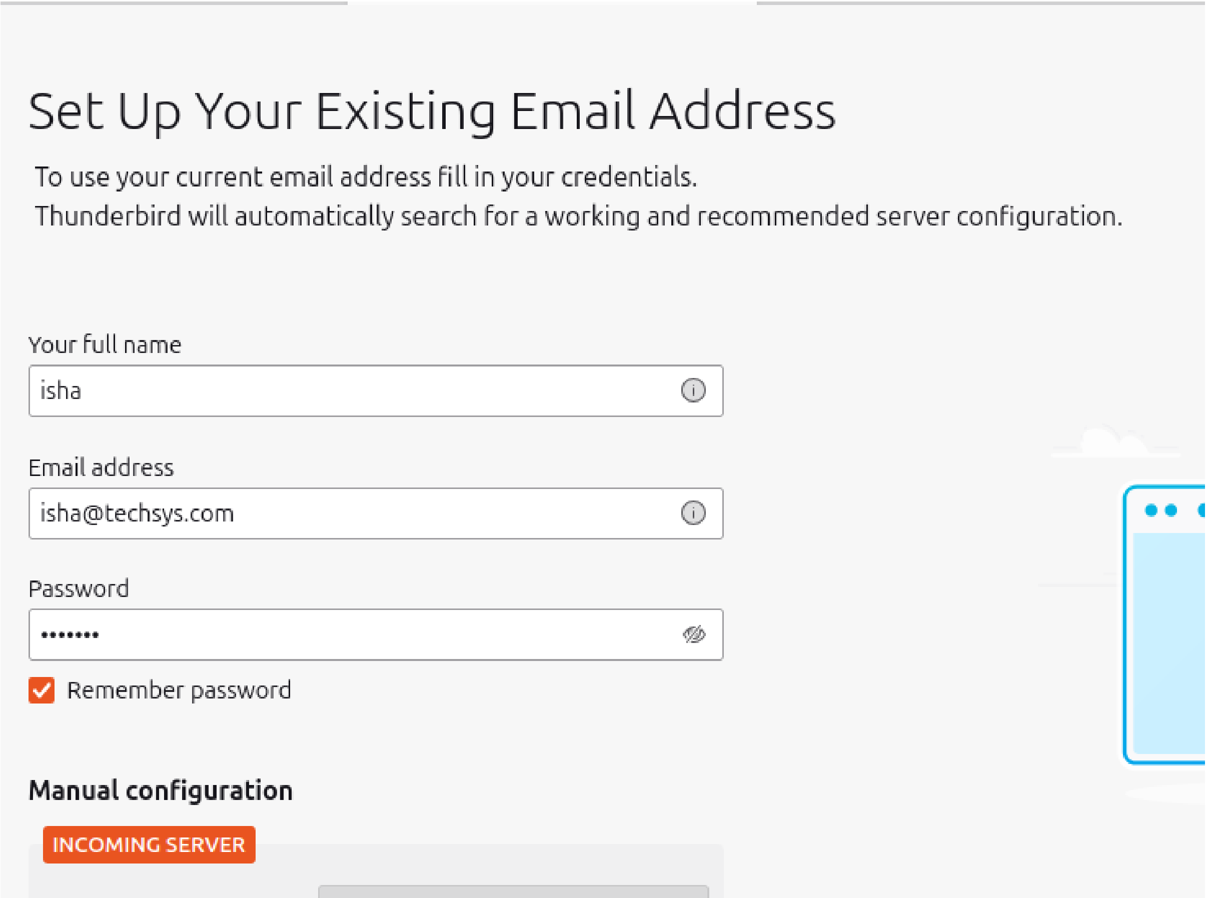
thunderbird
Canonical
Productivity, Social

Channel latest/stable 128.9.1e... Install

924 votes Good
Confinement Strict
Download size 220.36 MB
License MPL-2.0
Version 128.9.1esr-2
Published Apr 10, 2025
Links Developer website Contact Canonical

A problem arise as I'm trying to log in, steps to solve it in troubleshooting section, issue 1, we then continue from it to this next step:

Next I enter the details of created users:



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: isha

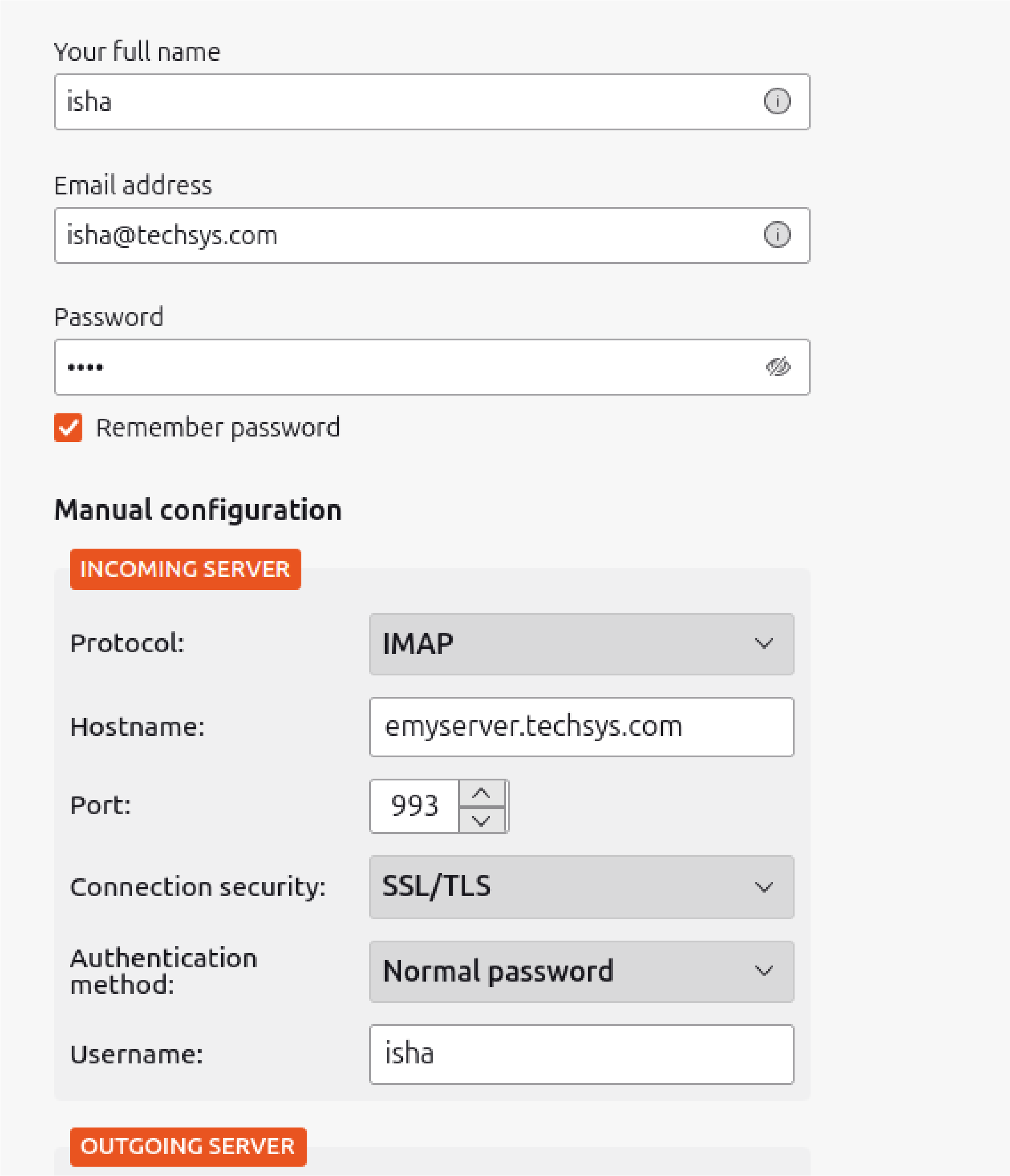
Email address: isha@techsys.com

Password: •••••••

☑ Remember password

Manual configuration

Then enter the configuration of user:



Your full name

isha

Email address

isha@techsys.com

Password

••••

☑ Remember password

Manual configuration

INCOMING SERVER

Protocol: IMAP

Hostname: emyserver.techsys.com

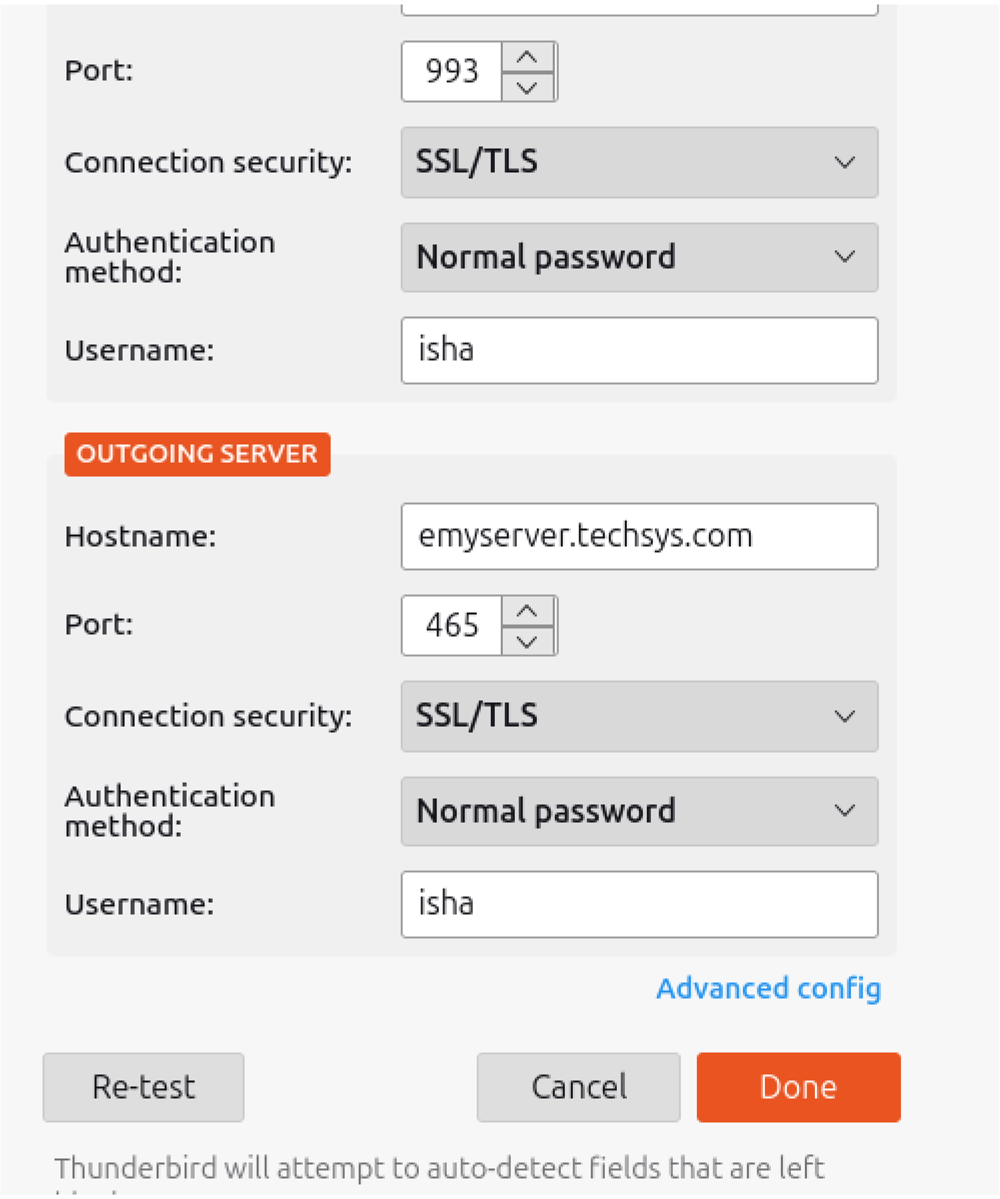
Port: 993

Connection security: SSL/TLS

Authentication method: Normal password

Username: isha

OUTGOING SERVER



Port: 993

Connection security: SSL/TLS

Authentication method: Normal password

Username: isha

OUTGOING SERVER

Hostname: emyserver.techsys.com

Port: 465

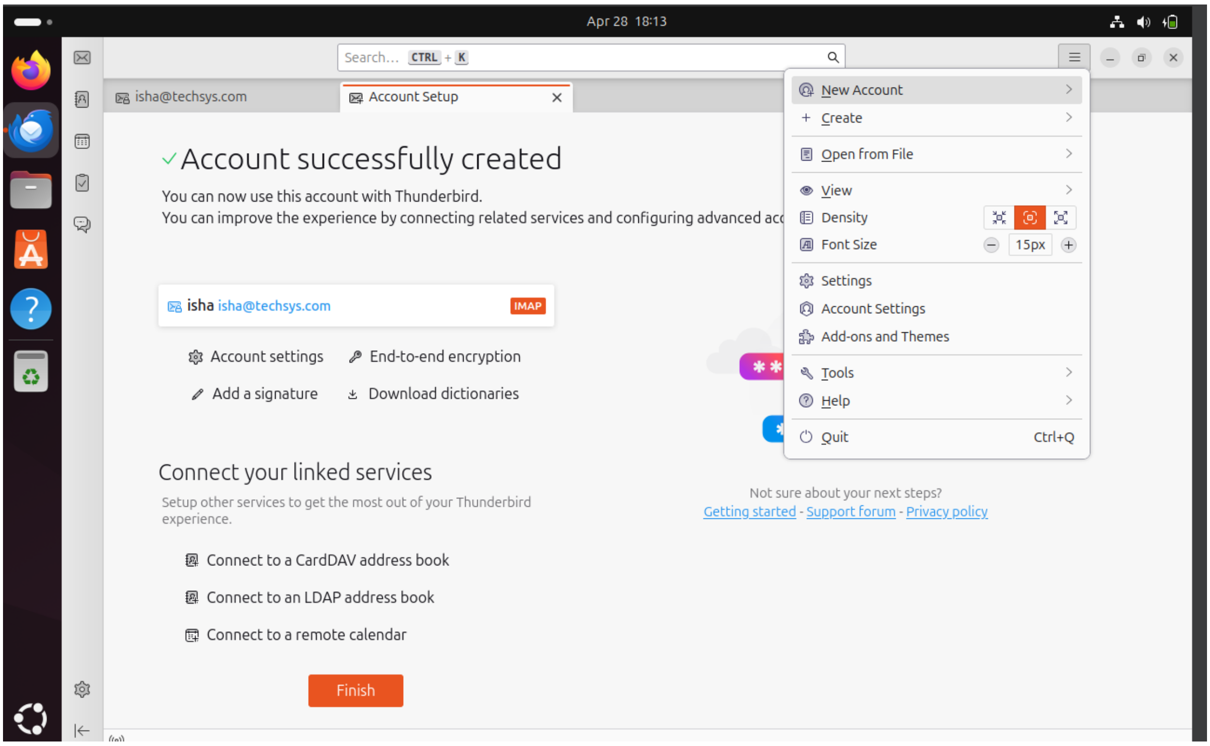
Connection security: SSL/TLS

Authentication method: Normal password

Username: isha

Thunderbird will attempt to auto-detect fields that are left

After logging in, time to log in into the 2nd user account by clicking the three lines and then “new account”:



Account successfully created

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

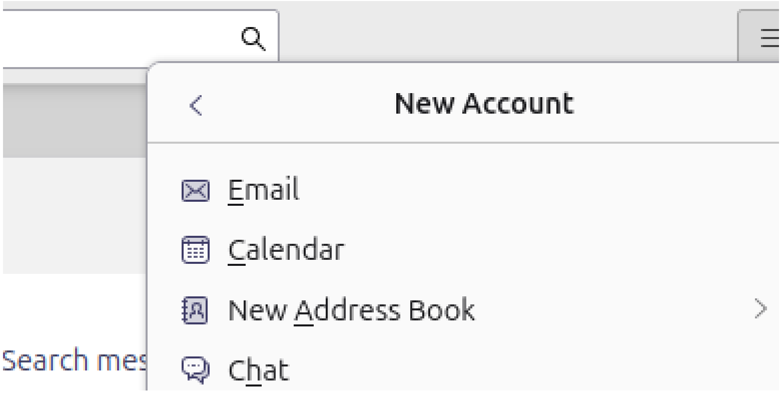
isha isha@techsys.com IMAP

Connect your linked services

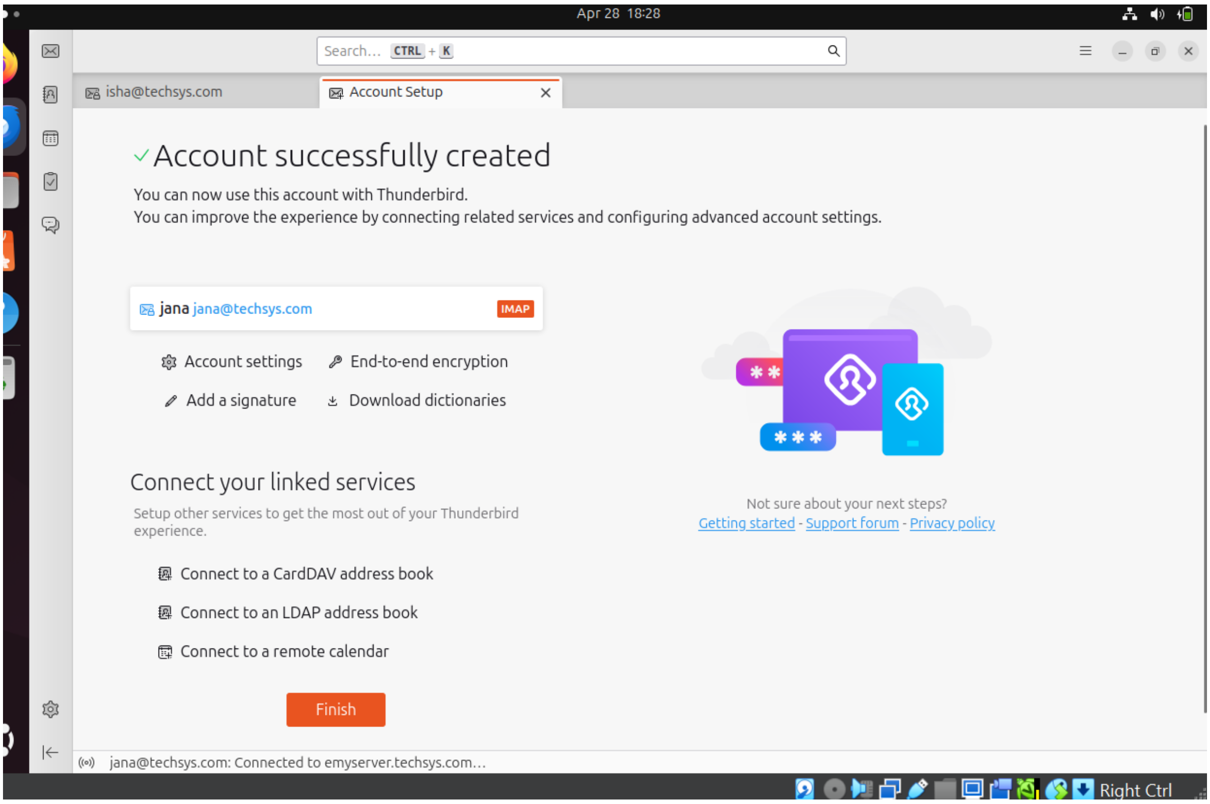
Setup other services to get the most out of your Thunderbird experience.

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

we then click “Email”



And repeat the previous steps for the 2nd user:


Apr 28 18:28

isha@techsys.com

Account Setup

✓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.

jana jana@techsys.com IMAP

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.

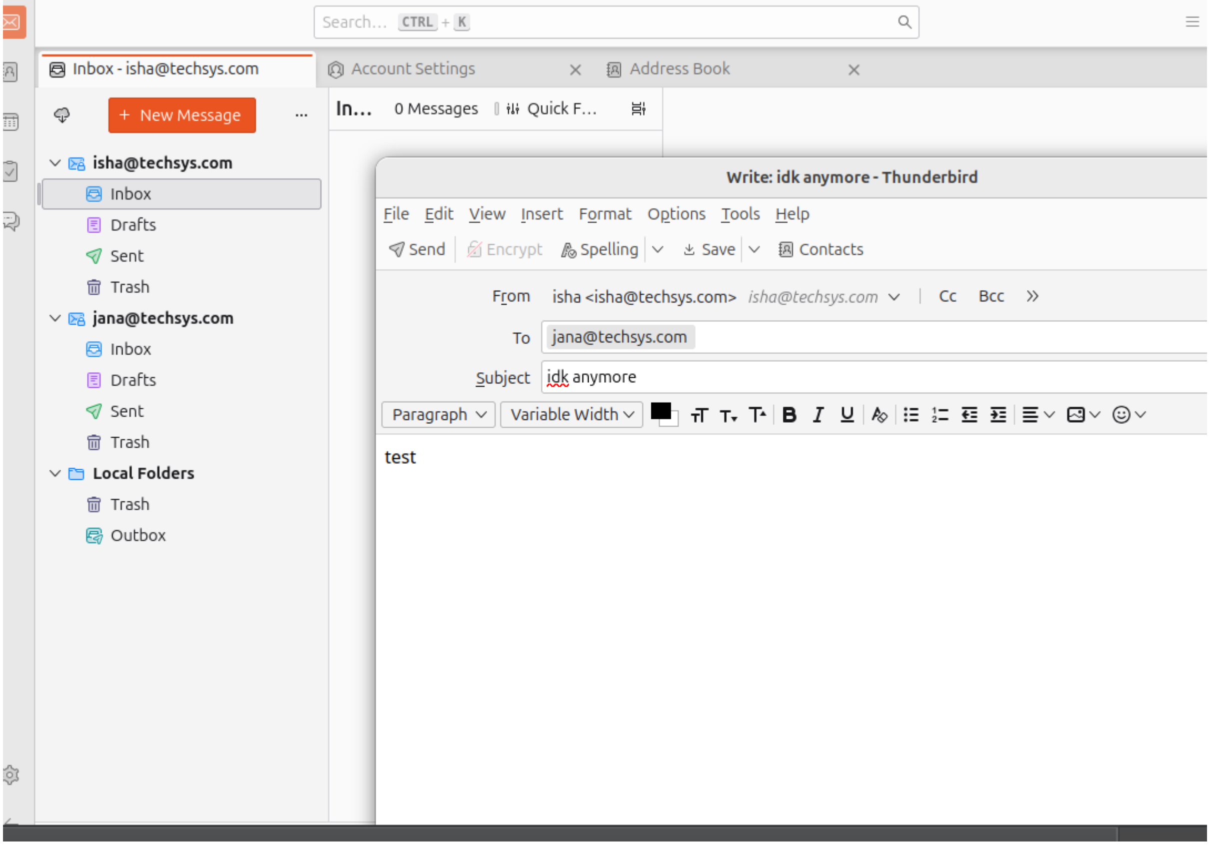
- Connect to a CardDAV address book
- Connect to an LDAP address book
- Connect to a remote calendar

Finish

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

jana@techsys.com: Connected to emyserver.techsys.com…

Now let’s try sending an Email as a test, to send an email from “isha” user “jana” we click “+ New message” write the mail and then send it:


Inbox - isha@techsys.com | Account Settings | Address Book

+ New Message

- isha@techsys.com: Inbox, Drafts, Sent, Trash
- jana@techsys.com: Inbox, Drafts, Sent, Trash
- Local Folders: Trash, Outbox

In… 0 Messages Quick F…

Write: idk anymore - Thunderbird

File Edit View Insert Format Options Tools Help

Send Encrypt Spelling Save Contacts

From: isha <isha@techsys.com> isha@techsys.com

To: jana@techsys.com

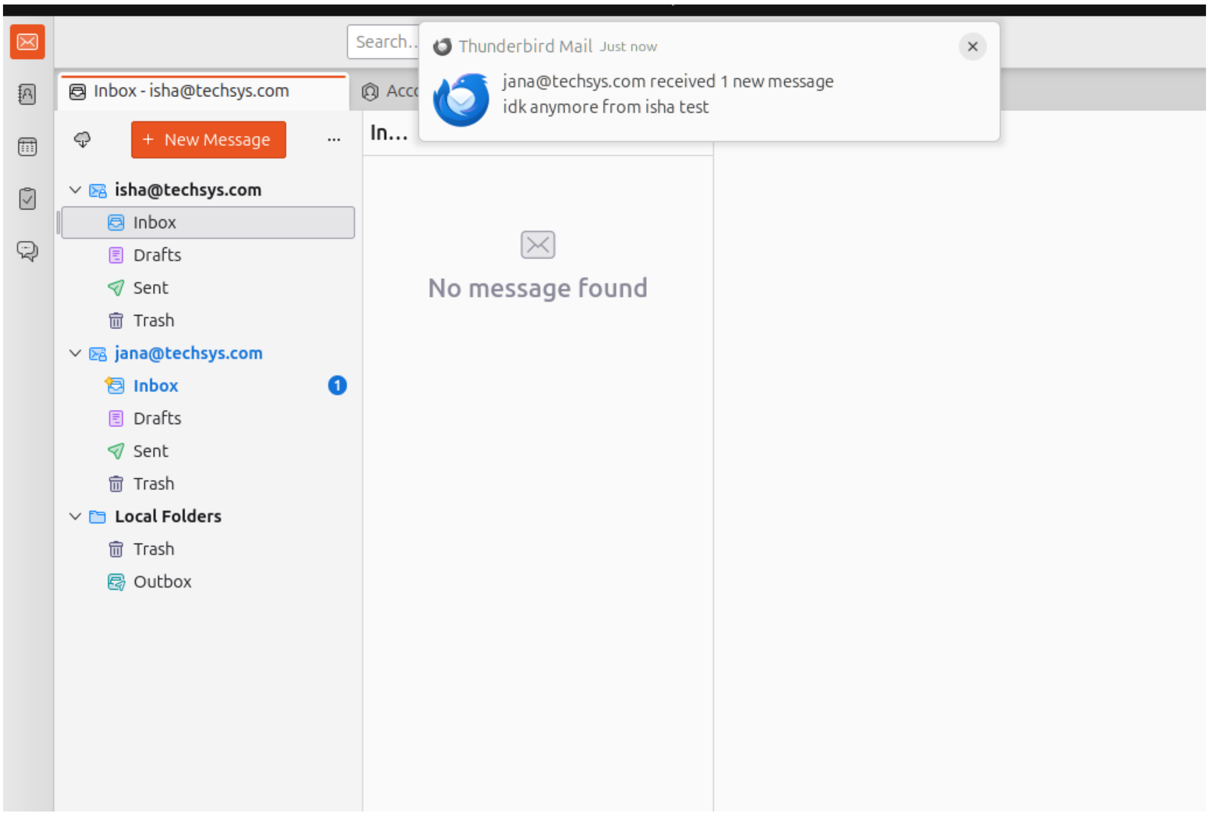
Subject: idk anymore

Paragraph · Variable Width

test

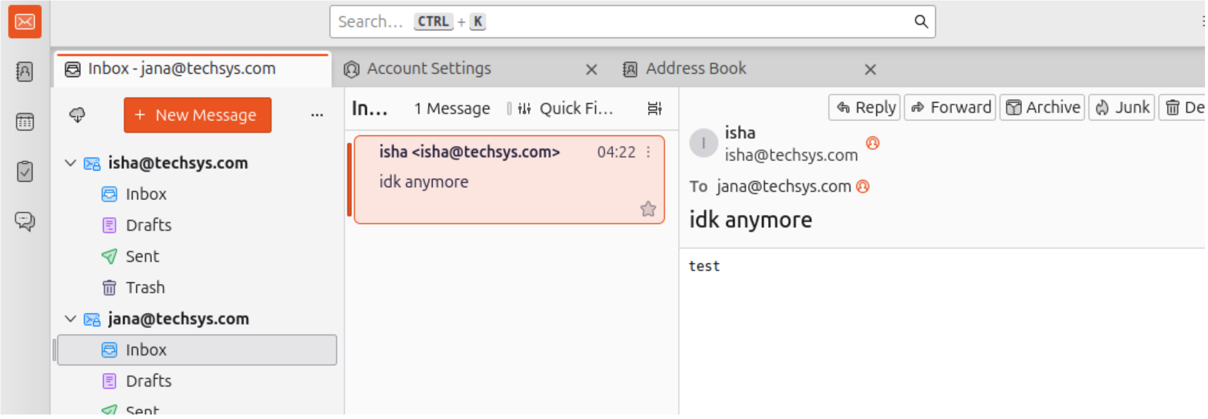
Another problem was faced in sending the mail, steps to solving it in troubleshooting section, issue 2. then we continue from it to this next step:

And the Email is successfully received by the recipient:



Thunderbird Mail Just now

jana@techsys.com received 1 new message
idk anymore from isha test



isha <isha@techsys.com> 04:22
idk anymore

isha
isha@techsys.com
To jana@techsys.com

idk anymore

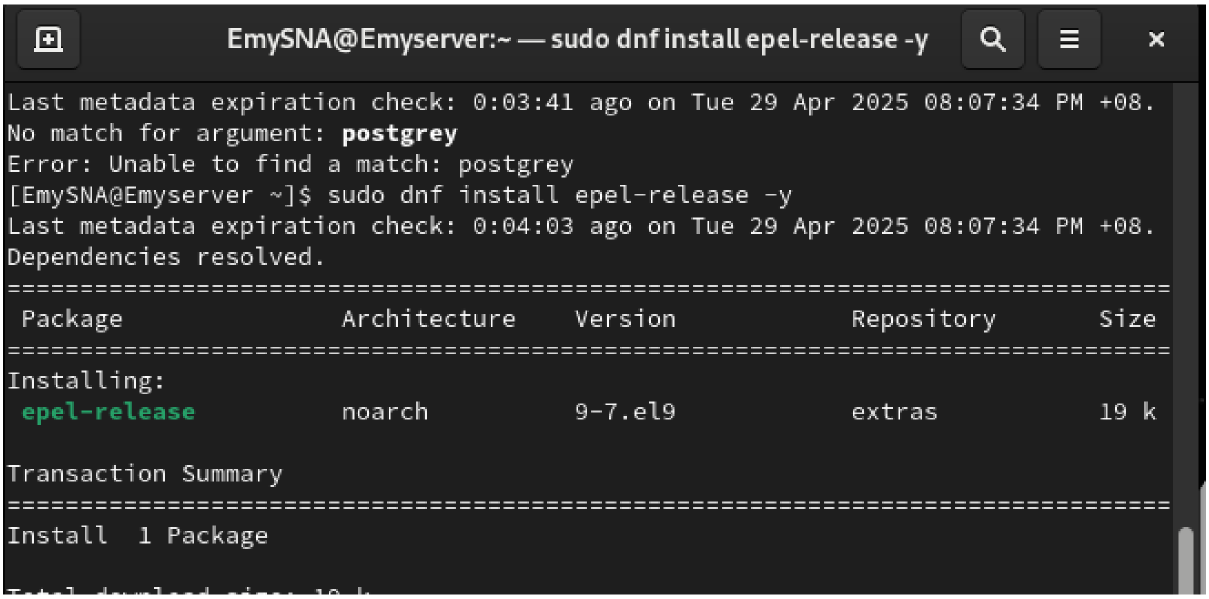
test

And with that we're done making a fully functioning email server.

Additional service:

For the additional service I'll be installing a Postfix server called Postgrey mail which is used for greylisting, which is a method to filters spam by temporarily rejecting emails from unknown senders as spam sending server don't retry sending emails but legitimate mail servers do so after a short duration of time hence if the server retries sending mail it's regarded as legitimate mail and delivered normally on the mail server's second attempt.

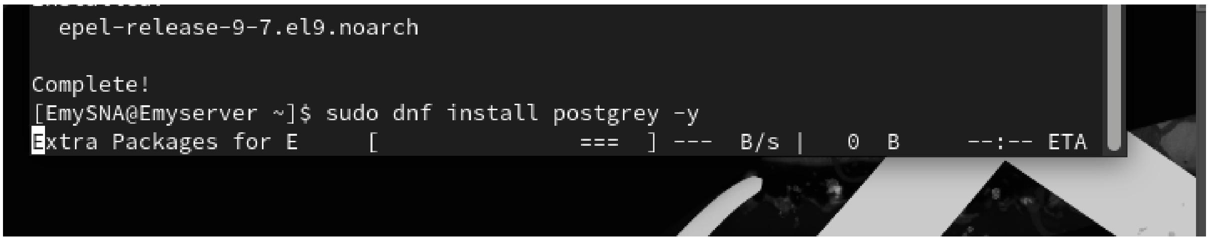
As postgrey isn't found in my machine I must enable EPEL (extra packages for enterprise linux):



EmySNA@Emyserver:~ — sudo dnf install epel-release -y

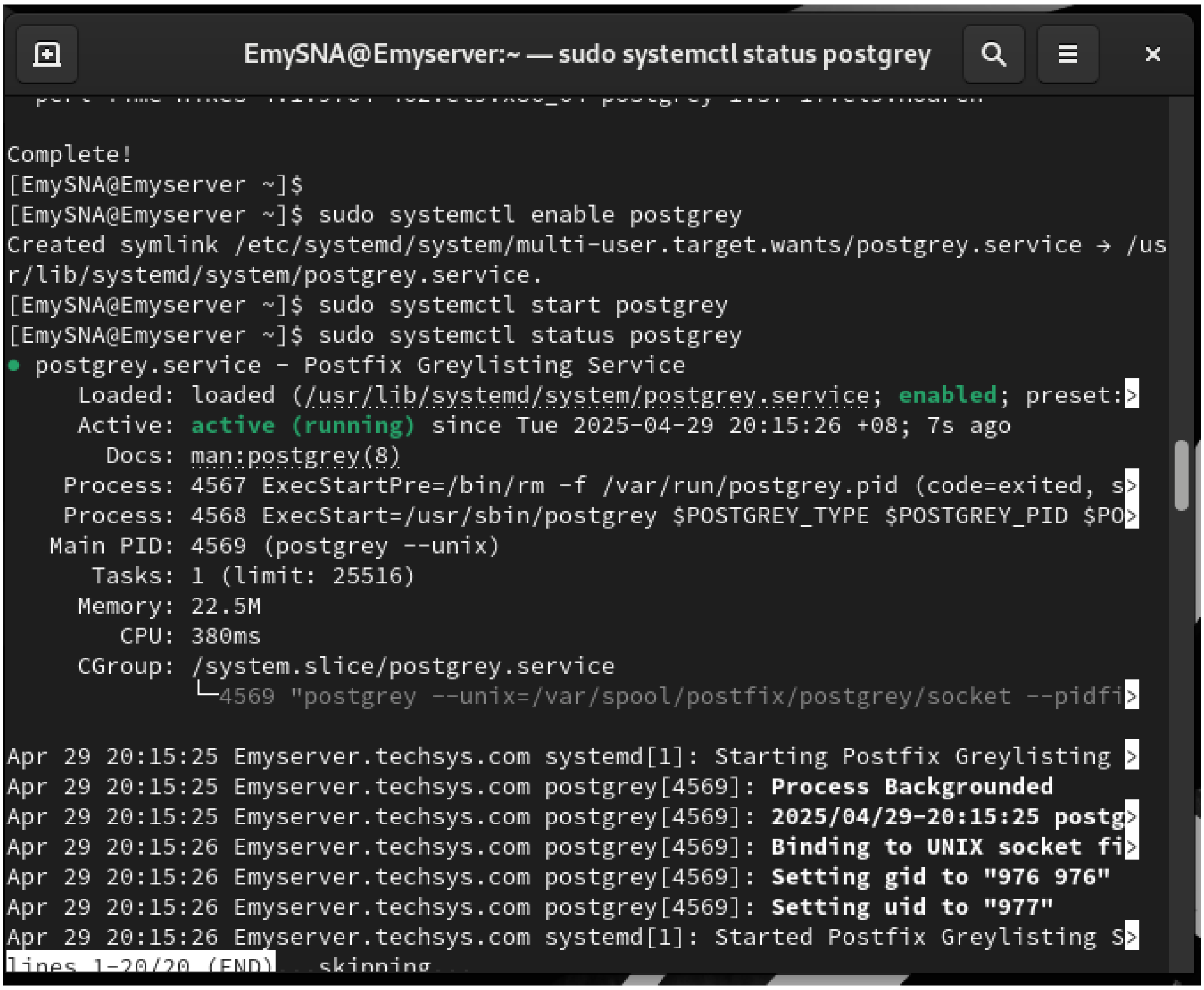
```
Last metadata expiration check: 0:03:41 ago on Tue 29 Apr 2025 08:07:34 PM +08.
No match for argument: postgrey
Error: Unable to find a match: postgrey
[EmySNA@Emyserver ~]$ sudo dnf install epel-release -y
Last metadata expiration check: 0:04:03 ago on Tue 29 Apr 2025 08:07:34 PM +08.
Dependencies resolved.
================================================================================
 Package                Architecture    Version            Repository      Size
================================================================================
Installing:
 epel-release           noarch          9-7.el9            extras          19 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 19 k
```

Then I installed postgrey:



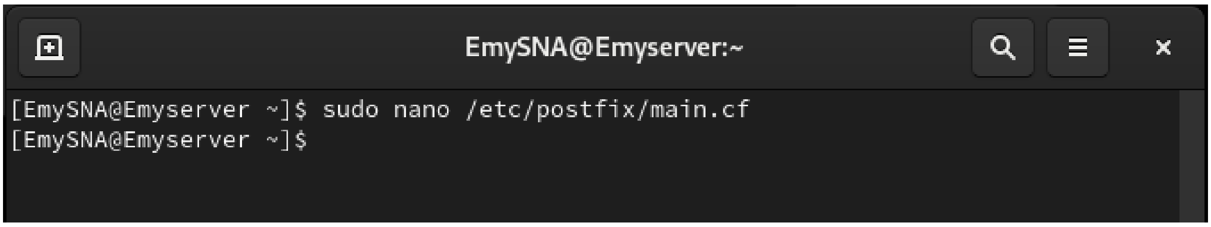
```
Installed:
  epel-release-9-7.el9.noarch

Complete!
[EmySNA@Emyserver ~]$ sudo dnf install postgrey -y
Extra Packages for E     [                ===  ] ---  B/s |   0  B     --:-- ETA
```

Afterwards postgrey is enabled started then I checked it’s status:



```
Complete!
[EmySNA@Emyserver ~]$
[EmySNA@Emyserver ~]$ sudo systemctl enable postgrey
Created symlink /etc/systemd/system/multi-user.target.wants/postgrey.service → /us
r/lib/systemd/system/postgrey.service.
[EmySNA@Emyserver ~]$ sudo systemctl start postgrey
[EmySNA@Emyserver ~]$ sudo systemctl status postgrey
● postgrey.service - Postfix Greylisting Service
     Loaded: loaded (/usr/lib/systemd/system/postgrey.service; enabled; preset:>
     Active: active (running) since Tue 2025-04-29 20:15:26 +08; 7s ago
       Docs: man:postgrey(8)
    Process: 4567 ExecStartPre=/bin/rm -f /var/run/postgrey.pid (code=exited, s>
    Process: 4568 ExecStart=/usr/sbin/postgrey $POSTGREY_TYPE $POSTGREY_PID $PO>
   Main PID: 4569 (postgrey --unix)
      Tasks: 1 (limit: 25516)
     Memory: 22.5M
        CPU: 380ms
     CGroup: /system.slice/postgrey.service
             └─4569 "postgrey --unix=/var/spool/postfix/postgrey/socket --pidfi>

Apr 29 20:15:25 Emyserver.techsys.com systemd[1]: Starting Postfix Greylisting >
Apr 29 20:15:25 Emyserver.techsys.com postgrey[4569]: Process Backgrounded
Apr 29 20:15:25 Emyserver.techsys.com postgrey[4569]: 2025/04/29-20:15:25 postg>
Apr 29 20:15:26 Emyserver.techsys.com postgrey[4569]: Binding to UNIX socket fi>
Apr 29 20:15:26 Emyserver.techsys.com postgrey[4569]: Setting gid to "976 976"
Apr 29 20:15:26 Emyserver.techsys.com postgrey[4569]: Setting uid to "977"
Apr 29 20:15:26 Emyserver.techsys.com systemd[1]: Started Postfix Greylisting S>
lines 1-20/20 (END)...skipping...
```

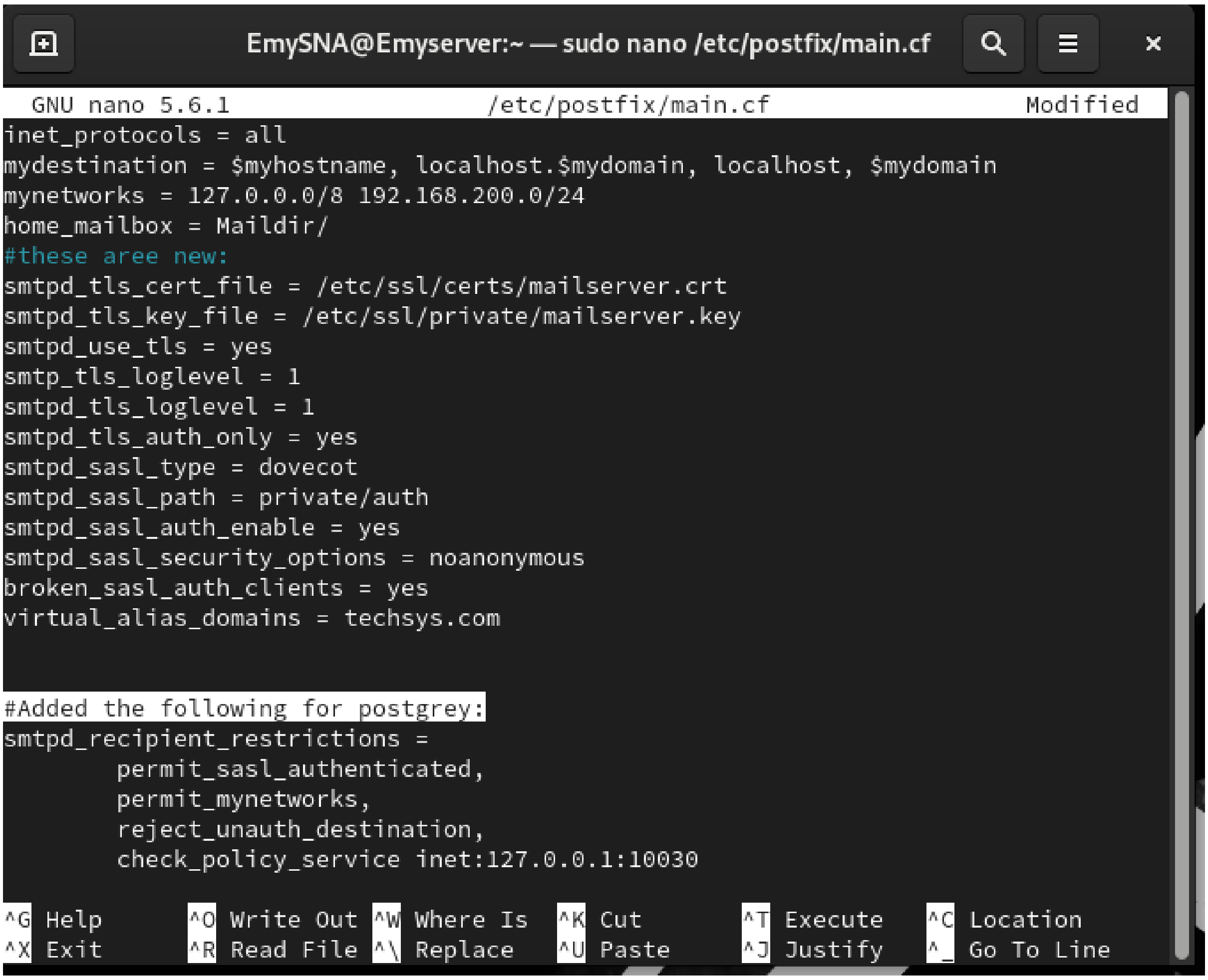
Next postgrey must be configured so we add it’s configuration inside postfix/main.cf file:



```
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/main.cf
[EmySNA@Emyserver ~]$
```

The last lines in the following picture are add:

smtpd_recipient_restrictions (Defines a set of rules for handling incoming email) permit_sasl_authenticated(Allows email from authenticated users) permit_mynetworks (Allows email from trusted networks) reject_unauth_destination (rejects email if the destination is not authorized) check_policy_service inet:127.0.0.1:10030(This is used for spam filtering or greylisting.)



```
  GNU nano 5.6.1                  /etc/postfix/main.cf                     Modified
inet_protocols = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mynetworks = 127.0.0.0/8 192.168.200.0/24
home_mailbox = Maildir/
#these aree new:
smtpd_tls_cert_file = /etc/ssl/certs/mailserver.crt
smtpd_tls_key_file = /etc/ssl/private/mailserver.key
smtpd_use_tls = yes
smtp_tls_loglevel = 1
smtpd_tls_loglevel = 1
smtpd_tls_auth_only = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
virtual_alias_domains = techsys.com


#Added the following for postgrey:
smtpd_recipient_restrictions =
        permit_sasl_authenticated,
        permit_mynetworks,
        reject_unauth_destination,
        check_policy_service inet:127.0.0.1:10030

^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
```

smtpd_recipient_restrictions = (Defines the rules that are used to decide if incoming mail is accepted or rejected)

permit_sasl_authenticated (mail from SASL authenticated users is accepted)

permit_mynetworks (mail from IP addresses or subnets defined in “mynetwork” in “mail.cf” is accepted)

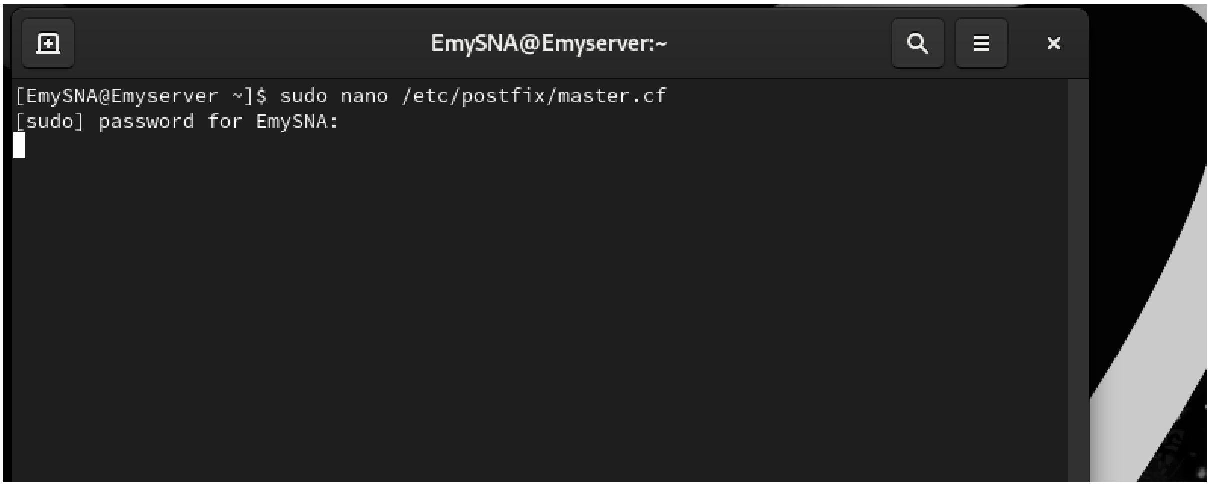
reject_unauth_destination (mail from IP addresses or subnets not defined or authorized in “mynetwork” in “mail.cf” is rejected)

check_policy_service inet:127.0.0.1:10030 (postfix socket specification tells postfix to connect to a policy server such as postgrey, that listens on port 10030, running on the same machine)

Troubleshooting:

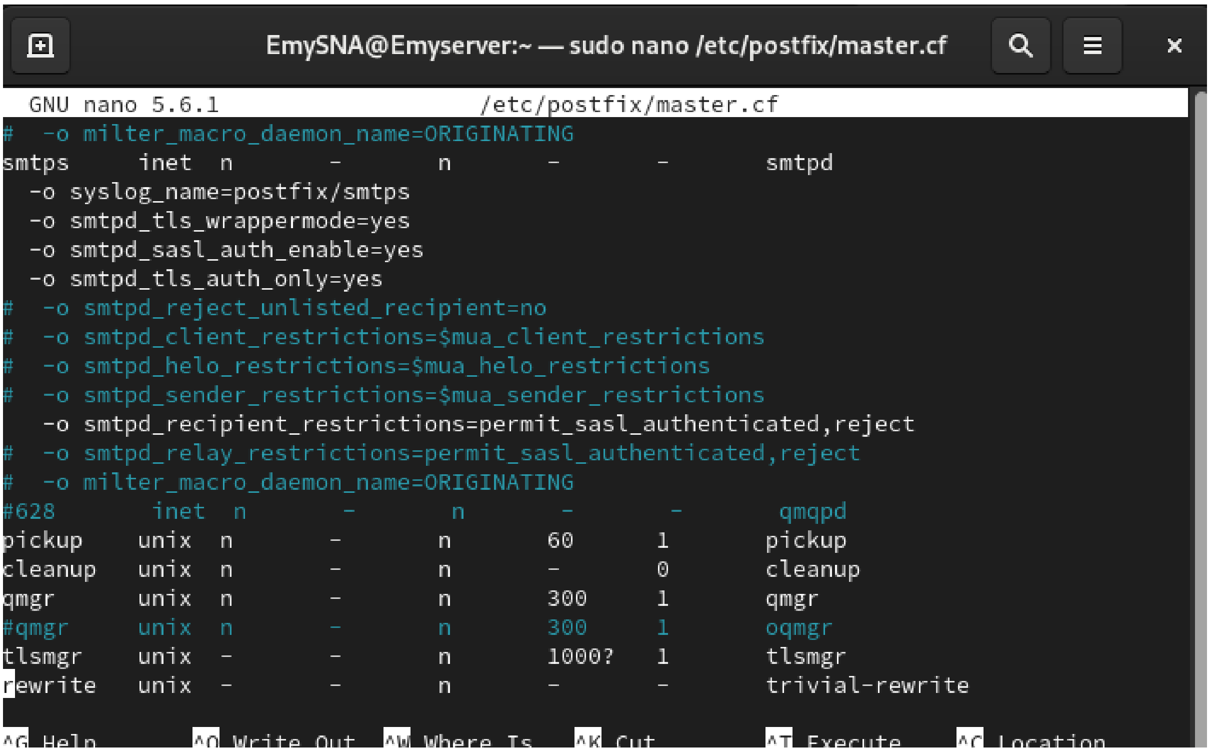
Troubleshooting, issue 1:

First open master.cf file:



```
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/master.cf
[sudo] password for EmySNA:
```

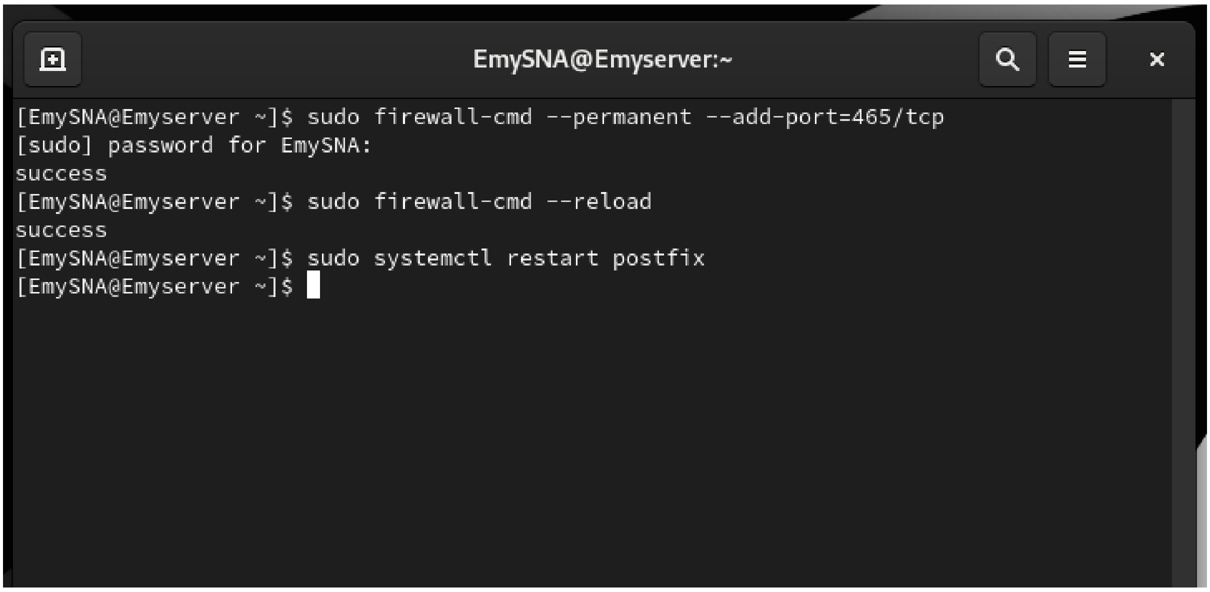
Uncomment/add the following lines:



```
  GNU nano 5.6.1                    /etc/postfix/master.cf
#   -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       n       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=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
   -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#   -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#   -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       n       -       -       qmqpd
pickup    unix  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
```

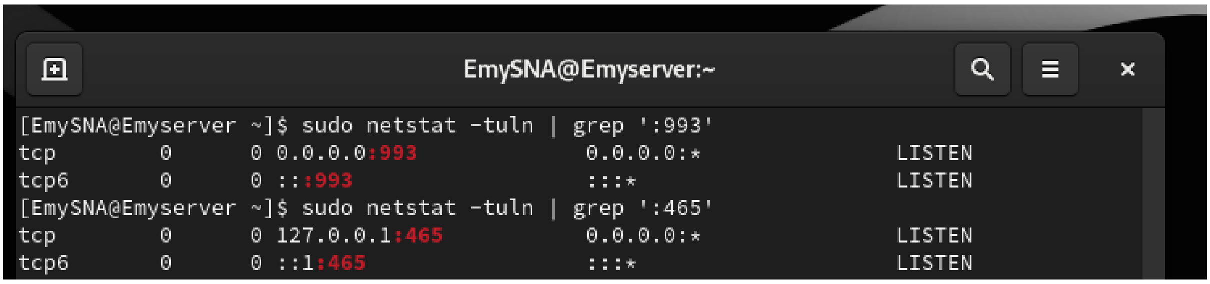
Uncommenting the first 4 lines in the picture to allow SMTP server to listen for encrypted connections on port 465 (SMTPS) over SSL/TLS to ensure secure communication between server and clients

then added “-o smtpd_tls_auth_only=yes” to make postfix use TLS for authentication and “permit_sasl_authenticated” after “-o smtpd_recipient_restrictions=” to enable only authenticated users can send emails through the postfix server we then configure the firewall to allow secure traffic (SMTP/SMTPS) which sends and receives mail over SSL/TLS, make it permanent then reload it to apply changes and restart it to apply new settings:

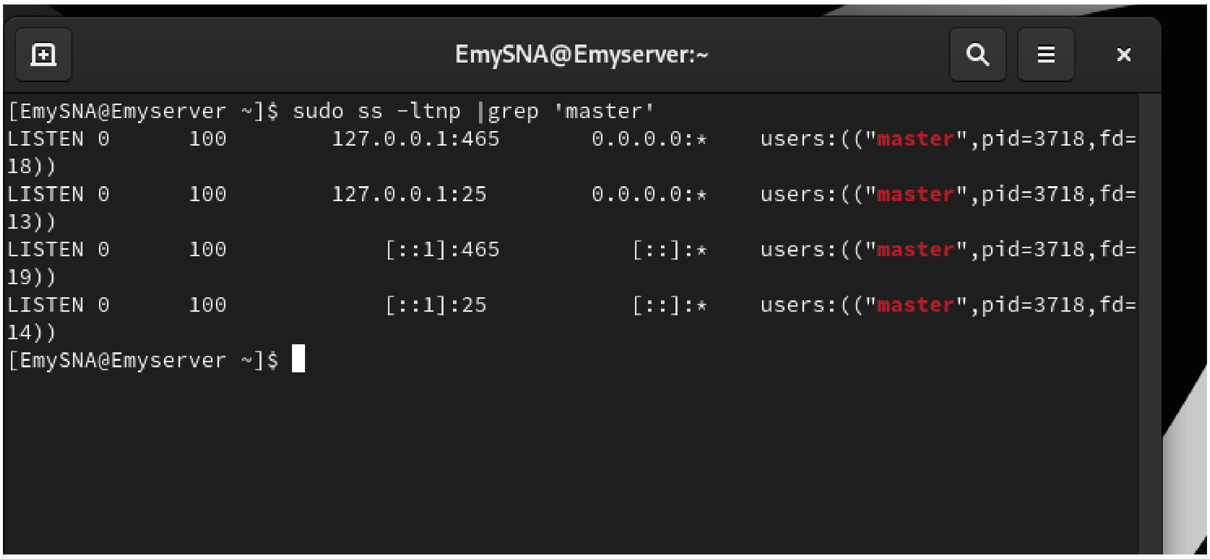


```
[EmySNA@Emyserver ~]$ sudo firewall-cmd --permanent --add-port=465/tcp
[sudo] password for EmySNA:
success
[EmySNA@Emyserver ~]$ sudo firewall-cmd --reload
success
[EmySNA@Emyserver ~]$ sudo systemctl restart postfix
[EmySNA@Emyserver ~]$
```

Ensure all ports are waiting for a connection and listening:

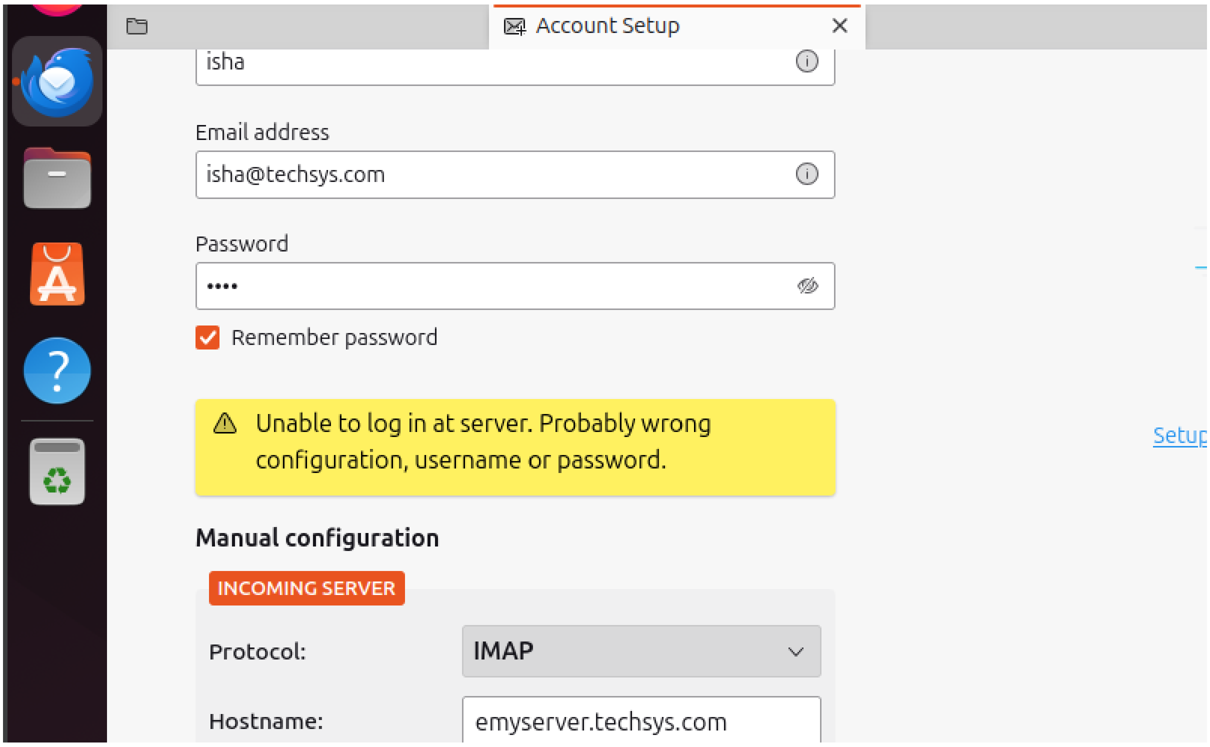


```
[EmySNA@Emyserver ~]$ sudo netstat -tuln | grep ':993'
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp6       0      0 :::993                  :::*                    LISTEN
[EmySNA@Emyserver ~]$ sudo netstat -tuln | grep ':465'
tcp        0      0 127.0.0.1:465           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:465                 :::*                    LISTEN
```



```
[EmySNA@Emyserver ~]$ sudo ss -ltnp |grep 'master'
LISTEN 0      100         127.0.0.1:465       0.0.0.0:*    users:(("master",pid=3718,fd=
18))
LISTEN 0      100         127.0.0.1:25        0.0.0.0:*    users:(("master",pid=3718,fd=
13))
LISTEN 0      100             [::1]:465          [::]:*    users:(("master",pid=3718,fd=
19))
LISTEN 0      100             [::1]:25           [::]:*    users:(("master",pid=3718,fd=
14))
[EmySNA@Emyserver ~]$ 
```

As the port listen to local host “127” I must check what’s binding it, as keeping it binded will make my thunderbird unable to properly connect with the mail server like this, so I must back track to fix it



isha

Email address
isha@techsys.com

Password
••••

☑ Remember password

⚠ Unable to log in at server. Probably wrong configuration, username or password.

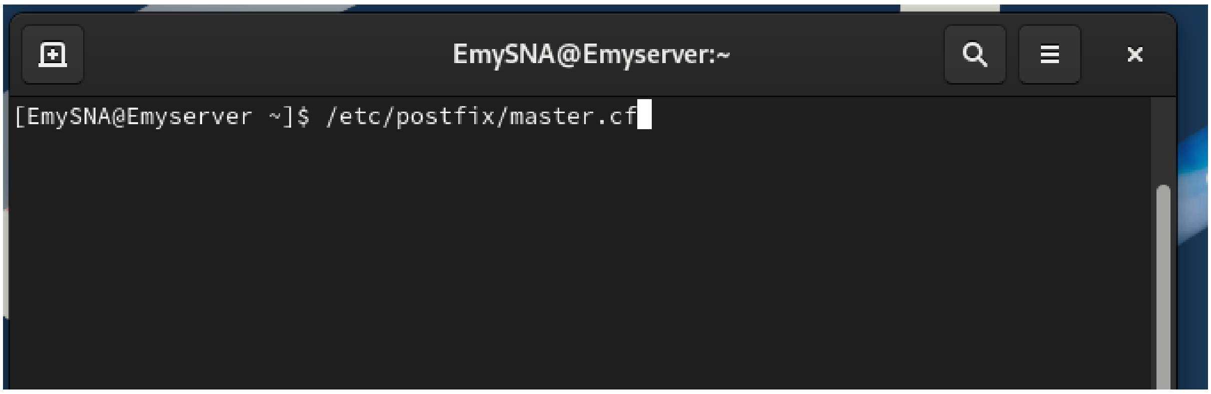
Manual configuration

INCOMING SERVER

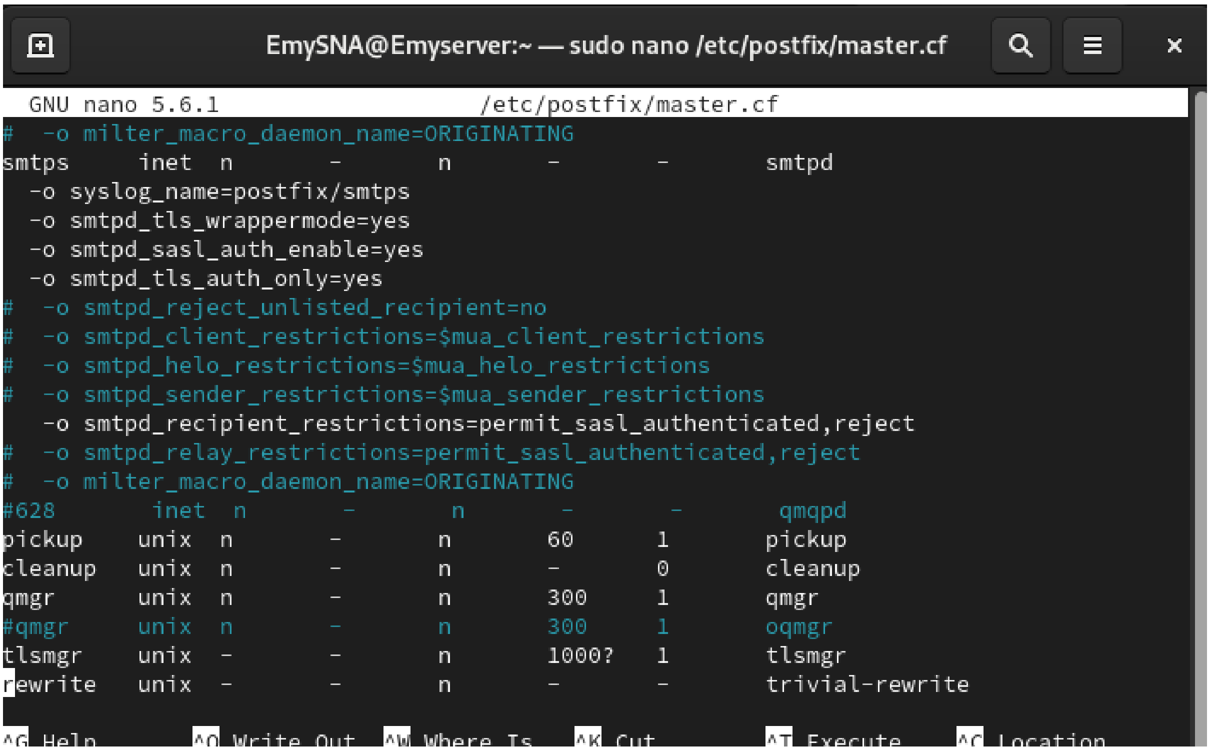
Protocol: IMAP

Hostname: emyserver.techsys.com

“/etc/postfic/master.cf” is checked and nothing is binding postfix to localhost or directly “127.0.0.1” :

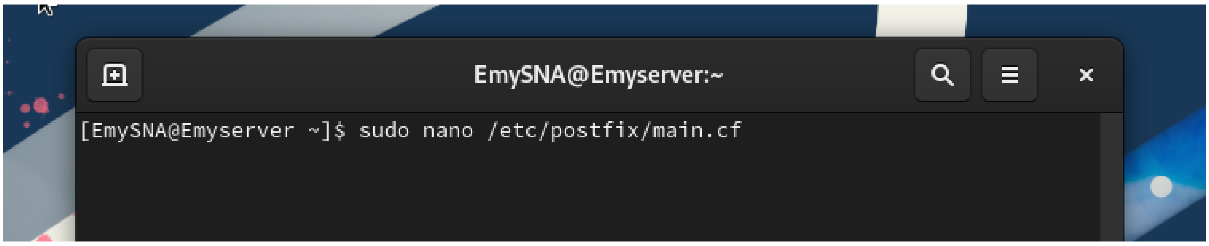


```
[EmySNA@Emyserver ~]$ /etc/postfix/master.cf
```

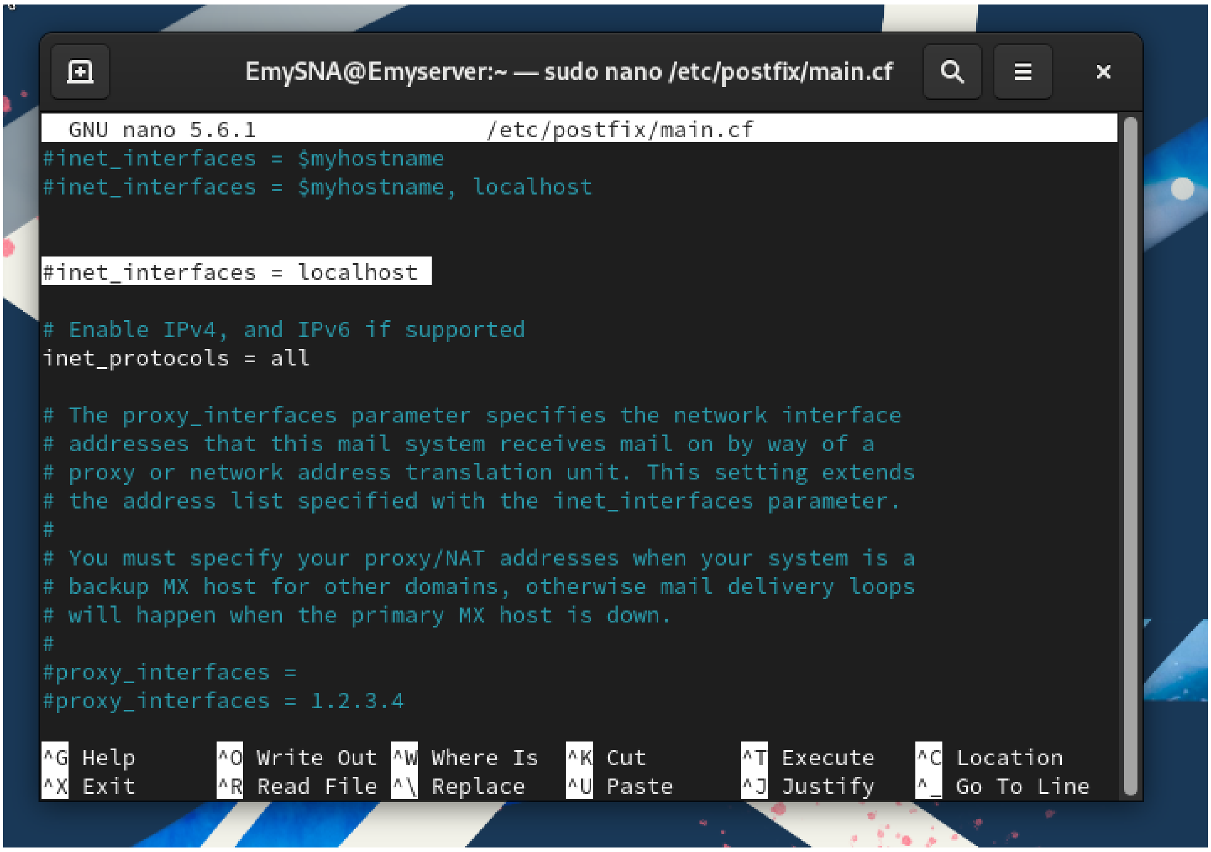


```
  GNU nano 5.6.1                   /etc/postfix/master.cf
#  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       n       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
   -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       n       -       -       qmqpd
pickup    unix  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
```

So next we check “main.cf” :



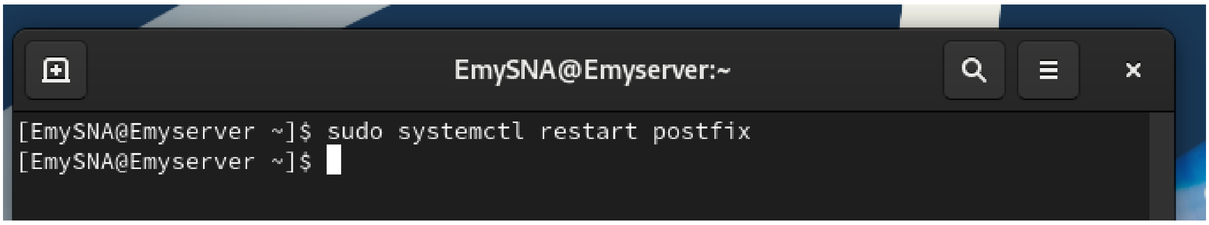
```
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/main.cf
```



```
  GNU nano 5.6.1                 /etc/postfix/main.cf
#inet_interfaces = $myhostname
#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.
#
#proxy_interfaces =
#proxy_interfaces = 1.2.3.4
```

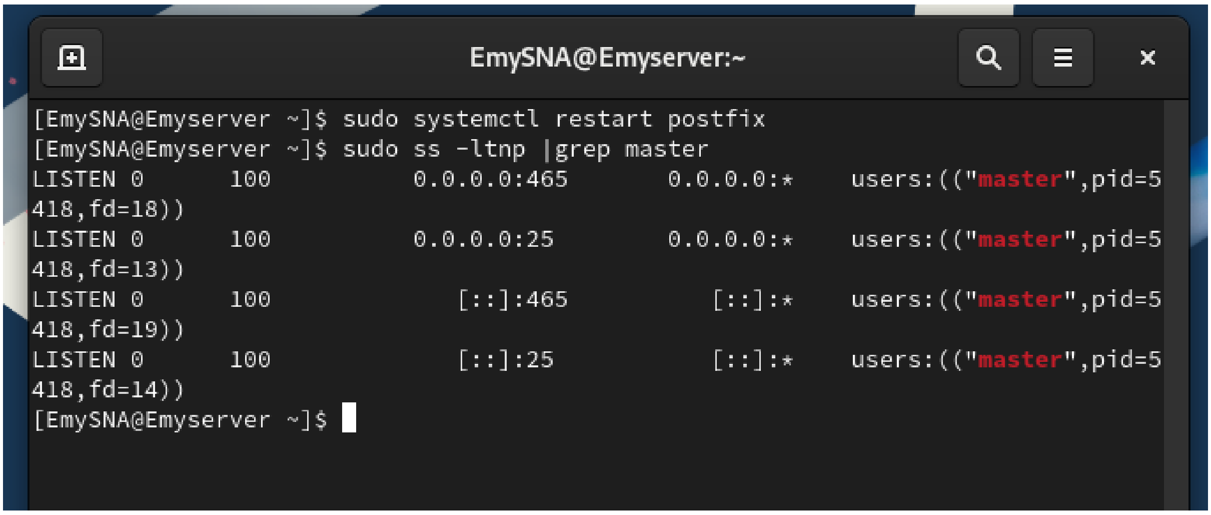
“inet_interfaces = localhost” was uncommented so we comment it un-bind it from port from listening to local host only.

Then we save the new buffer before restarting postfix to activate new settings:



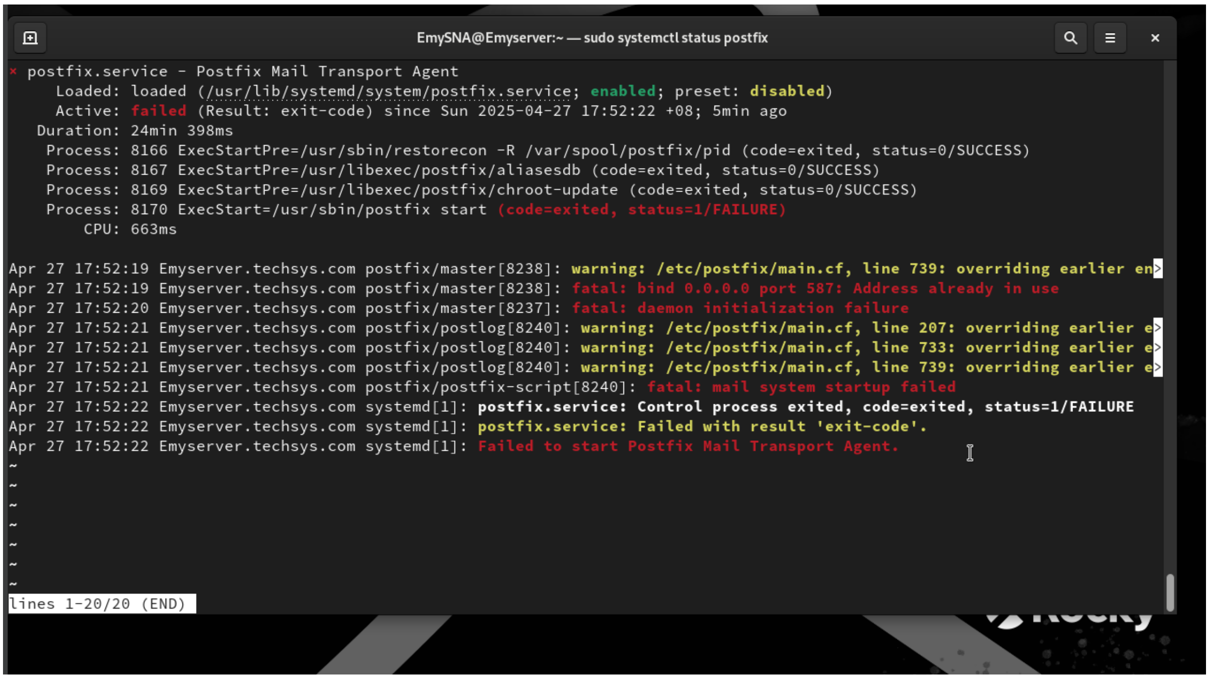
```
[EmySNA@Emyserver ~]$ sudo systemctl restart postfix
[EmySNA@Emyserver ~]$ 
```

checked again and surely now it’s accepting both public and private Ips:



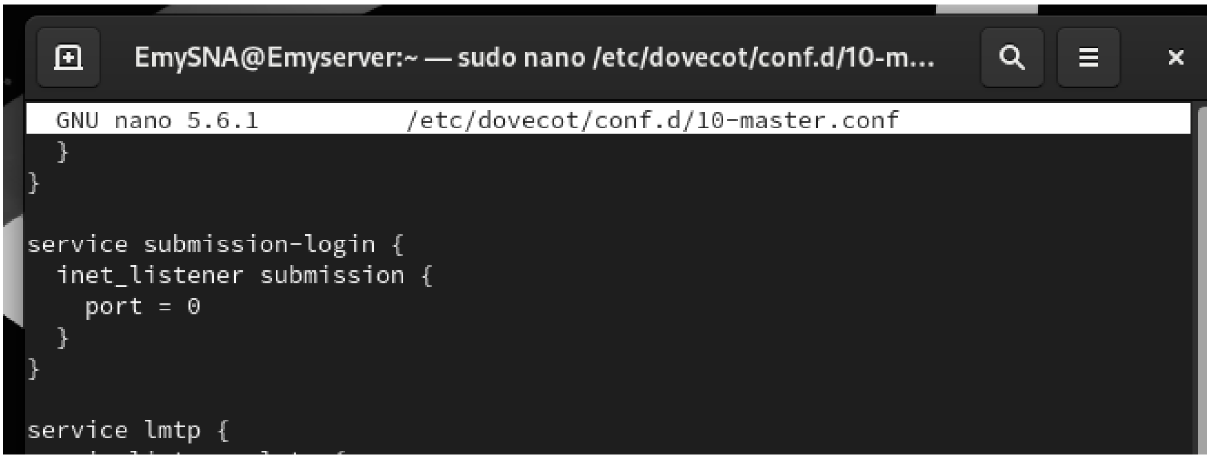
```
[EmySNA@Emyserver ~]$ sudo systemctl restart postfix
[EmySNA@Emyserver ~]$ sudo ss -ltnp |grep master
LISTEN 0      100          0.0.0.0:465        0.0.0.0:*    users:(("master",pid=5
418,fd=18))
LISTEN 0      100          0.0.0.0:25         0.0.0.0:*    users:(("master",pid=5
418,fd=13))
LISTEN 0      100             [::]:465           [::]:*    users:(("master",pid=5
418,fd=19))
LISTEN 0      100             [::]:25            [::]:*    users:(("master",pid=5
418,fd=14))
[EmySNA@Emyserver ~]$ 
```

However, I couldn’t restart postfix earlier after some of the modifications



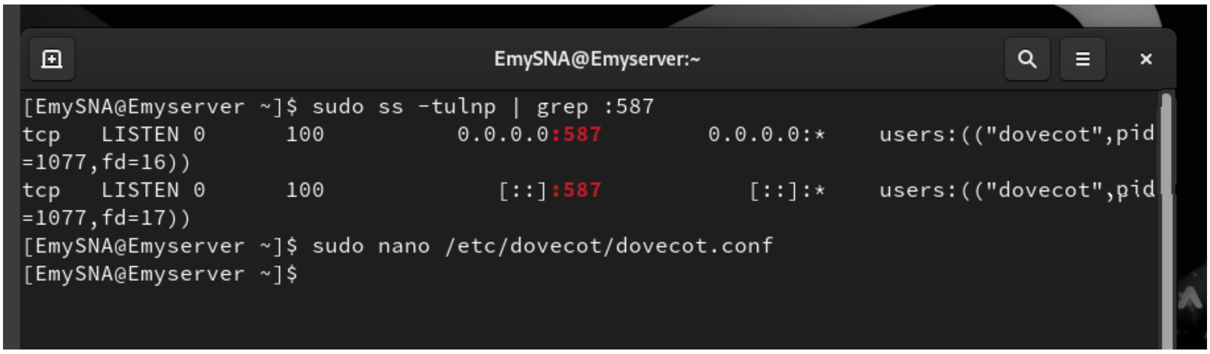
```
× postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; preset: disabled)
     Active: failed (Result: exit-code) since Sun 2025-04-27 17:52:22 +08; 5min ago
   Duration: 24min 398ms
    Process: 8166 ExecStartPre=/usr/sbin/restorecon -R /var/spool/postfix/pid (code=exited, status=0/SUCCESS)
    Process: 8167 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)
    Process: 8169 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)
    Process: 8170 ExecStart=/usr/sbin/postfix start (code=exited, status=1/FAILURE)
        CPU: 663ms

Apr 27 17:52:19 Emyserver.techsys.com postfix/master[8238]: warning: /etc/postfix/main.cf, line 739: overriding earlier en>
Apr 27 17:52:19 Emyserver.techsys.com postfix/master[8238]: fatal: bind 0.0.0.0 port 587: Address already in use
Apr 27 17:52:20 Emyserver.techsys.com postfix/master[8237]: fatal: daemon initialization failure
Apr 27 17:52:21 Emyserver.techsys.com postfix/postlog[8240]: warning: /etc/postfix/main.cf, line 207: overriding earlier e>
Apr 27 17:52:21 Emyserver.techsys.com postfix/postlog[8240]: warning: /etc/postfix/main.cf, line 733: overriding earlier e>
Apr 27 17:52:21 Emyserver.techsys.com postfix/postlog[8240]: warning: /etc/postfix/main.cf, line 739: overriding earlier e>
Apr 27 17:52:21 Emyserver.techsys.com postfix/postfix-script[8240]: fatal: mail system startup failed
Apr 27 17:52:22 Emyserver.techsys.com systemd[1]: postfix.service: Control process exited, code=exited, status=1/FAILURE
Apr 27 17:52:22 Emyserver.techsys.com systemd[1]: postfix.service: Failed with result 'exit-code'.
Apr 27 17:52:22 Emyserver.techsys.com systemd[1]: Failed to start Postfix Mail Transport Agent.
~
~
~
~
~
~
~
lines 1-20/20 (END)
```

The problem was that postfix can’t bind to port 587 because dovecot already took it, so to disable dovecot listening on 587 I opened “10-master.conf” file and change the “port = 587” to 0:



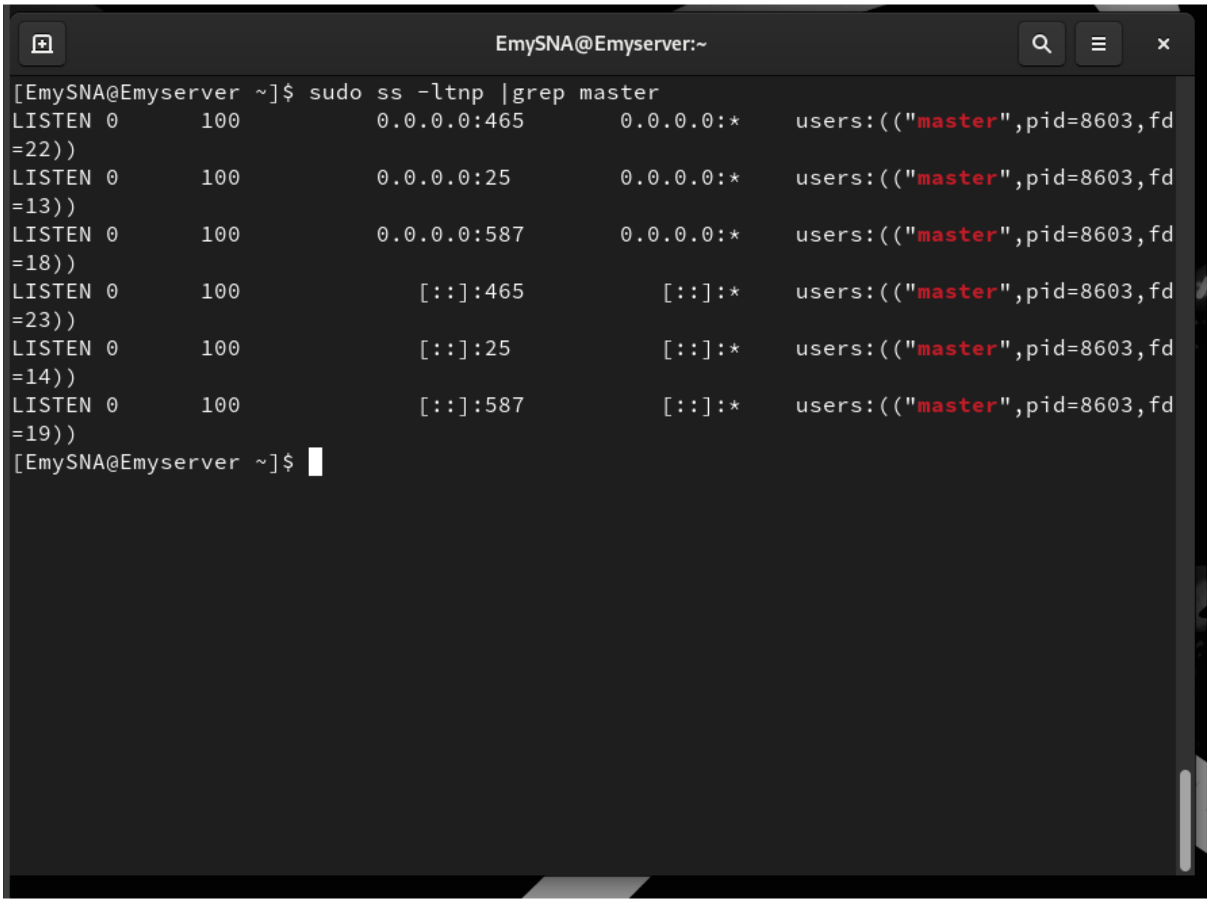
```
  GNU nano 5.6.1              /etc/dovecot/conf.d/10-master.conf
  }
}

service submission-login {
  inet_listener submission {
    port = 0
  }
}

service lmtp {
```

Then restart dovecot and check who’s using it:

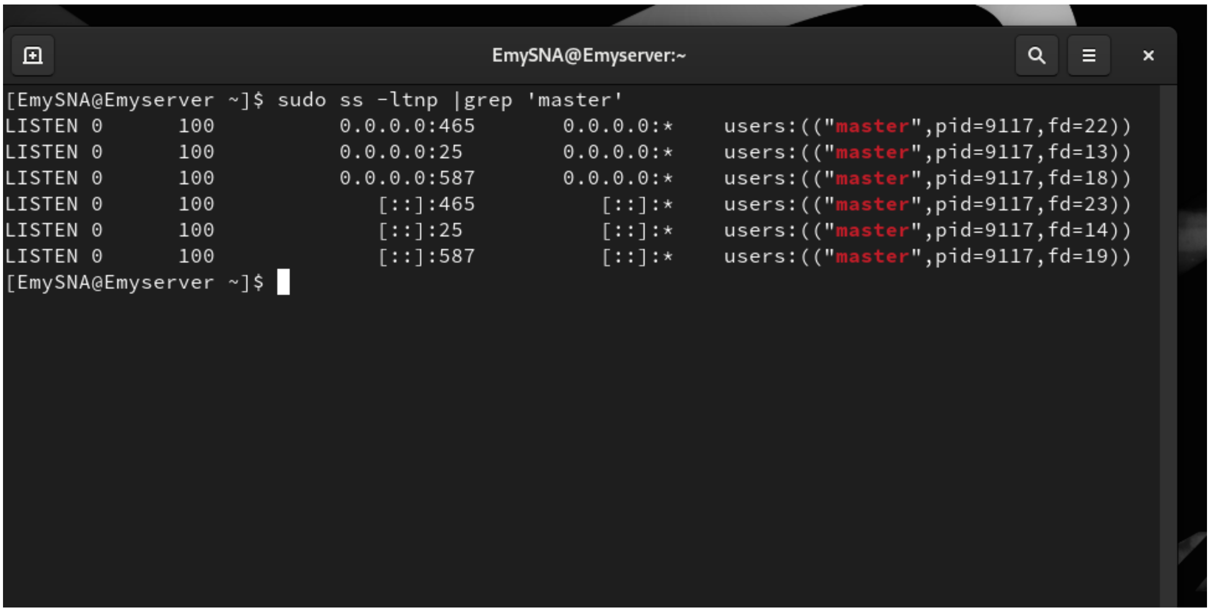


```
[EmySNA@Emyserver ~]$ sudo ss -tulnp | grep :587
tcp   LISTEN 0      100          0.0.0.0:587        0.0.0.0:*    users:(("dovecot",pid
=1077,fd=16))
tcp   LISTEN 0      100             [::]:587           [::]:*    users:(("dovecot",pid
=1077,fd=17))
[EmySNA@Emyserver ~]$ sudo nano /etc/dovecot/dovecot.conf
[EmySNA@Emyserver ~]$
```

And check the rest just to as a safe measure:

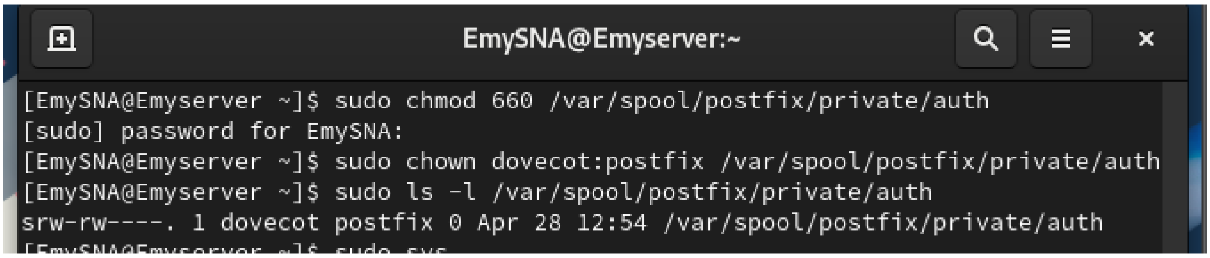


```
[EmySNA@Emyserver ~]$ sudo ss -ltnp |grep master
LISTEN 0      100          0.0.0.0:465        0.0.0.0:*    users:(("master",pid=8603,fd
=22))
LISTEN 0      100          0.0.0.0:25         0.0.0.0:*    users:(("master",pid=8603,fd
=13))
LISTEN 0      100          0.0.0.0:587        0.0.0.0:*    users:(("master",pid=8603,fd
=18))
LISTEN 0      100             [::]:465           [::]:*    users:(("master",pid=8603,fd
=23))
LISTEN 0      100             [::]:25            [::]:*    users:(("master",pid=8603,fd
=14))
LISTEN 0      100             [::]:587           [::]:*    users:(("master",pid=8603,fd
=19))
[EmySNA@Emyserver ~]$
```



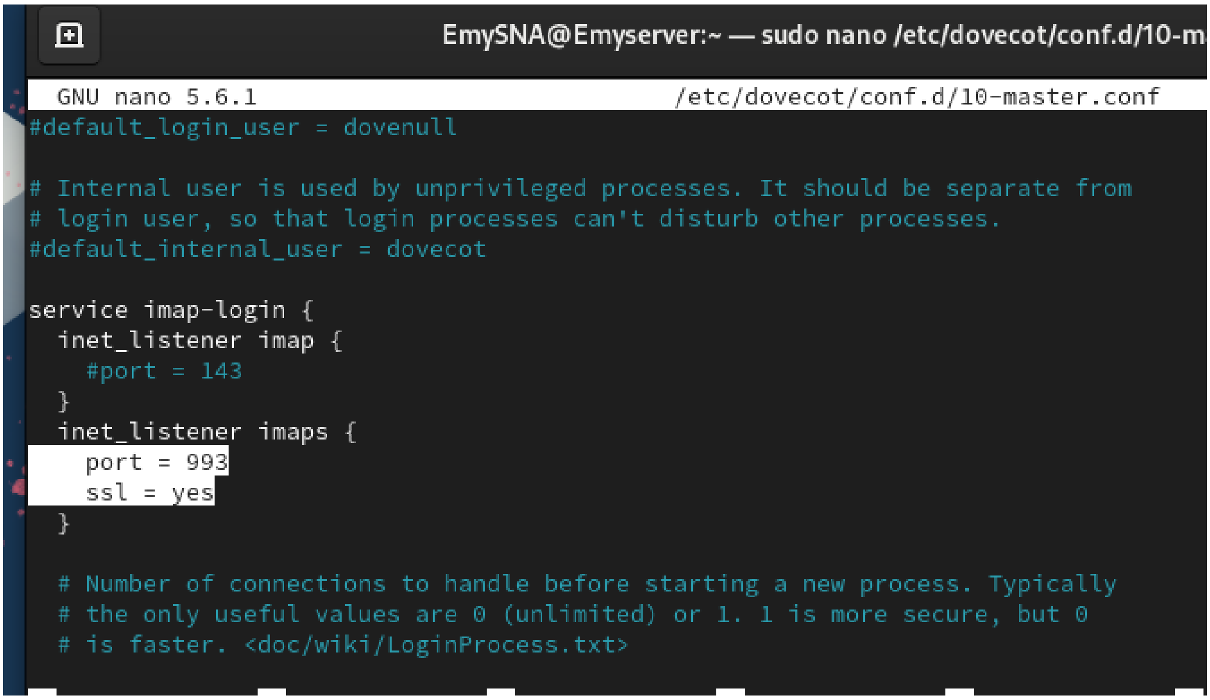
```
[EmySNA@Emyserver ~]$ sudo ss -ltnp |grep 'master'
LISTEN 0      100          0.0.0.0:465        0.0.0.0:*    users:(("master",pid=9117,fd=22))
LISTEN 0      100          0.0.0.0:25         0.0.0.0:*    users:(("master",pid=9117,fd=13))
LISTEN 0      100          0.0.0.0:587        0.0.0.0:*    users:(("master",pid=9117,fd=18))
LISTEN 0      100             [::]:465           [::]:*    users:(("master",pid=9117,fd=23))
LISTEN 0      100             [::]:25            [::]:*    users:(("master",pid=9117,fd=14))
LISTEN 0      100             [::]:587           [::]:*    users:(("master",pid=9117,fd=19))
[EmySNA@Emyserver ~]$ 
```

After trying to log in again the issue persisted so auth socket in dovecot permissions are changed so only the owner (dovecot) and group(postfix) can read and write it to communicate and verify the usernames and passwords (SASL auth), then change ownership of socket to dovecot since it created and group to postfix so it can access it to allow authenticated user sending mails:



```
[EmySNA@Emyserver ~]$ sudo chmod 660 /var/spool/postfix/private/auth
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo chown dovecot:postfix /var/spool/postfix/private/auth
[EmySNA@Emyserver ~]$ sudo ls -l /var/spool/postfix/private/auth
srw-rw----. 1 dovecot postfix 0 Apr 28 12:54 /var/spool/postfix/private/auth
[EmySNA@Emyserver ~]$ sudo sys
```

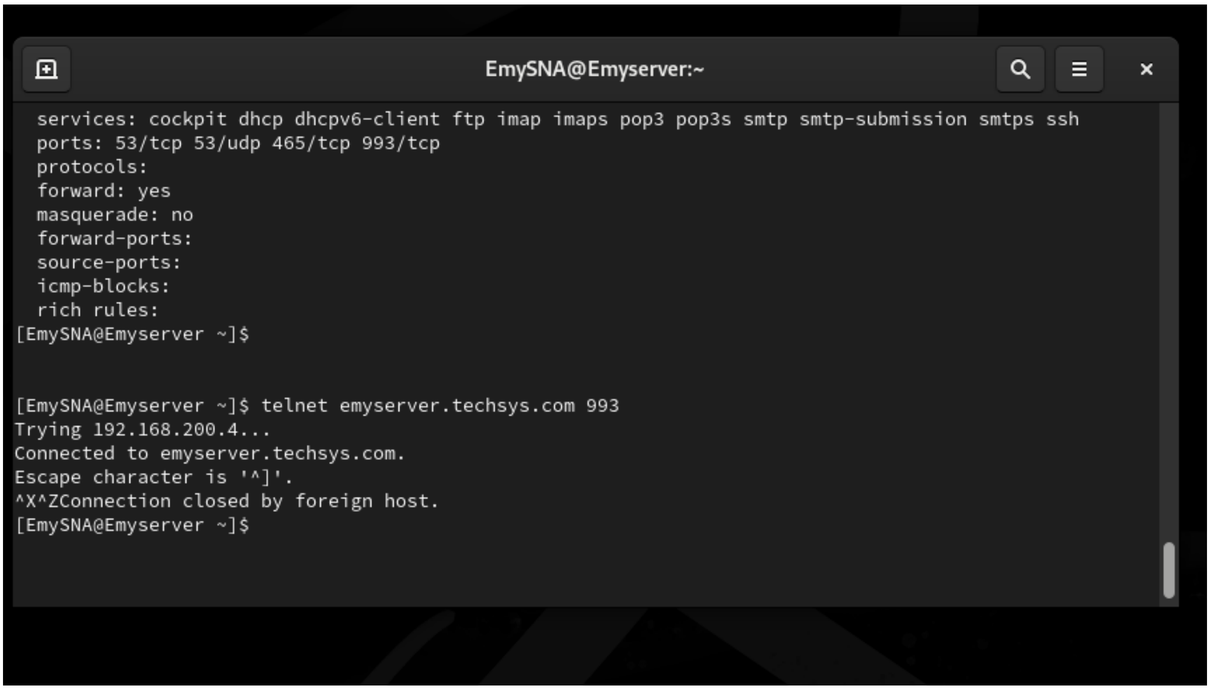
Uncomment the following two lines to enable dovecot to listen on port 993 for encrypted IMAPS for secure email retrieval to enable clients to securely receive their mail over SSL/TLS



```
  GNU nano 5.6.1                              /etc/dovecot/conf.d/10-master.conf
#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
  # is faster. <doc/wiki/LoginProcess.txt>
```

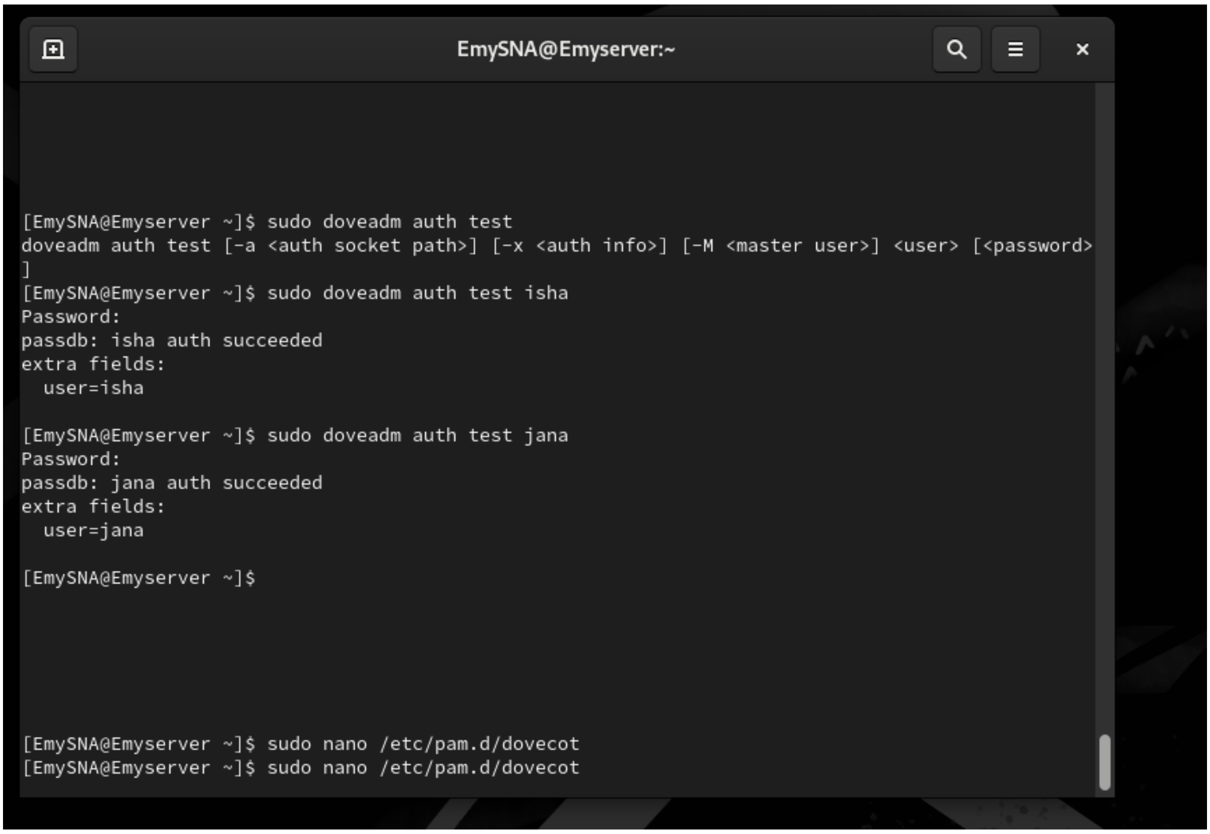
Then run “sudo firewall-cmd --list-all” to view all current firewall setting to check ports like 993 and 465 aren’t blocked.

After that I tried to connect to port 993 using Telnet to test if IMAPS port is reachable and dovecot is listening, not being blocked by the firewall

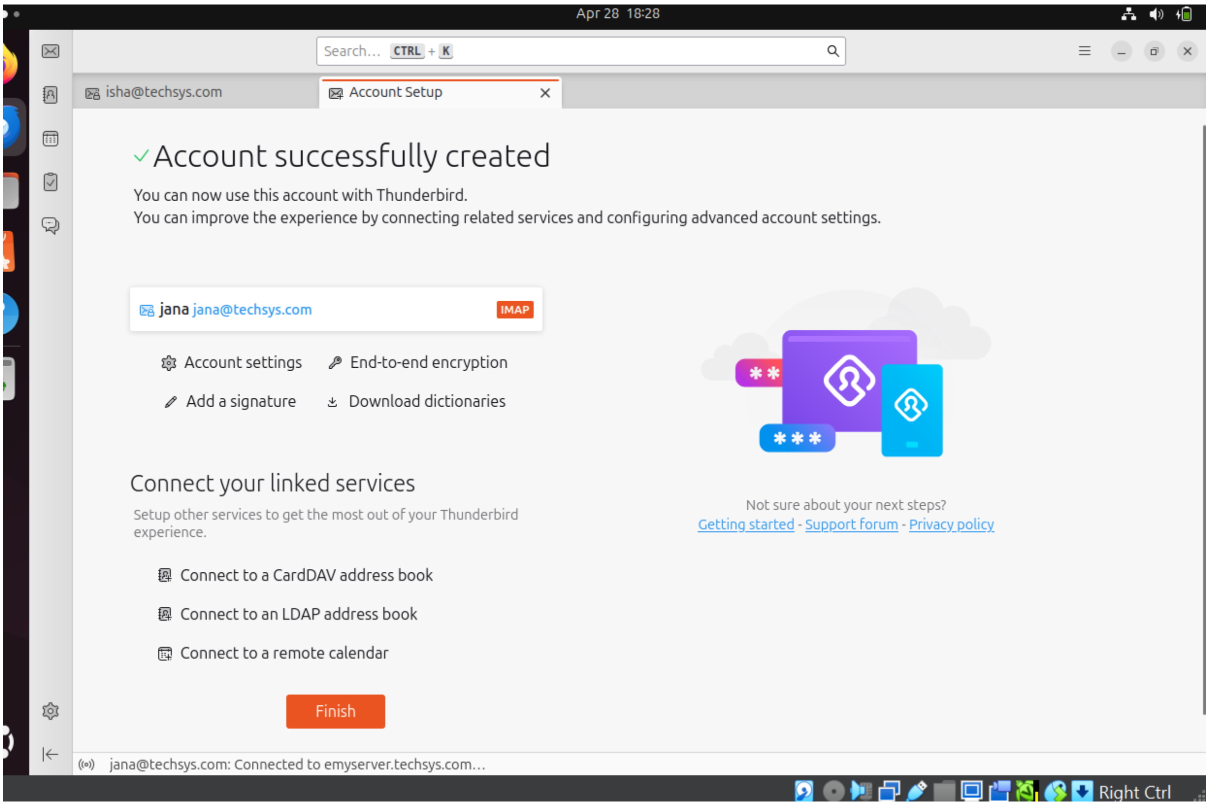


```
  services: cockpit dhcp dhcpv6-client ftp imap imaps pop3 pop3s smtp smtp-submission smtps ssh
  ports: 53/tcp 53/udp 465/tcp 993/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[EmySNA@Emyserver ~]$


[EmySNA@Emyserver ~]$ telnet emyserver.techsys.com 993
Trying 192.168.200.4...
Connected to emyserver.techsys.com.
Escape character is '^]'.
^X^ZConnection closed by foreign host.
[EmySNA@Emyserver ~]$
```

Final to ensure that users can log in, dovecot’s own auth system is used to test it to make sure authentication is working before trying from the actual mail client:



```
[EmySNA@Emyserver ~]$ sudo doveadm auth test
doveadm auth test [-a <auth socket path>] [-x <auth info>] [-M <master user>] <user> [<password>
]
[EmySNA@Emyserver ~]$ sudo doveadm auth test isha
Password:
passdb: isha auth succeeded
extra fields:
  user=isha

[EmySNA@Emyserver ~]$ sudo doveadm auth test jana
Password:
passdb: jana auth succeeded
extra fields:
  user=jana

[EmySNA@Emyserver ~]$





[EmySNA@Emyserver ~]$ sudo nano /etc/pam.d/dovecot
[EmySNA@Emyserver ~]$ sudo nano /etc/pam.d/dovecot
```



Apr 28 18:28
Search… CTRL + K
isha@techsys.com
Account Setup

✓ 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.

jana jana@techsys.com IMAP

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.

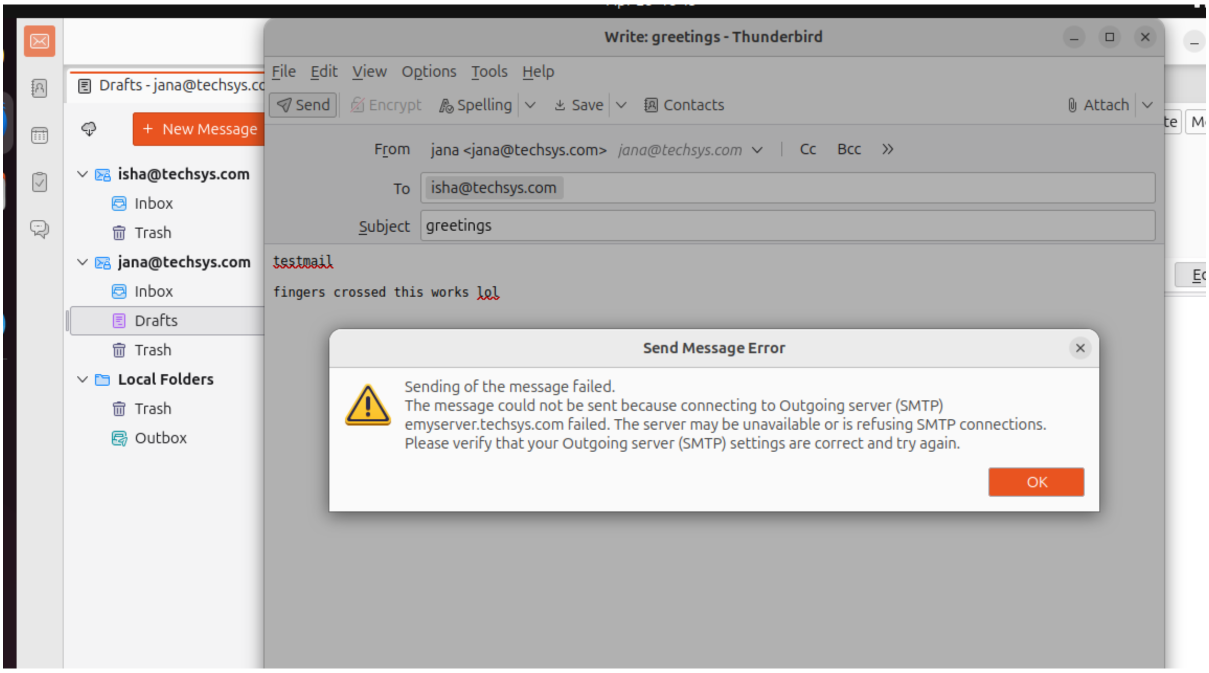
Connect to a CardDAV address book
Connect to an LDAP address book
Connect to a remote calendar
Finish
Not sure about your next steps?
Getting started - Support forum - Privacy policy
Right Ctrl

jana@techsys.com: Connected to emyserver.techsys.com…

Which enabled me to log in and connect to the server.

Troubleshooting, issue 2:

The next problem I had to troubleshoot is that the client was unable to send emails because connecting to my outgoing server (SMTP) failed.



From jana <jana@techsys.com> jana@techsys.com

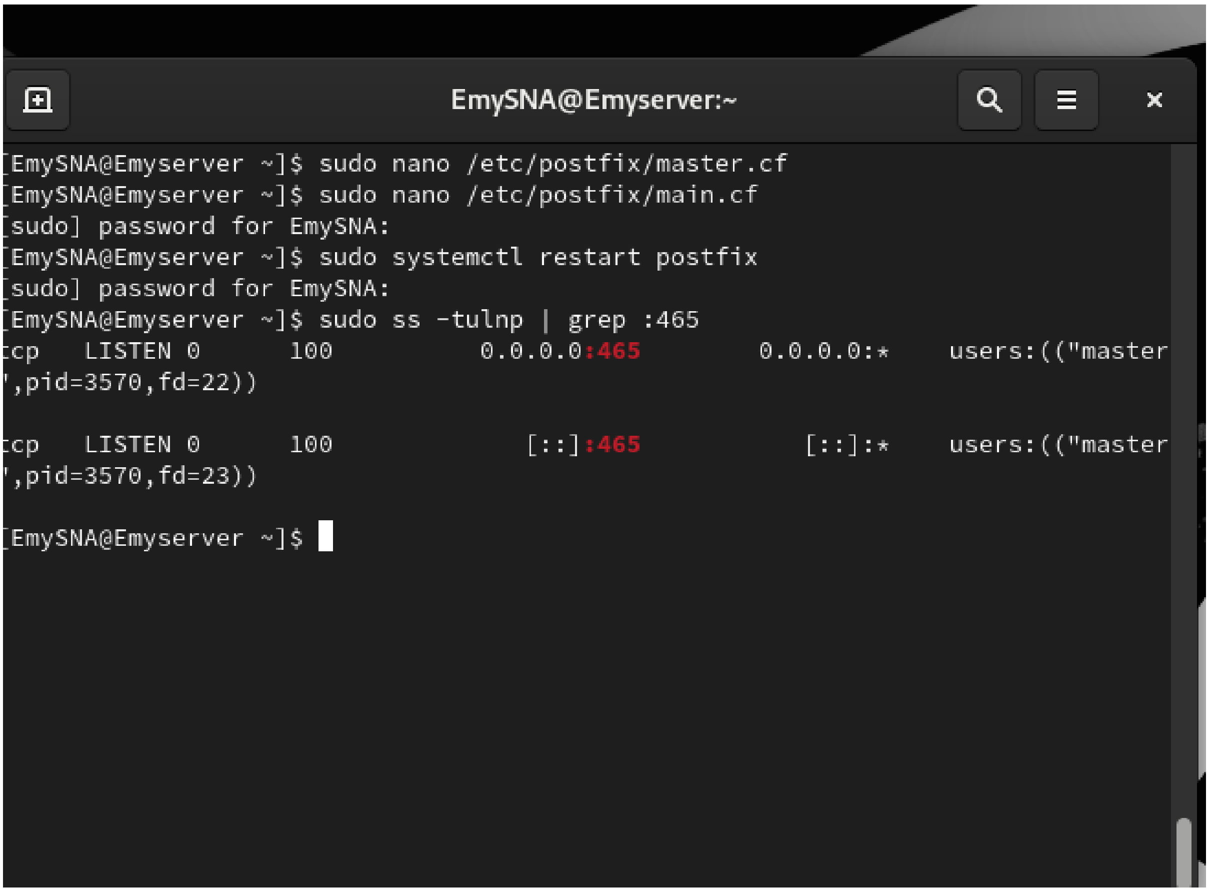
To isha@techsys.com

Subject greetings

```
testmail
fingers crossed this works lol
```

Sending of the message failed.
The message could not be sent because connecting to Outgoing server (SMTP) emyserver.techsys.com failed. The server may be unavailable or is refusing SMTP connections. Please verify that your Outgoing server (SMTP) settings are correct and try again.

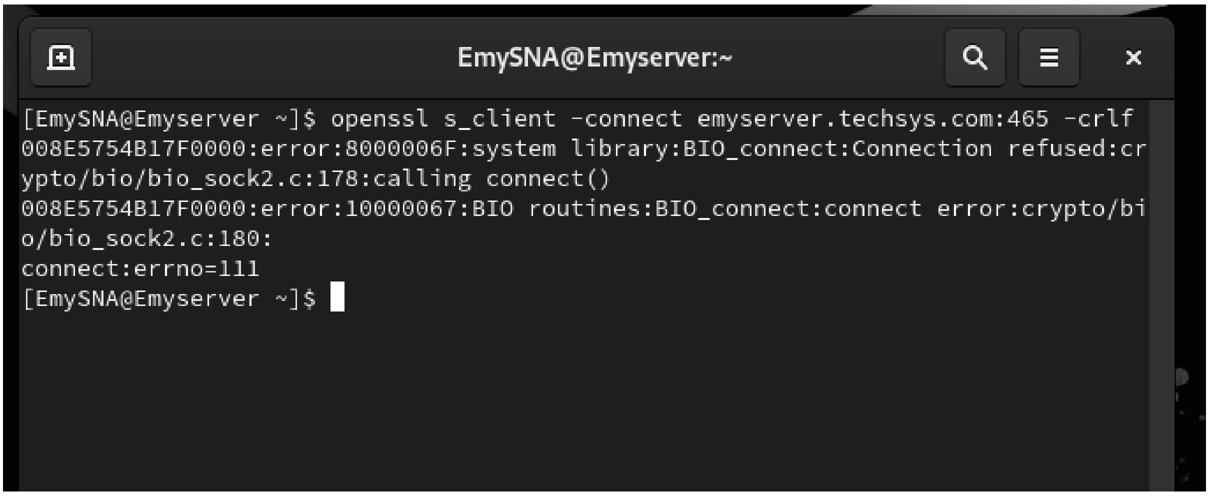
I double checked the "/etc/postfix/main.cf" to double-check configuration is correct with typos and it was I then double-checked postfix ports connection, and it wasn't set to accept only Rocky's local hosts as it previously was



```
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/master.cf
[EmySNA@Emyserver ~]$ sudo nano /etc/postfix/main.cf
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo systemctl restart postfix
[sudo] password for EmySNA:
[EmySNA@Emyserver ~]$ sudo ss -tulnp | grep :465
tcp   LISTEN 0      100          0.0.0.0:465        0.0.0.0:*    users:(("master
",pid=3570,fd=22))

tcp   LISTEN 0      100             [::]:465           [::]:*    users:(("master
",pid=3570,fd=23))

[EmySNA@Emyserver ~]$ 
```

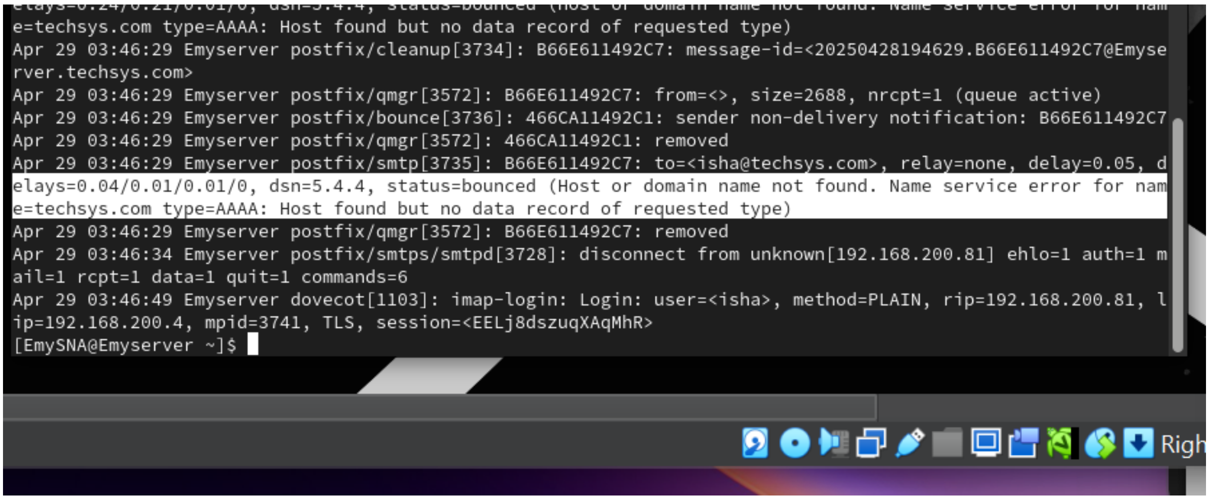
So, I ran “openssl s_client -connect emyserver.techsys.com:465 -crlf” to connect the mail server on port 465 using SSL/TLS to test SMTP commands.

The



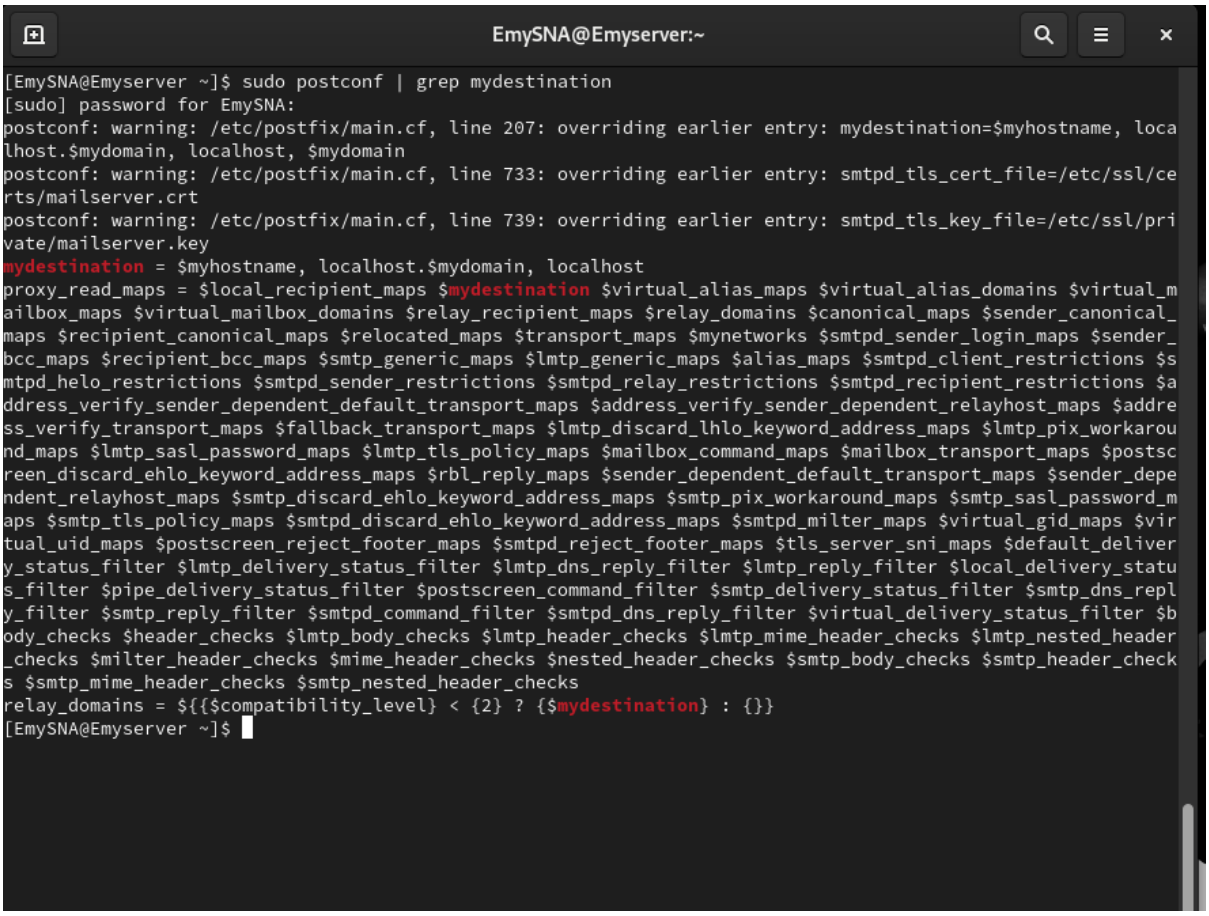
```
[EmySNA@Emyserver ~]$ openssl s_client -connect emyserver.techsys.com:465 -crlf
008E5754B17F0000:error:8000006F:system library:BIO_connect:Connection refused:cr
ypto/bio/bio_sock2.c:178:calling connect()
008E5754B17F0000:error:10000067:BIO routines:BIO_connect:connect error:crypto/bi
o/bio_sock2.c:180:
connect:errno=111
[EmySNA@Emyserver ~]$ 
```

The error shows the “status=bounced” which means it was sent but couldn’t be delivered/received and sent back to sender :



```
elays=0.24/0.21/0.01/0, dsn=5.4.4, status=bounced (Host or domain name not found. Name service error for nam
e=techsys.com type=AAAA: Host found but no data record of requested type)
Apr 29 03:46:29 Emyserver postfix/cleanup[3734]: B66E611492C7: message-id=<20250428194629.B66E611492C7@Emyse
rver.techsys.com>
Apr 29 03:46:29 Emyserver postfix/qmgr[3572]: B66E611492C7: from=<>, size=2688, nrcpt=1 (queue active)
Apr 29 03:46:29 Emyserver postfix/bounce[3736]: 466CA11492C1: sender non-delivery notification: B66E611492C7
Apr 29 03:46:29 Emyserver postfix/qmgr[3572]: 466CA11492C1: removed
Apr 29 03:46:29 Emyserver postfix/smtp[3735]: B66E611492C7: to=<isha@techsys.com>, relay=none, delay=0.05, d
elays=0.04/0.01/0.01/0, dsn=5.4.4, status=bounced (Host or domain name not found. Name service error for nam
e=techsys.com type=AAAA: Host found but no data record of requested type)
Apr 29 03:46:29 Emyserver postfix/qmgr[3572]: B66E611492C7: removed
Apr 29 03:46:34 Emyserver postfix/smtps/smtpd[3728]: disconnect from unknown[192.168.200.81] ehlo=1 auth=1 m
ail=1 rcpt=1 data=1 quit=1 commands=6
Apr 29 03:46:49 Emyserver dovecot[1103]: imap-login: Login: user=<isha>, method=PLAIN, rip=192.168.200.81, l
ip=192.168.200.4, mpid=3741, TLS, session=<EELj8dszuqXAqMhR>
[EmySNA@Emyserver ~]$
```

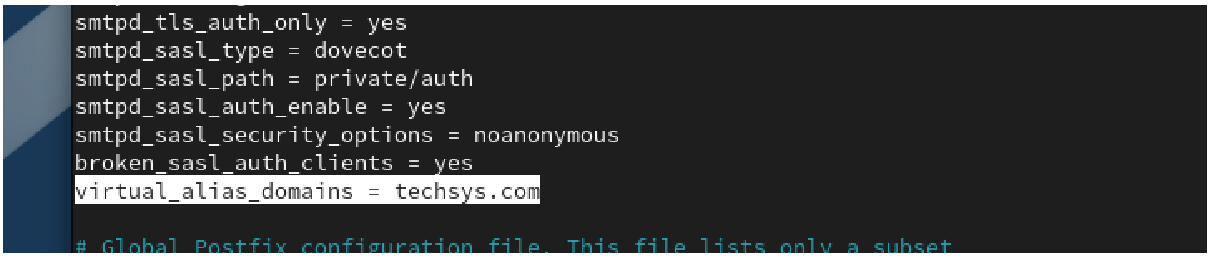
Then I ran “sudo postconf | grep mydestination” to check “mydestination” values to ensure the server identifies the proper domains that should receive the mail:



```
[EmySNA@Emyserver ~]$ sudo postconf | grep mydestination
[sudo] password for EmySNA:
postconf: warning: /etc/postfix/main.cf, line 207: overriding earlier entry: mydestination=$myhostname, loca
lhost.$mydomain, localhost, $mydomain
postconf: warning: /etc/postfix/main.cf, line 733: overriding earlier entry: smtpd_tls_cert_file=/etc/ssl/ce
rts/mailserver.crt
postconf: warning: /etc/postfix/main.cf, line 739: overriding earlier entry: smtpd_tls_key_file=/etc/ssl/pri
vate/mailserver.key
mydestination = $myhostname, localhost.$mydomain, localhost
proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_maps $virtual_alias_domains $virtual_m
ailbox_maps $virtual_mailbox_domains $relay_recipient_maps $relay_domains $canonical_maps $sender_canonical_
maps $recipient_canonical_maps $relocated_maps $transport_maps $mynetworks $smtpd_sender_login_maps $sender_
bcc_maps $recipient_bcc_maps $smtp_generic_maps $lmtp_generic_maps $alias_maps $smtpd_client_restrictions $s
mtpd_helo_restrictions $smtpd_sender_restrictions $smtpd_relay_restrictions $smtpd_recipient_restrictions $a
ddress_verify_sender_dependent_default_transport_maps $address_verify_sender_dependent_relayhost_maps $addre
ss_verify_transport_maps $fallback_transport_maps $lmtp_discard_lhlo_keyword_address_maps $lmtp_pix_workarou
nd_maps $lmtp_sasl_password_maps $lmtp_tls_policy_maps $mailbox_command_maps $mailbox_transport_maps $postsc
reen_discard_ehlo_keyword_address_maps $rbl_reply_maps $sender_dependent_default_transport_maps $sender_depe
ndent_relayhost_maps $smtp_discard_ehlo_keyword_address_maps $smtp_pix_workaround_maps $smtp_sasl_password_m
aps $smtp_tls_policy_maps $smtpd_discard_ehlo_keyword_address_maps $smtpd_milter_maps $virtual_gid_maps $vir
tual_uid_maps $postscreen_reject_footer_maps $smtpd_reject_footer_maps $tls_server_sni_maps $default_deliver
y_status_filter $lmtp_delivery_status_filter $lmtp_dns_reply_filter $lmtp_reply_filter $local_delivery_statu
s_filter $pipe_delivery_status_filter $postscreen_command_filter $smtp_delivery_status_filter $smtp_dns_repl
y_filter $smtp_reply_filter $smtpd_command_filter $smtpd_dns_reply_filter $virtual_delivery_status_filter $b
ody_checks $header_checks $lmtp_body_checks $lmtp_header_checks $lmtp_mime_header_checks $lmtp_nested_header
_checks $milter_header_checks $mime_header_checks $nested_header_checks $smtp_body_checks $smtp_header_check
s $smtp_mime_header_checks $smtp_nested_header_checks
relay_domains = ${{$compatibility_level} < {2} ? {$mydestination} : {}}
[EmySNA@Emyserver ~]$
```

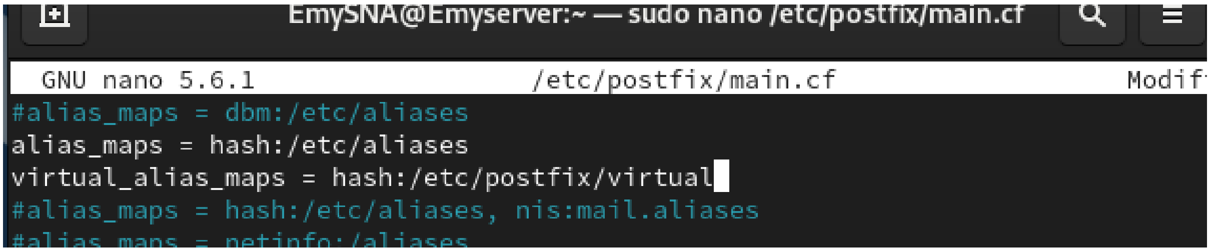
And based on the first few lines there has been an overriding.

So to have postfix direct mail to respective system user “virtual_alias_domains = techsys.com” must be added to “main.cf” so postfix treats “techsys.com” as local:



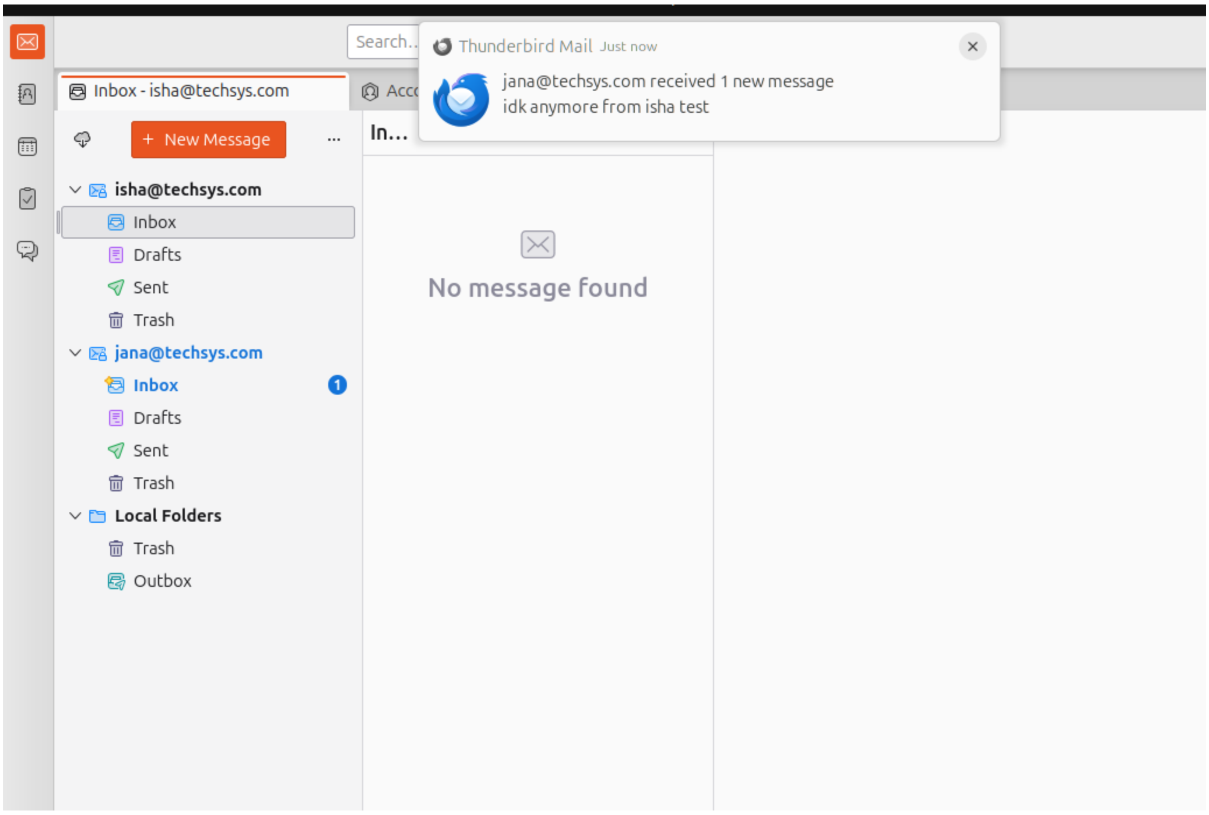
```
smtpd_tls_auth_only = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
virtual_alias_domains = techsys.com

# Global Postfix configuration file. This file lists only a subset
```

Then we add “sudo postconf | grep mydestination” to point to postfix the “/etc/postfix/virtual” file that has the virtual aliases of users so postfix knows which user to deliver mail to when giving an Email account:



```
  GNU nano 5.6.1                   /etc/postfix/main.cf                   Modif
#alias_maps = dbm:/etc/aliases
alias_maps = hash:/etc/aliases
virtual_alias_maps = hash:/etc/postfix/virtual
#alias_maps = hash:/etc/aliases, nis:mail.aliases
#alias_maps = netinfo:/aliases
```

And now mails are properly sent:



Thunderbird Mail Just now

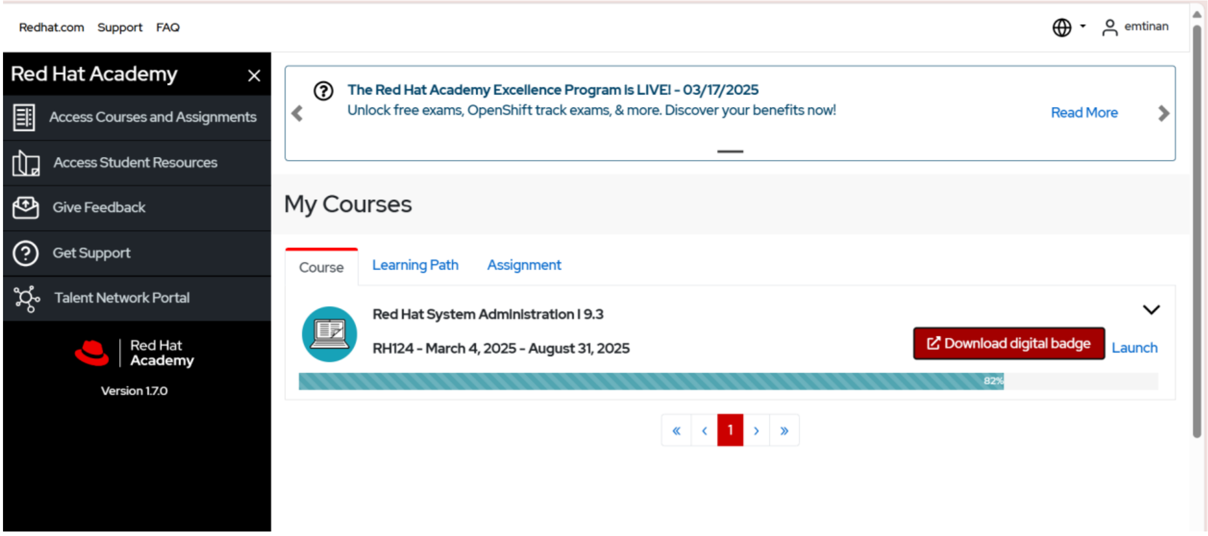
jana@techsys.com received 1 new message
idk anymore from isha test

No message found

Thunderbird now works and receives emails normally.

RedHat Academy Certificate/Progress:

Certificate wasn’t given upon course completion, but a badge was given:



The Red Hat Academy Excellence Program is LIVE! - 03/17/2025

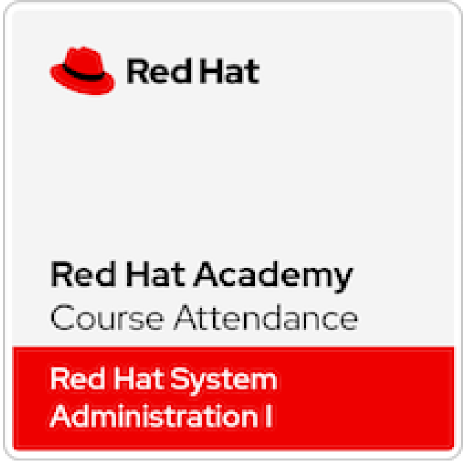
Unlock free exams, OpenShift track exams, & more. Discover your benefits now!

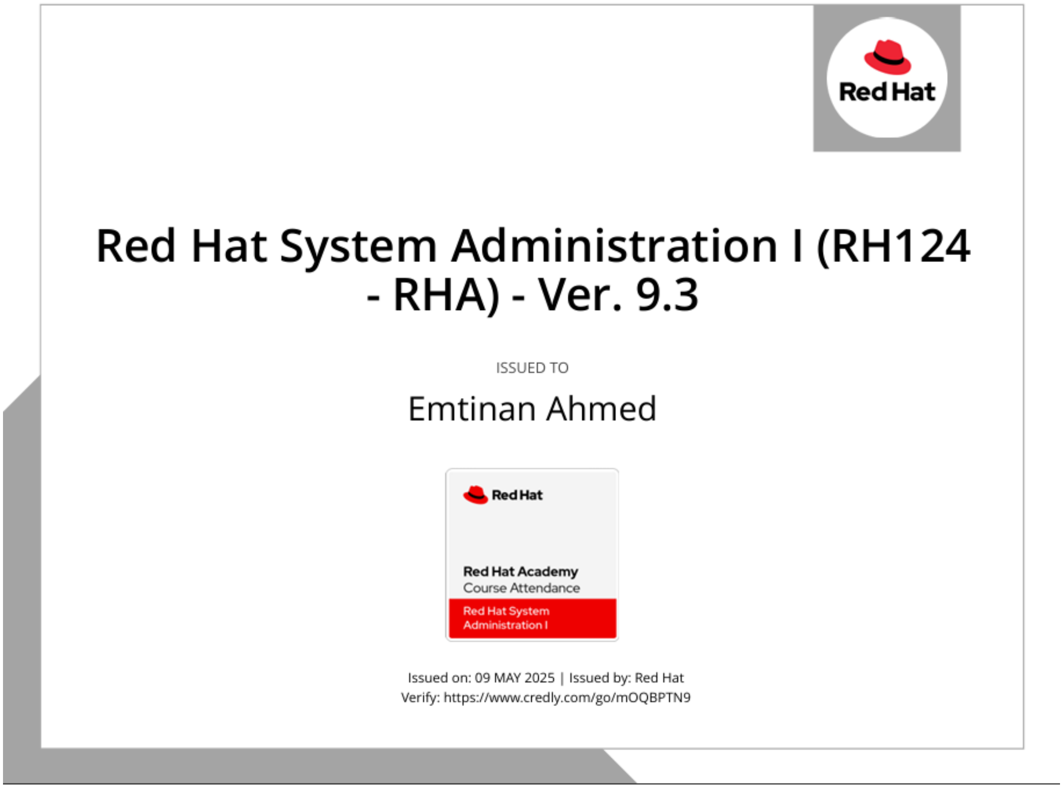
My Courses

Red Hat System Administration I 9.3

RH124 - March 4, 2025 - August 31, 2025

RedHat Academy course completion badge:





Red Hat

Red Hat System Administration I (RH124 - RHA) - Ver. 9.3

ISSUED TO

Emtinan Ahmed

Red Hat

Red Hat Academy
Course Attendance

Red Hat System
Administration I

Issued on: 09 MAY 2025 | Issued by: Red Hat
Verify: https://www.credly.com/go/mOQBPTN9