

APD2F2409

HAND OUT DATE: WEEK 2 2024

HAND IN DATE: WEEK 12 2024

WEIGHTAGE:

INSTRUCTIONS TO CANDIDATES:

**1 Submit your assignment at the administrative counter.**

**2 Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**

**3 Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.**

**4 Cases of plagiarism will be penalized.**

**5 The assignment should be bound in an appropriate style (comb bound or stapled).**

**6 Where the assignment should be submitted in both hardcopy and softcopy, the softcopy of the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**

**7 You must obtain 50% overall to pass this module.**

**Name: Goh Yuan Kee**

**TP number: TP07012ss6**

Contents

s[1 Introduction 5](#_Toc182661240)

[1.1 Objective 5](#_Toc182661241)

[1.2 Network Integration and Security 5](#_Toc182661242)

[1.3 SSL/TLS ENCRYPTION: 5](#_Toc182661243)

[1.4 Project Overview of Steps 5](#_Toc182661244)

[2 Configuration and Setup of Email Server 7](#_Toc182661245)

[2.1 Network Configuration 7](#_Toc182661246)

[Static IP Setup 7](#_Toc182661247)

[2.2 DHCP Configuration: 9](#_Toc182661248)

[Objective: 9](#_Toc182661249)

[Verification: 9](#_Toc182661250)

[2.2.1 Brief Introduction for DHCP 11](#_Toc182661251)

[Cons of DHCP **Error! Bookmark not defined.**](#_Toc182661252)

[2.3 DNS Configuration: 12](#_Toc182661253)

[Objective: 12](#_Toc182661254)

[Verification: 13](#_Toc182661255)

[2.3.1 Brief Introduction of DNS 14](#_Toc182661256)

[2.4 Postfix installation and configuration 15](#_Toc182661257)

[Installation: 15](#_Toc182661258)

[Tasks to be done: 15](#_Toc182661259)

[Verify: 16](#_Toc182661260)

[Configuration: 17](#_Toc182661261)

[Testing 18](#_Toc182661262)

[Process 18](#_Toc182661263)

[2.4.1 Brief Introduction of Postfix 19](#_Toc182661264)

[2.5 Installation and Configuration of Dovecot Installation: 20](#_Toc182661265)

[Objective: 20](#_Toc182661266)

[Configuration: 21](#_Toc182661267)

[Testing: 23](#_Toc182661268)

[2.5.1Brief introduction of Dovecot 25](#_Toc182661269)

[2.6 SSL/TLS Encryption Setup Certificate Creation: 26](#_Toc182661270)

[2.6.1 Steps: 26](#_Toc182661271)

[2.6.2 Postfix SSL Configuration 27](#_Toc182661272)

[2.6.3 Dovecot SSL Configuration: 28](#_Toc182661273)

[2.6.4 SSL/TLS Verification 29](#_Toc182661274)

[2.6.5 Brief Introduction of SSL and TLS 31](#_Toc182661275)

[2.7 Troubleshooting and Testing 32](#_Toc182661276)

[2.7.1 Testing Email functionality 32](#_Toc182661277)

[2.7.2 Troubleshooting Process 33](#_Toc182661278)

[3 Conclusion 34](#_Toc182661279)

[4 Certificate of red head 35](#_Toc182661280)

[5 Proof of video 36](#_Toc182661281)

[6 References 37](#_Toc182661282)

# Introduction

Secure and reliable email communication is the prerequisite for both personal and professional life in the digital landscape today. This project aims at setting up a fully functional, secure email server on a Linux-based system. The server configuration is on Rocky Linux, and client configuration is on Ubuntu, which is considered the new modern practice for open-source, secure, and flexible networking solutions.

## Objective

The key objective in this project is to develop an email server that supports the basic functions of sending, receiving, and storing emails with confidentiality and integrity of data. We use Postfix as the MTA for handling outgoing emails and Dovecot as the IMAP/POP3 server for handling incoming retrieval of email. Through proper configuration of these two components, we enable users to communicate via email and maintain access to data while keeping the same secure and private.

## Network Integration and Security

A secure email server does not function in isolation but rather requires smooth integration with several network services that will deliver connectivity, address management, and data protection. For the purposes of this project, we have integrated the following core services:

* **DNS:** Domain Name System It translates domain names into IP addresses. As a result, any machine in the network can find the email server by searching for a human-friendly domain name; hence it is easier to access and interact with a server.
* **DHCP (Dynamic Host Configuration Protocol):** DHCP simplifies the management of IP addresses since DHCP automatically assigns IP addresses, thus allowing devices in the network to easily connect with minimal configuration. The use of DHCP ensures that IP addresses are well-controlled for usage across the network and is particularly useful for dynamic environments.

## SSL/TLS ENCRYPTION:

Email servers deal with sensitive information most of the time. All data exchanged between the client and the server must be encrypted, and with the usage of SSL/TLS encryption between Postfix and Dovecot, this is ensured, thus keeping unauthorized people from accessing the information or intercepting it. SSL/TLS gives secure communication channels, thus satisfying the needs of confidentiality, and users trust the system more.

## Project Overview of Steps

This is an involved project that will involve several steps, from establishing a Rocky Linux server and an Ubuntu client. It will go through network services setup to the installation and setting up email server components (Postfix and Dovecot) and implementing SSL/TLS encryption. Each step is documented thoroughly in the form of configuration files, commands used, and troubleshooting actions.

Moreover, checking email function through third-party client applications such as Thunderbird ensures that your server is functioning correctly and securely. That way, you have assured your network can reliably support email communication according to modern standards for secure and resilient systems.

# Configuration and Setup of Email Server

## Network Configuration

Static IP Setup:

Objective: Ensure a static IP on the Rocky Linux server is utilized to guarantee that one can access the server with reliability.

**Steps:**

* Edit the configuration file of the network file: /etc/sysconfig/network-scripts/ifcfg-eth0 (or similar on your network interface).
* Set or add the following parameters using IP address, netmask, gateway, and DNS:

A screenshot of a computer

Description automatically generated

Figure Configuration file for setting a static IP address on Rocky Linux.

* Save and exit the file.
* Reboot the network service, for changes to take effect: (systemctl restart network).
* Testing (Check the IP address by running the Ip addr show command or ifconfig)

A screenshot of a computer

Description automatically generated

Figure 1.2 Configuration file for setting a static IP address on Ubuntu

For the Figure 1 shows the hostname and configuration for static IP address for Rocky Linux, and Figure 1.2 shows the hostname and configuration for static IP address on Ubuntu.

The main purpose of a static IP address is to provide an unchanging address for a device or a server in order to make it easier for crucial of things such as remote access , hosting website and online services that need a static IP address. A static IP address is like a home address.

## DHCP Configuration:

### Objective:

DHCP server setup and dynamic IP assignment to network devices.

**Steps:**

* Edit the DHCP configuration file: /etc/dhcp/dhcpd.conf.
* Define IP address range, subnet mask, and others DHCP parameters.
* Save the file and restart the DHCP service: systemctl start dhcpd (or systemctl restart dhcpd if already running).

### Verification:

Now check the status of DHCP, using systemctl status dhcpd.

A screenshot of a computer

Description automatically generated

Check dhcpd status [Rocky Linux]

* By using the command sudo systemctl status dhcpd to check the dhcp status.
* Based on the picture shown above, dhcp is running and active. The log messages show carious DHCP server activities, such as "Listening on LPF/enp013/08:00:27:65:71:11", "Sending on LPF/enp053/05:00:27:09:71", and "DHCPREQUEST for 192.168.200.100 from 08:00:27:65:71:11". These messages confirm that the DHCP server is processing requests and responding to clients.

A screenshot of a computer

Description automatically generated

dhcp work well [on Ubuntu]

A screenshot of a computer

Description automatically generated

dhcp work well [on rocky]

### 2.2.1 Brief Introduction for DHCP

**What is DHCP**

* DHCP also known as Dynamic Host Configuration Protocol is a network protocol that automatically assigns IP addresses to devices quickly. It makes the configuration step more effortless and streamlined.

**Functionality of DHCP**

* DHCP is used for configuring the default gateway, subnet mask, and DNS server information on the device.
* DHCP assigns an IP address to the device automatically.

For small businesses and small home:

* + - Router acts as the DHCP server.

For large networks

* + - A single computer can take the role.
* Unused IP addresses can be reclaimed by the DHCP server. This can be utilized more effectively.

A close-up of a router

Description automatically generated

DHCP(What is DHCP?(nd))

## DNS Configuration:

## Objective:

Configure DNS so that domain names will be translated into the corresponding IP addresses to make accessing network resources more convenient.

**Step:**

* Open the configuration file for DNS: /etc/named.conf.
* Define your zones and records in the configuration, indicating forward and reverse mappings:

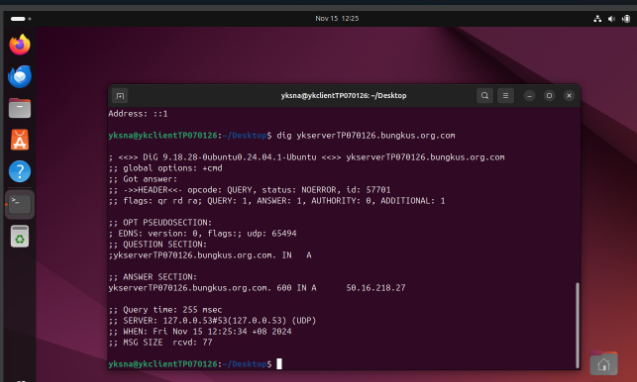
A screenshot of a computer

Description automatically generated

Figure DNS configuration in /etc/named.conf for resolving hostnames to IP addresses.[on rocky Linux]

* Let us restart the DNS service with systemctl restart named.

Verification:  
Test DNS with commands like this: Example usage: nslookup example.com; dig example.com.



DNS works well [on Ubuntu]

A screenshot of a computer

Description automatically generated

DNS works well [on rocky]

### 2.3.1 Brief Introduction of DNS

**What is DNS**

* DNS often called Domain Name System is a system that human-readable domain names such as google.com into machine-readable IP addresses like 142.250.186.142.
* DNS can also able to convert machine-readable IP addresses into human-readable domain names.

**Functionality of DNS**

* In order to allow computers to communicate with each other, DNS converts domain names into IP addresses.
* DNS manages to improve user experience. This is owing to DNS making it easier for users to remember and access websites using domain names instead of complex IP addresses.
* DNS is capable of routing emails to the correct servers based on domain names. This enables email delivery.

**Cons of DNS**

* Disrupt internet access worldwide will occur if a considerable number of DNS failures.
* Cyberattacks including DNS poisoning and DDoS attacks, which can redirect users to malicious websites are usually faced by DNS servers. This is due to the reason that DNS servers are frequent targets for cyberattacks.
* DNS will issue some privacy concerns. This is caused by traditional DNS queries can expose user browsing habits to third-party entities.

## Postfix installation and configuration

Installation:  
Install Postfix as MTA for sending emails.

### Tasks to be done:

* Install postfix from the package manager.
* Start and enable postfix at boot.

A screenshot of a computer

Description automatically generated

Figure Command output showing successful installation of Postfix on Rocky Linux.

Figure 3 shows that Postfix was successfully installed on Rocky Linux.

A screenshot of a computer

Description automatically generated

Figure Command for starting postfix in Rocky Linux.

Figure 4 shows that Postfix was started by using the command sudo systemctl start postfix.

Verify:  
Confirm by running systemctl status postfix

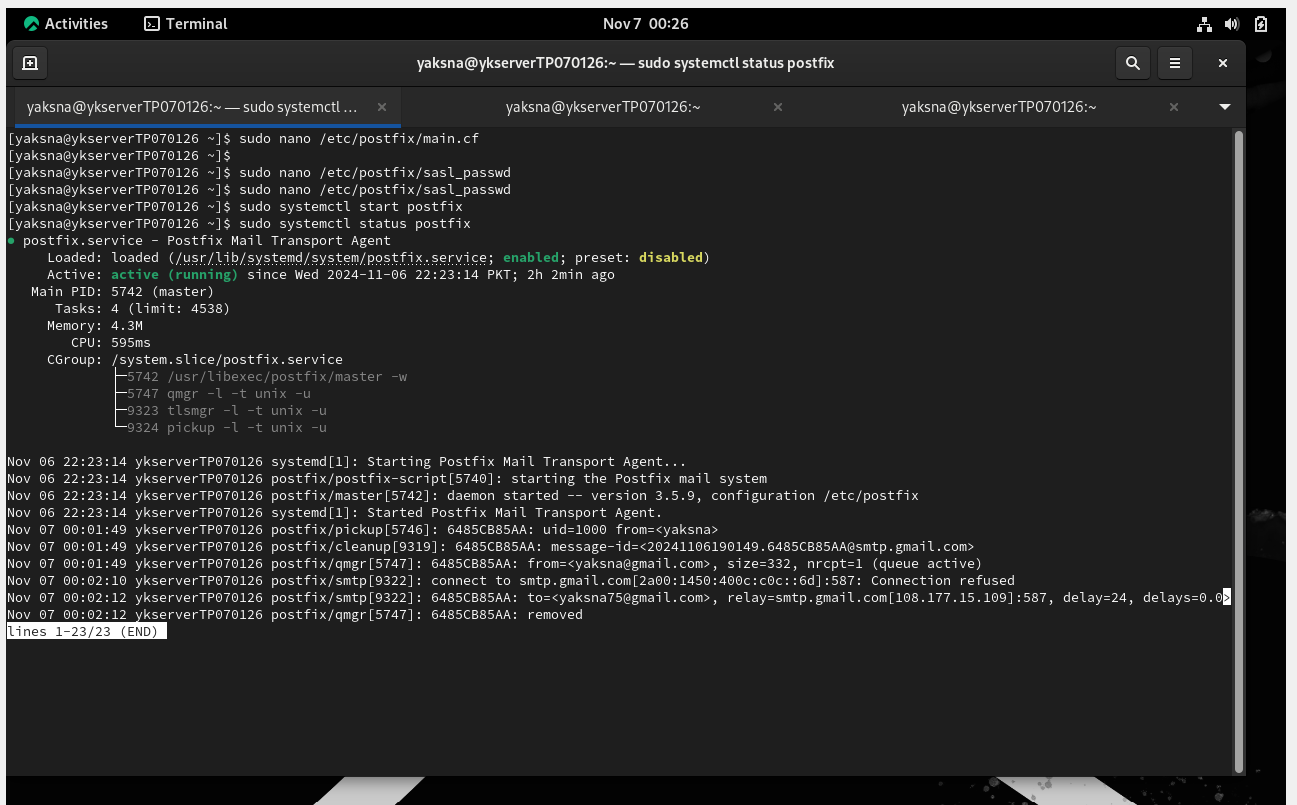
****

Figure Status check showing Postfix service is active and running.

Figure 5 shows that the status of Postfix which is active and running.

Configuration:

* Configure Postfix to manage outgoing emails for specific domains and particular users.  
  Tasks to be done.
* Open main configuration file /etc/postfix/main.cf, and set the necessary parameters for handling domains and users.
* Restart Postfix: Make changes take effect, Sudo systemctl restart postfix.

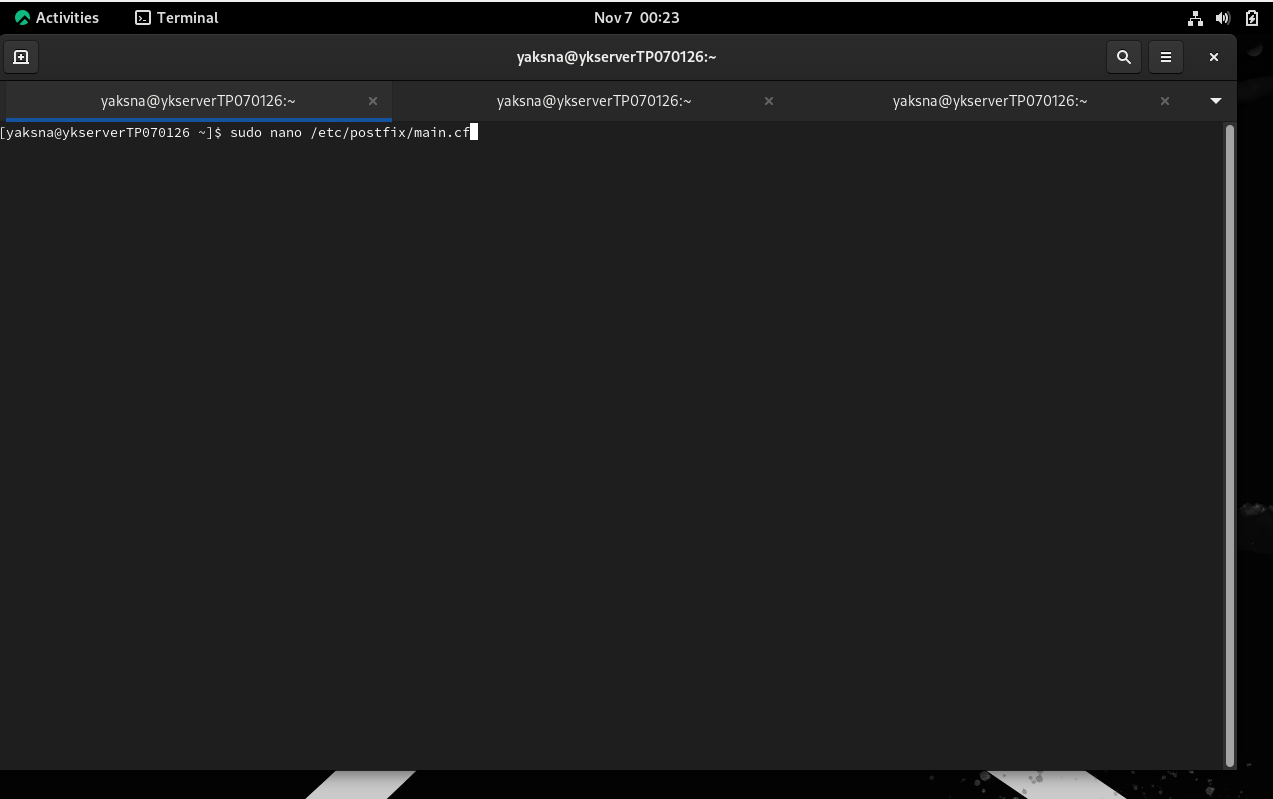


Figure Postfix main configuration file.

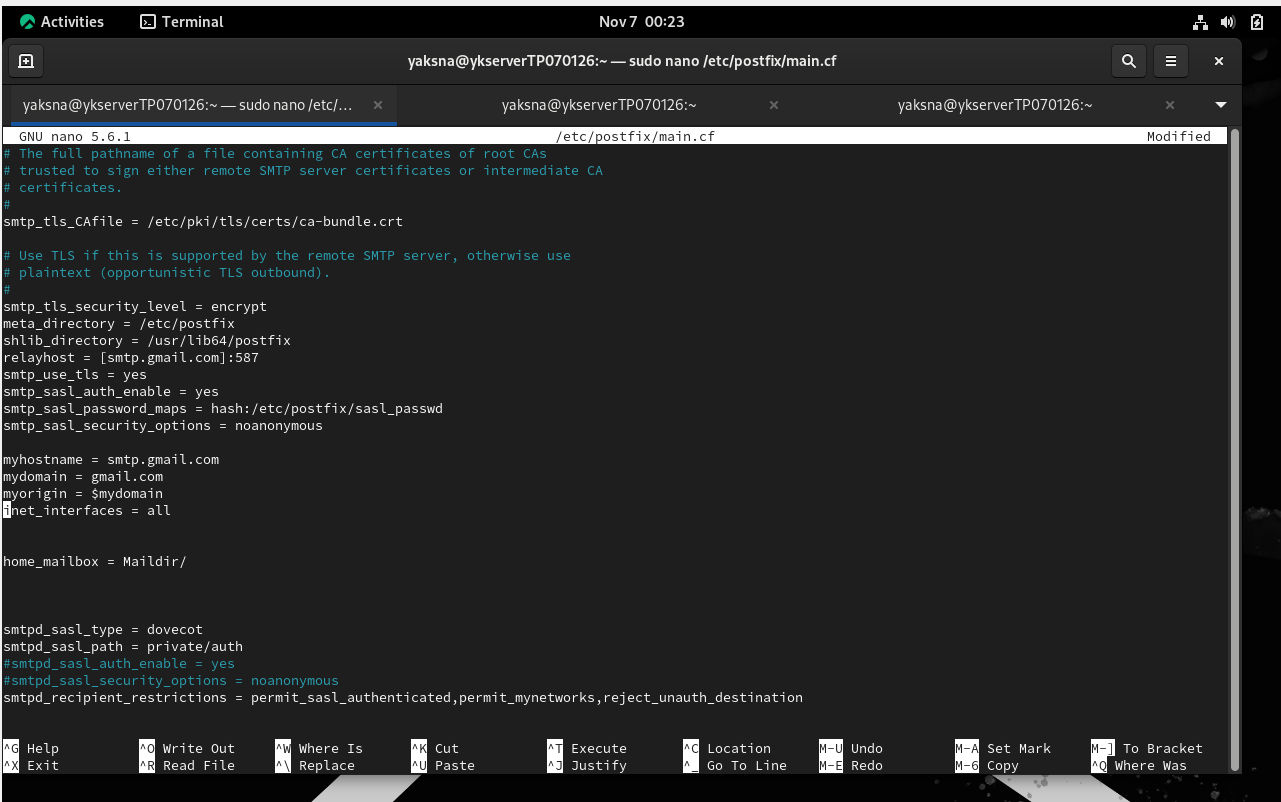


Figure Postfix main configuration file with domain and user settings in /etc/postfix/main.cf..

Figure 7 shows the Postfix main configuration file with domain and user settings in /etc/postfix/main.cf. Those configuration directives were needed insides the /etc/postfix/main.cf.

### Testing

**Objective:** Confirm that Postfix runs smoothly.

### Process

* Test your email using the terminal:
* Check the maillog at /var/log/maillog.

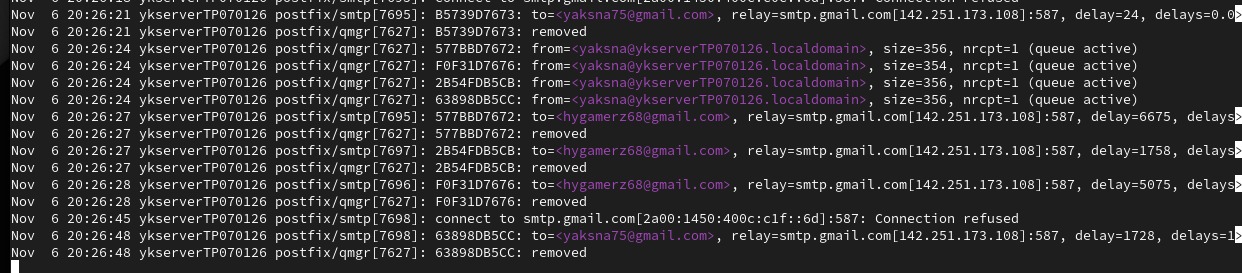


Figure Mail log.

### 2.4.1 Brief Introduction of Postfix

**What is Postfix**

* Postfix is a powerful and widely used Mail Transfer Agent (MTA).
* Postfix is released in 1998 under the name VMailer.
* Postfix is in charge of sending, receiving, and transferring messages between networks.

**Functionality of Postfix**

* Incoming email messages from other mail servers and local clients are accepted by Postfix.
* To protect the privacy of the users and the management of the security, Postfix implements various of security measures. For instance, TLS encryption and authentication.
* Postfix can be configured to handle a wide range of email scenarios, from small personal setups to large enterprise deployments.

**Cons of Postfix**

* Similar to other software, Postfix has security vulnerabilities. It is important that keep it up-to-date to improve security.
* Command-line tools are the primary relies for configuration and management on Postfix, which might not cater to all user needs.
* Mastering Postfix requires a solid understanding of email protocols and system administration, which can be a steep learning curve for beginners.

## Installation and Configuration of Dovecot Installation:

Objective:   
Dovecot configuration to receive the incoming mails through IMAP/POP3.

**Steps:**

* Install Dovecot:
* Dovecot ON

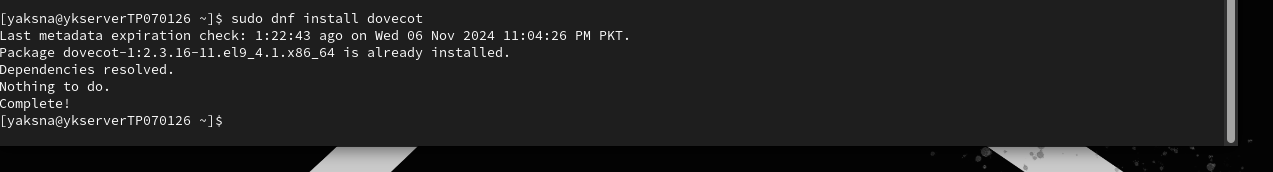


Figure Command output showing successful installation of Dovecot. [on rocky Linux]

Figure 9 shows that Dovecot is successfully installed on Rocky Linux.

A computer screen with white text

Description automatically generated

Figure Status check confirming Dovecot is active and operational.[on Rocky Linux]

Figure 10 shows the status of Dovecot which is running and enable.

Configuration:  
Objective: Configuring Dovecot with Postfix.

Steps:

* edit /etc/dovecot/dovecot.conf for simple settings.
* configure user authentication in 10-auth.conf

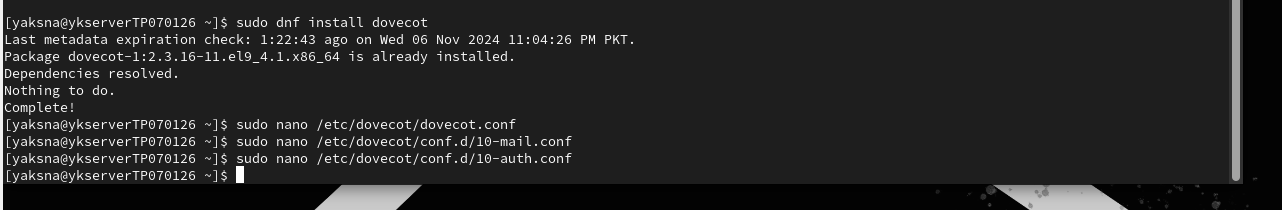


Figure Dovecot configuration file (auth.cf).[on Rocky Linux]

Figure 11 shows the configuration file that needs to be edit using nano command.

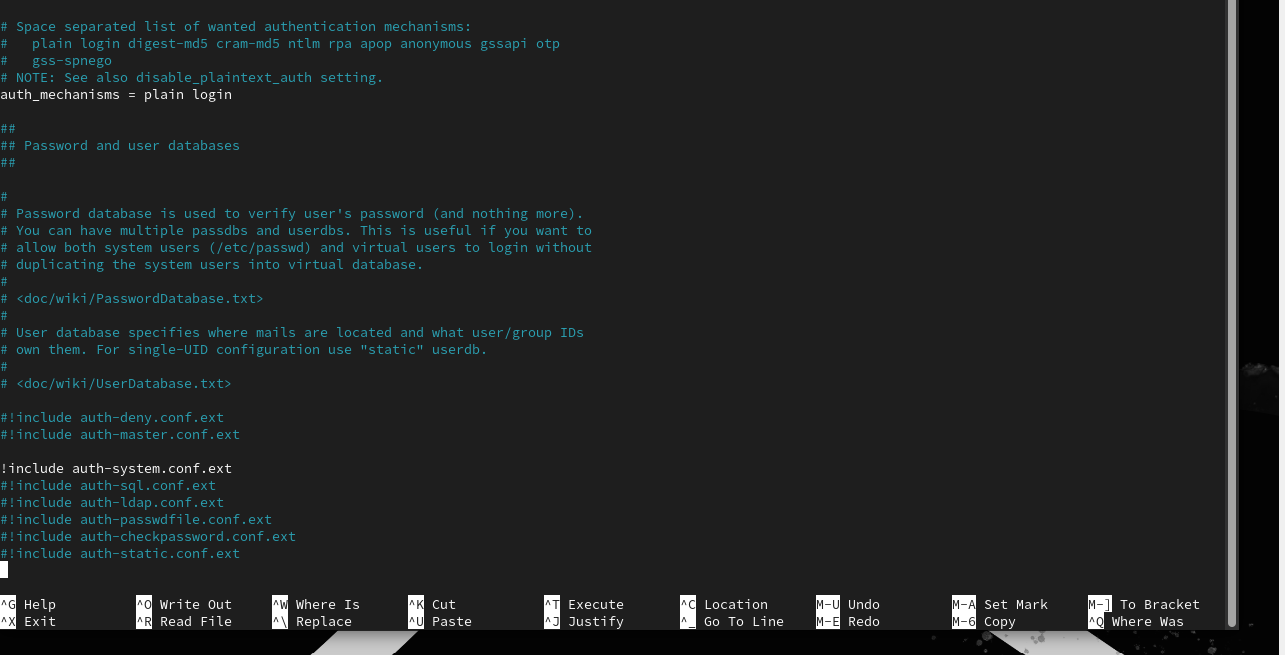


Figure Dovecot configuration file settings for user authentication (auth.cf).[on Rocky Linux]

Figure shows that Dovecot configuration file settings for user authentication (auth.cf).



Figure Dovecot configuration file (dovecot.cf).[on Rocky Linux]

Figure shows Dovecot configuration file

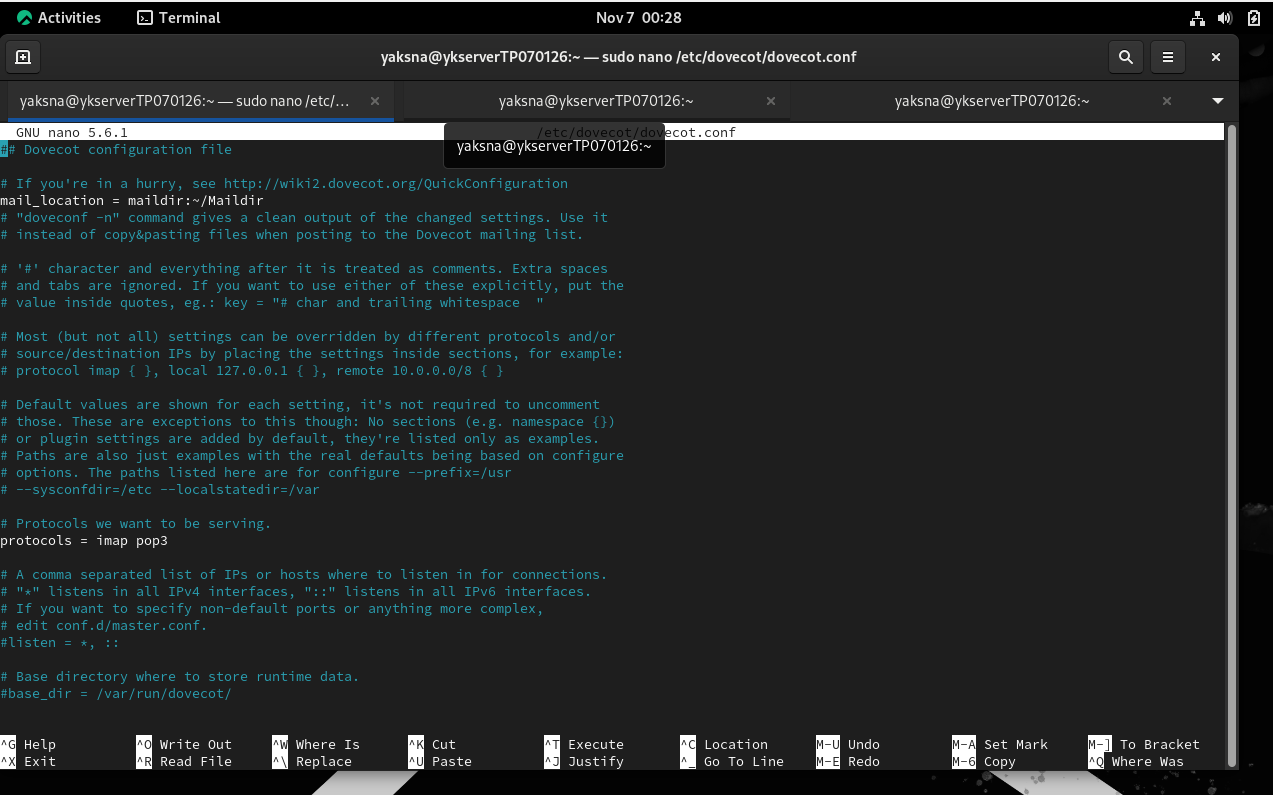


Figure Dovecot configuration file settings for protocols and mail location.[on Rocky Linux]

Figure Dovecot configuration file settings for protocols and mail location. The file is /etc/dovecot/dovecot.conf

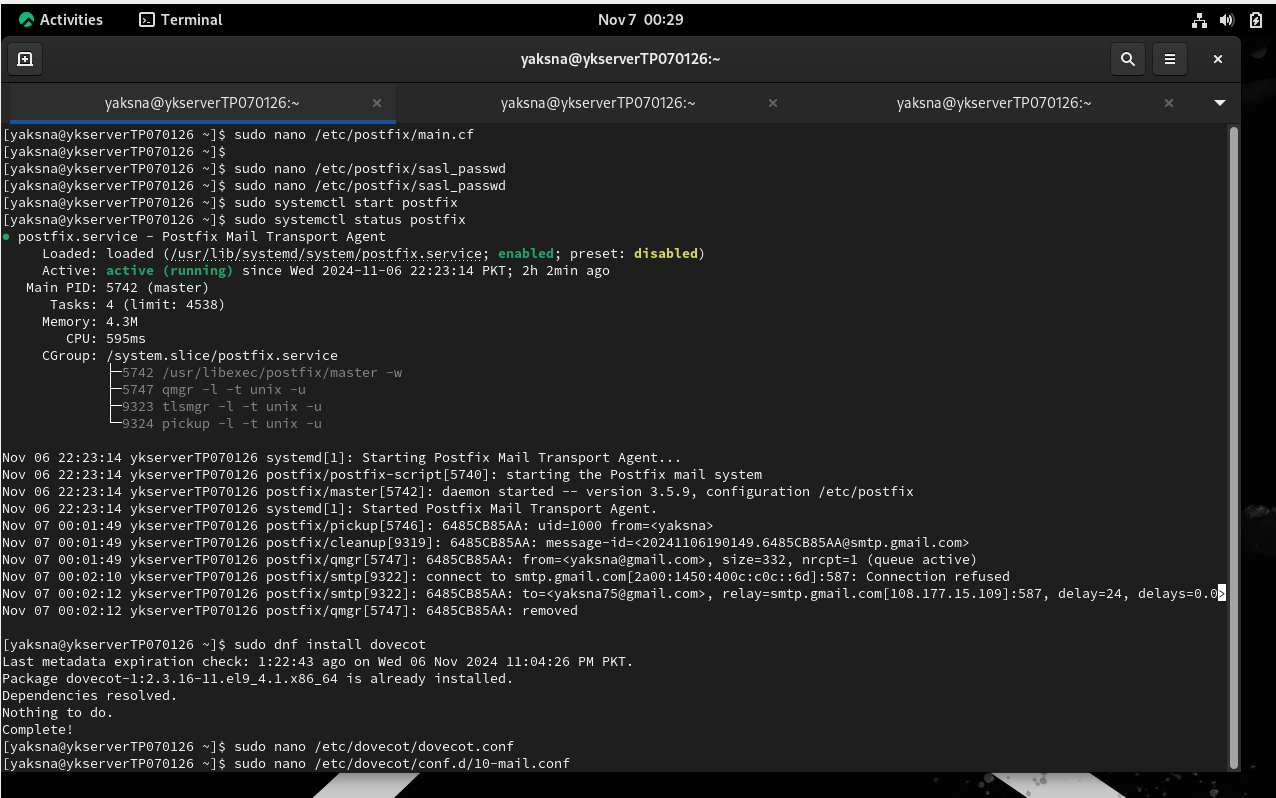


Figure Dovecot configuration file (mail.cf).[on Rocky Linux]

Figure 15 shows the status of Dovecot which running and enable.

A screenshot of a computer

Description automatically generated

Figure Dovecot configuration file (mail.cf) setting for mbox-specific locking methods to manage concurrent access and ensure data integrity.[on Rocky Linux]

Figure Dovecot configuration file (mail.cf) setting for mbox-specific locking methods to manage concurrent access and ensure data integrity.

Testing:  
**Objective:**

Testing Dovecot

**Steps:**

* Test IMAP or POP3 functionality with openssl:
* Openssl s\_client -connect smtp.gmail.com:993.

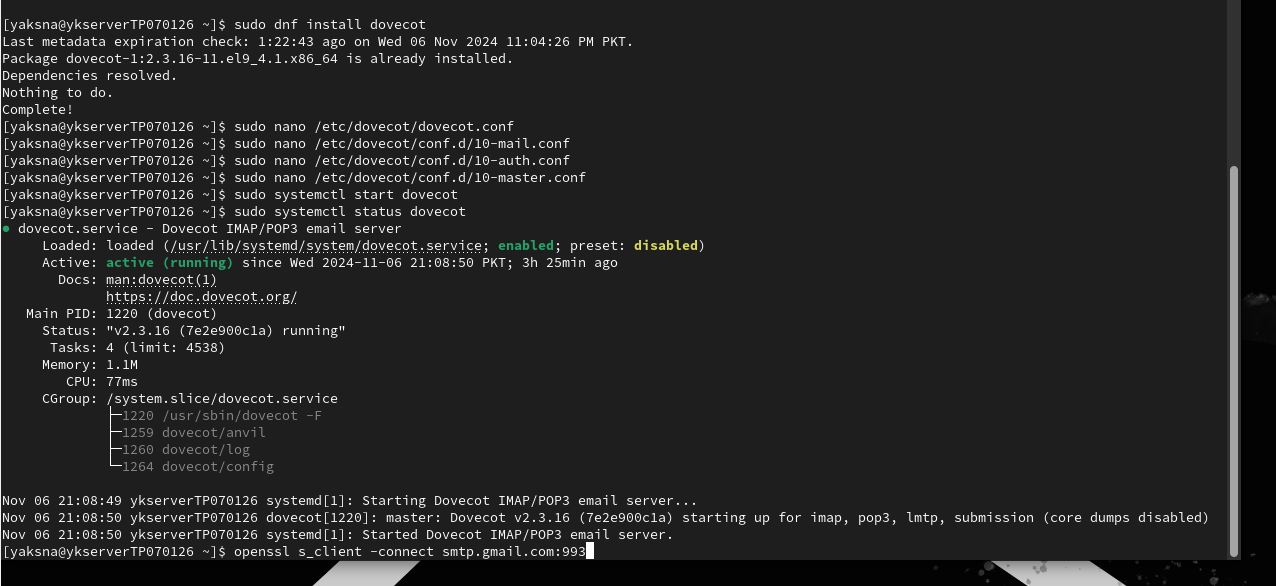


Figure Testing dovecot is listening or not.[on Rocky Linux]

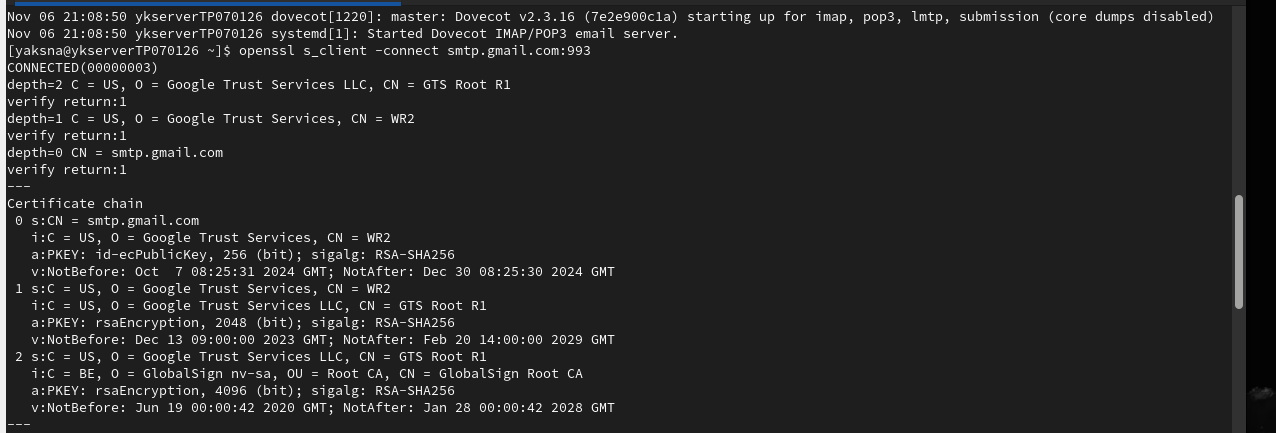


Figure Dovecot is listening successfully on 993 ports.[on Rocky Linux]

### 2.5.1Brief introduction of Dovecot

**What is Dovecot**

* Dovecot is a powerful and secure IMAP and POP3 server for Unix-like operating systems.
* Dovecot is primarily designed to serve as a mail storage server.
* Through diverse of email programs, such as Outlook, Thunderbird, or webmail interfaces, users can view their emails.

**Functionality of Dovecot**

* To ensure the safety of data while it is being transmitted, Dovecot offers secure communication protocols including POP3S (POP3 over SSL/TLS) and IMAPS (IMAP over SSL/TLS).
* Dovecot can handle large numbers of users and emails efficiently.
* Other mail servers like Postfix can be integrated with Dovecot to provide a complete email solution.

**Cons of Dovecot**

* Similar to other software, Dovecot has security vulnerabilities. It is important that keep it up-to-date to improve security.
* Dovecot will consume a lot of resources in a high-traffic environment, especially CPU and memory, which will indirectly affect the overall performance of the server.

## SSL/TLS Encryption Setup Certificate Creation:

**Certificate Creation:**

2.6.1 Steps:

* Generate a certificate using OpenSSL.

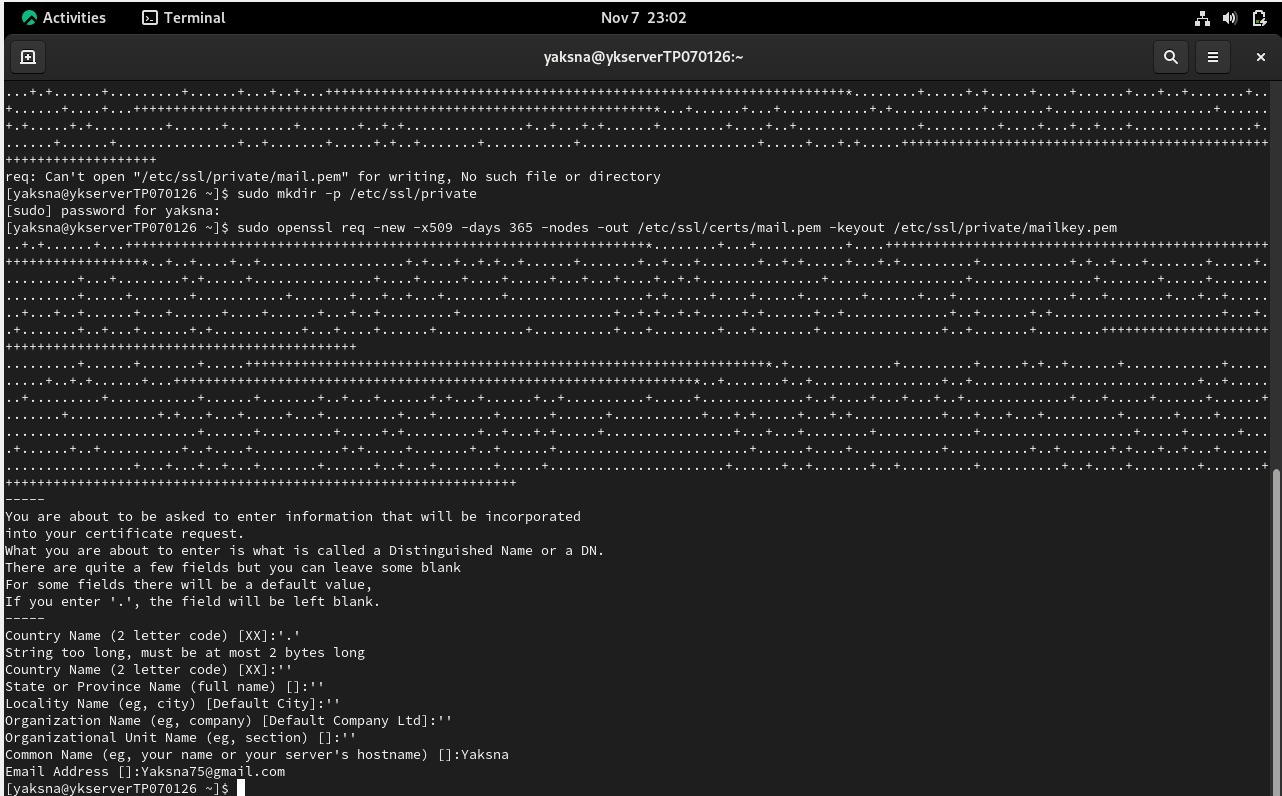


Figure OpenSSL command to generate SSL certificate for encrypted email communication.[on Rocky Linux]

Figure 19 shows the SSL certificate for encrypted email communication by using the command (OpenSSL…...pem).

2.6.2 Postfix SSL Configuration:

* **Steps:**  
  Enable SSL at /etc/postfix/main.cf

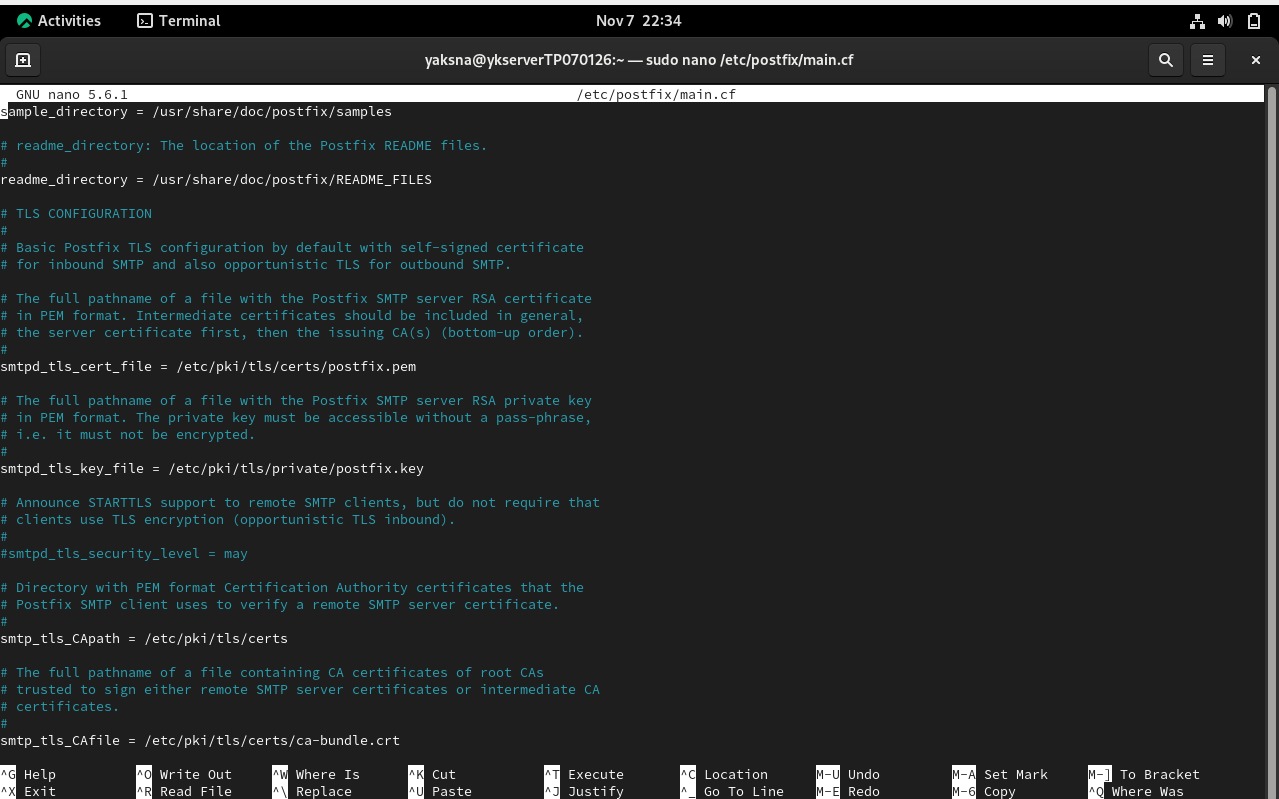


Figure SSL configuration in Postfix's main.cf to enforce secure email transmission.[on Rocky Linux]

Figure 20 shows that SSL configuration in Postfix’s main.cf.

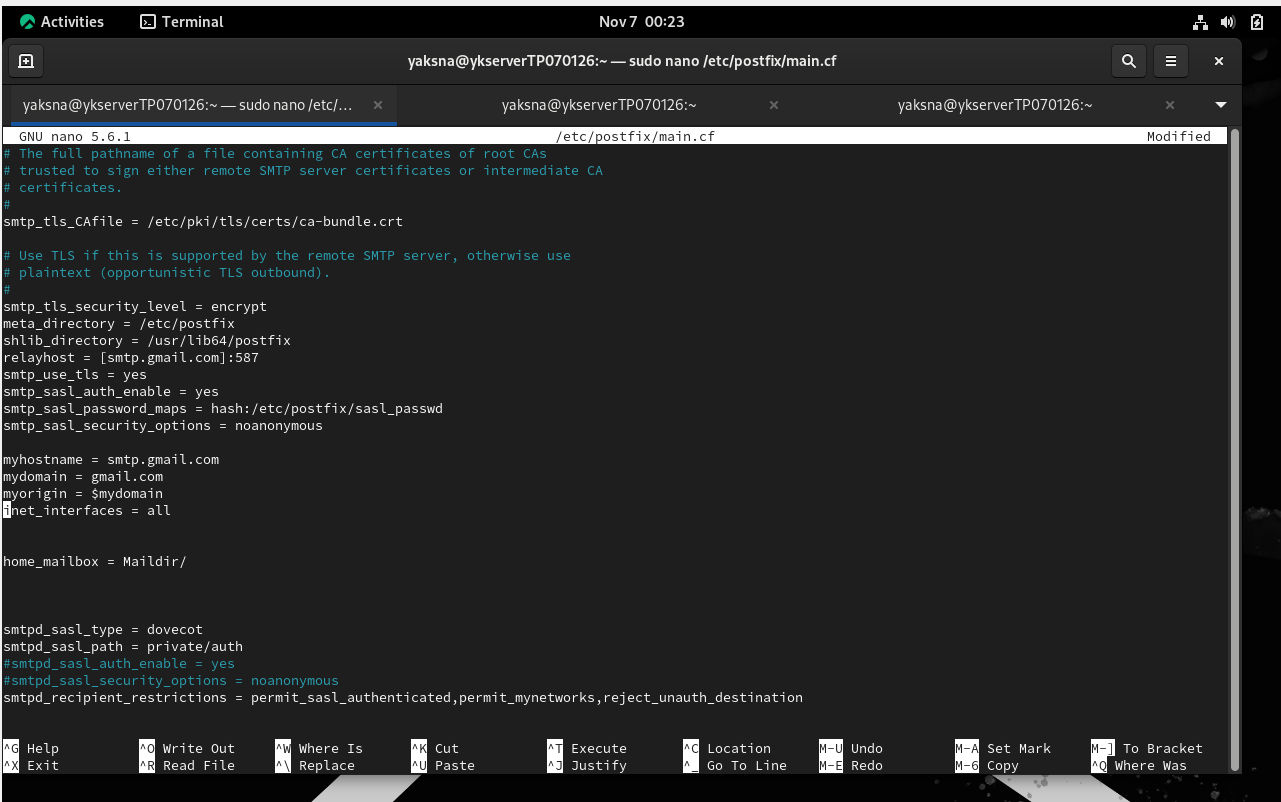


Figure SSL configuration in Postfix's main.cf to enforce secure email transmission.[on Rocky Linux]

### 2.6.3 Dovecot SSL Configuration:

**Steps:**

Edit /etc/dovecot/conf.d/10-ssl.conf.

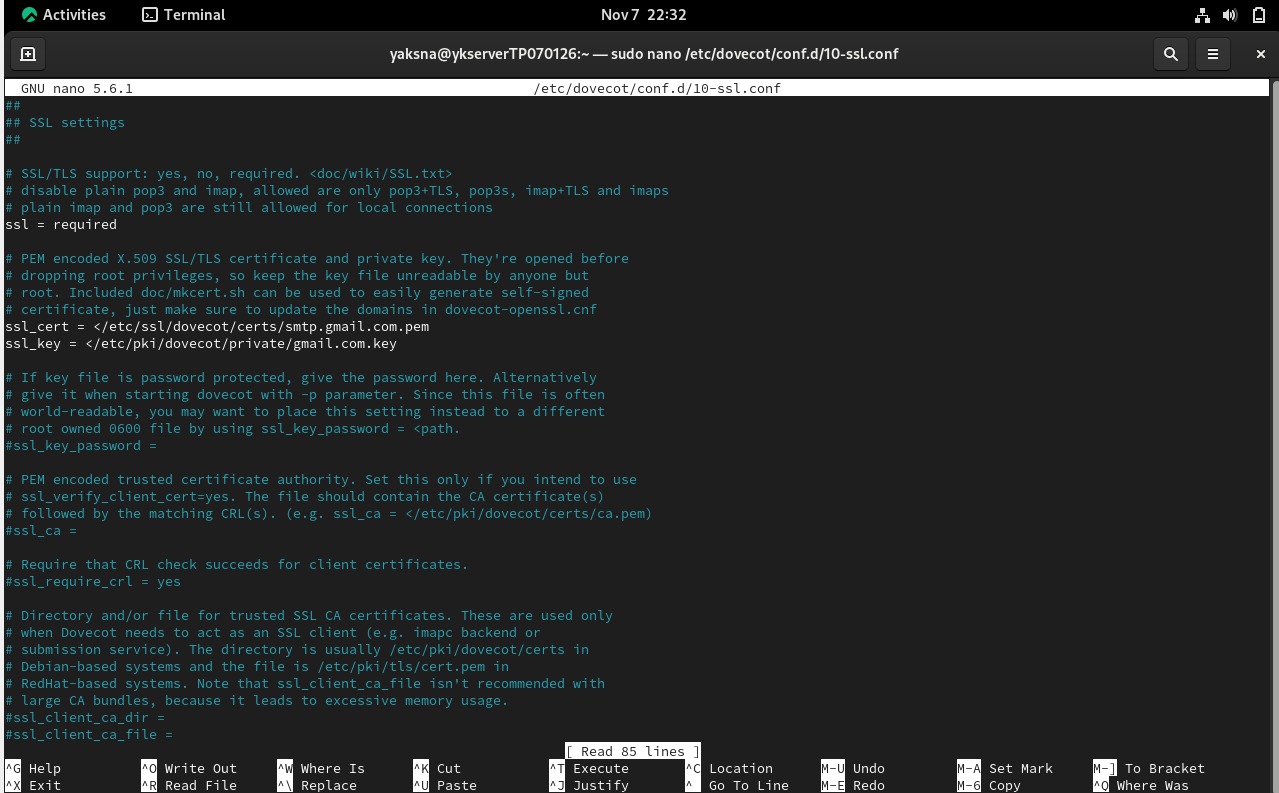


Figure SSL settings in Dovecot's configuration file for secure IMAP/POP3 communication.[on Rocky Linux]

### 2.6.4 SSL/TLS Verification

**Testing Commands**

* Use openssl s\_client to test secure connection.

A screenshot of a computer

Description automatically generated

Figure Command for using openssl.[on Rocky Linux]

A screenshot of a computer

Description automatically generated

Figure Command output from openssl s\_client showing successful SSL/TLS connection to the mail server.[on Rocky Linux]

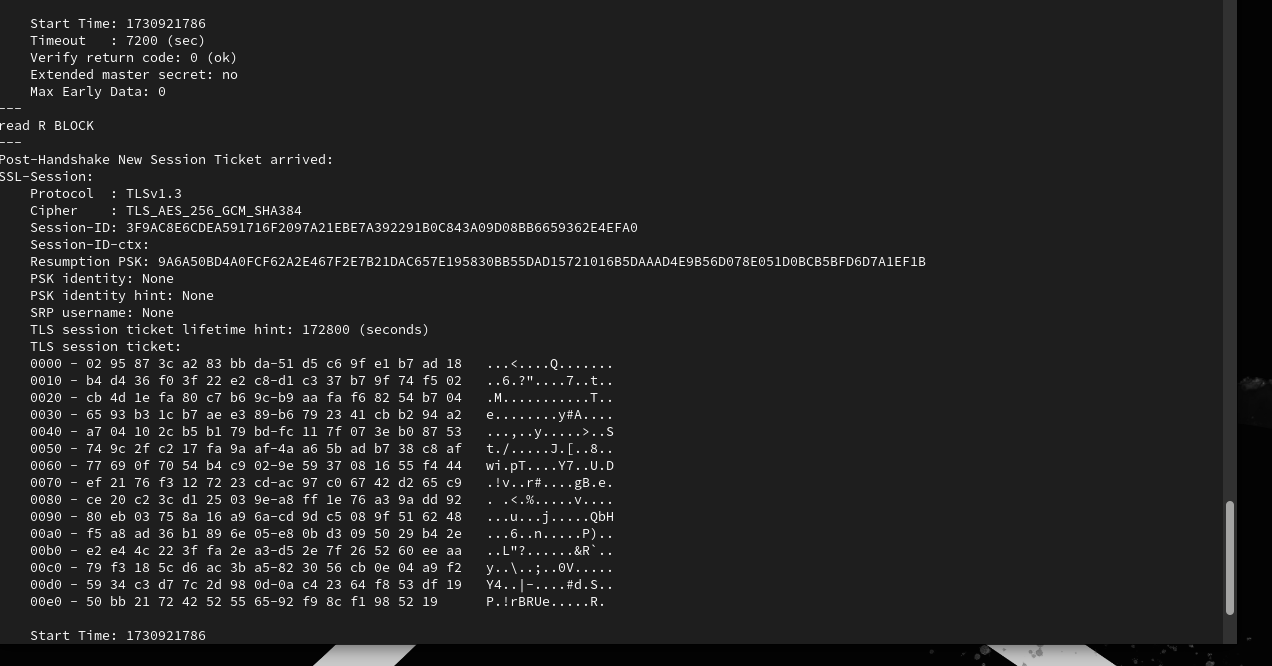


Figure Command output from openssl s\_client showing successful SSL/TLS connection to the mail server.[on Rocky Linux]

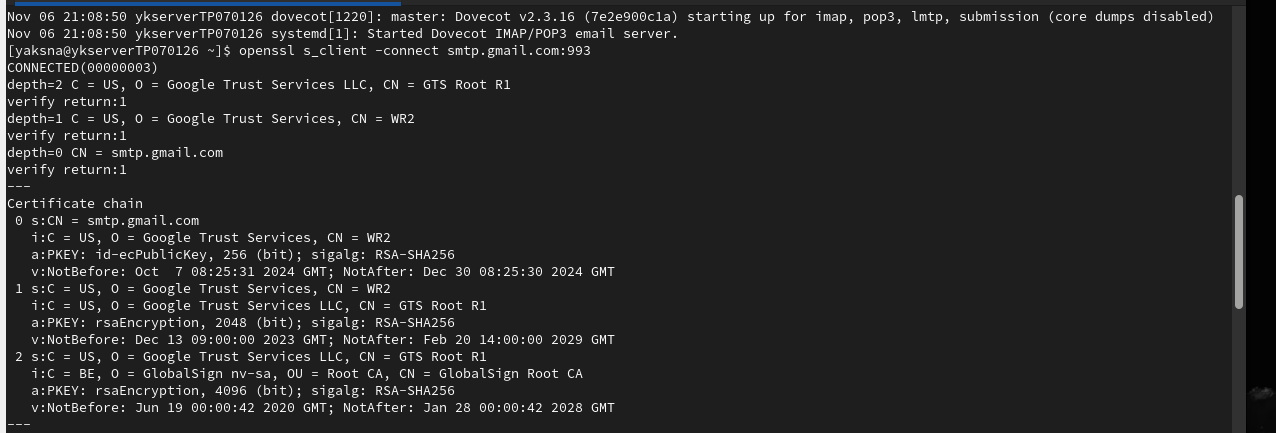


Figure Command output from openssl s\_client showing successful SSL/TLS connection to the mail server.[on Rocky Linux]

### 2.6.5 Brief Introduction of SSL and TLS

**What is SSL**

SSL identified as Secure Sockets Layer was an early protocol for protecting internet communication. However, in later editions, these vulnerabilities were addressed.

**What is TLS**

TLS also referred to as Transport Layer Security has almost the same function as SSL but is more favourable than SSL. It's a well-defined protocol that has evolved over time to address security challenges.

**Differentiate between SSL and TLS**

|  |  |  |
| --- | --- | --- |
| **Feature** | **SSL** | **TLS** |
| Development | Established by Netscape in the 1990s | * More favorable than SSL. * First version released in 1999 |
| Versions | SSL 1.0, 2.0, 3.0 | TLS 1.0, 1.1, 1.2, 1.3 |
| Security | Evaluated insecure and outdated | More secure with improved algorithms |
| Handshake Process | Less efficient | More efficient with reduced round trips |
| Cipher Suites | Limited and less secure options | More extensive and secure options |
| Error Handling | Basic error handling | Improved error handling and reporting |
| Usage | Rarely used in modern applications | Widely used in HTTPS and secure communications |

## Troubleshooting and Testing

### 2.7.1 Testing Email functionality

* Using Thunderbird, test email functionality with SSL/TLS

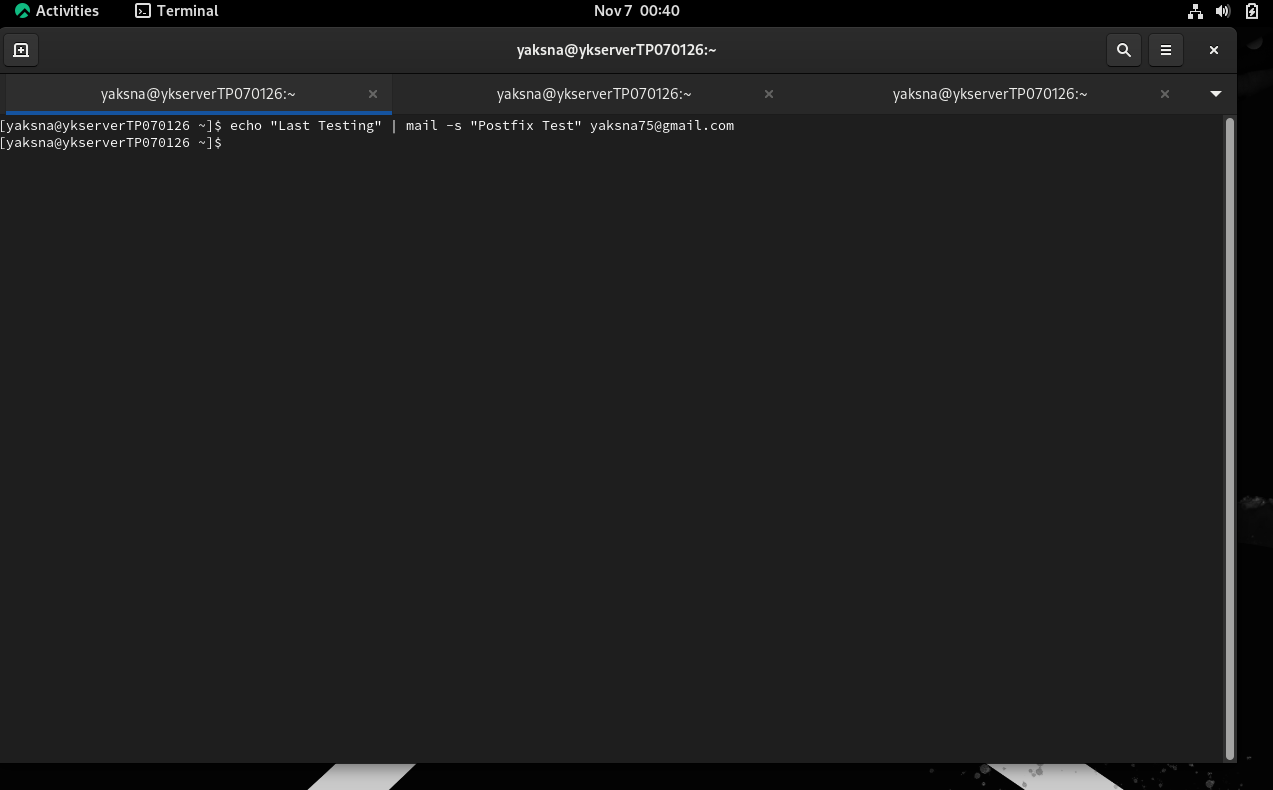


Figure Command output from openssl s\_client showing successful SSL/TLS connection to the mail server.[on Rocky Linux]

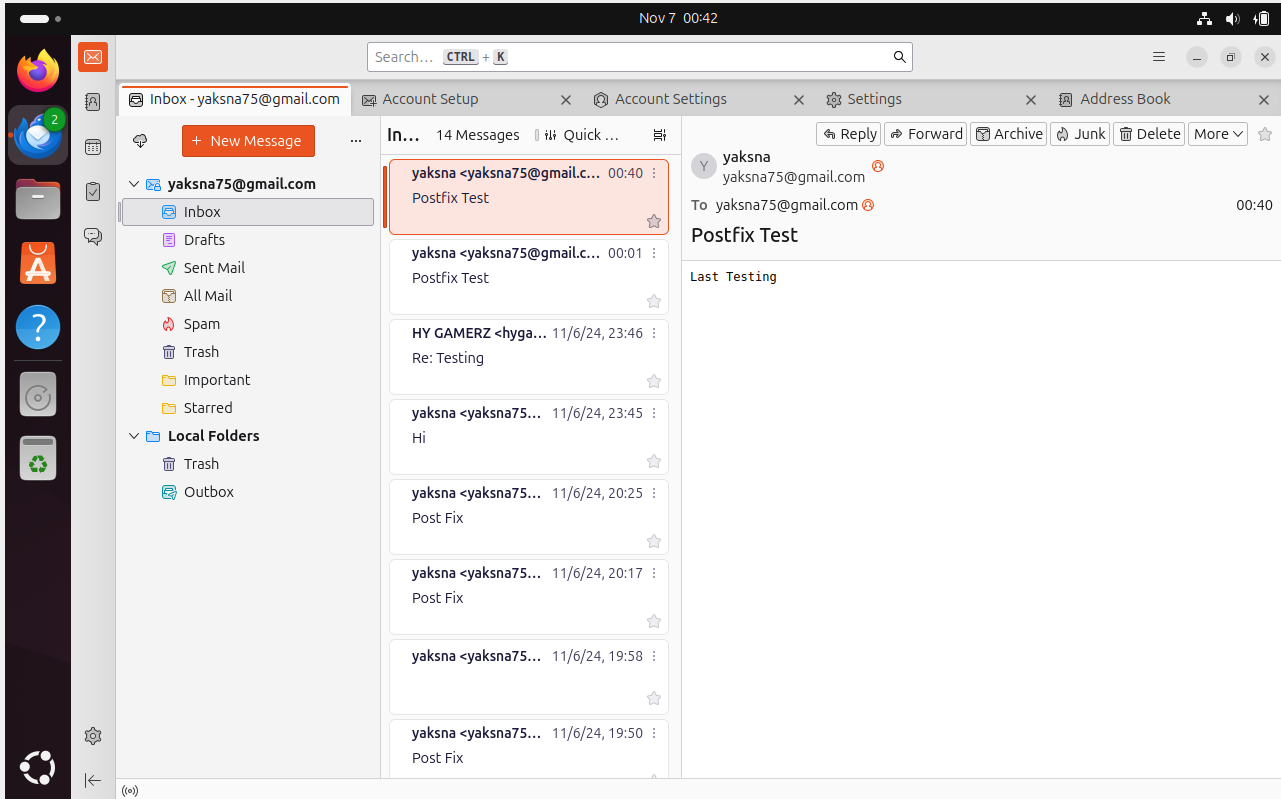


Figure Successful email send and receive test in Thunderbird with SSL/TLS enabled.[on Ubuntu]

2.7.2 Troubleshooting Process:

* With logs, record error and resolutions met.

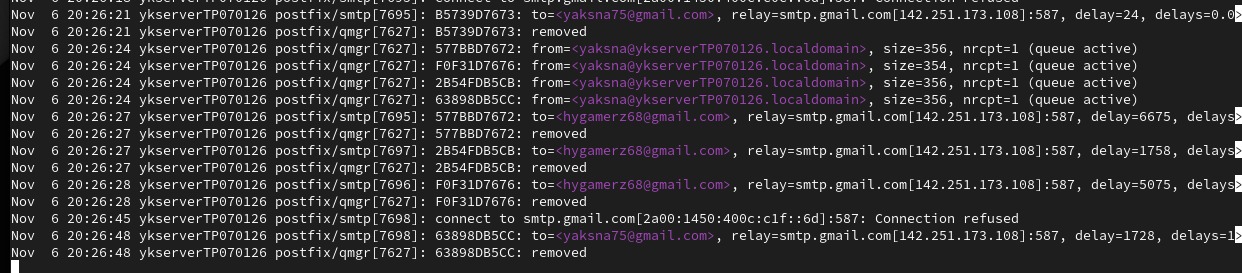


Figure No errors received.

# Conclusion

This project has configured a fully functional email server, where Rocky Linux was used as the server and Ubuntu used as the client. It has designed and established an email communication system that meets modern security standards, carefully integrating all the necessary network services like DNS, DHCP, and SSL/TLS encryption. It can give a stable network foundation by attaining reliable connectivity and effective IP management through static IP, DNS, and DHCP configurations. Finally, postfix configured as the Mail Transfer Agent and Dovecot for IMAP/POP3 email retrieval resulted as the core email functionalities in order for the users to actually send and receive emails; SSL/TLS encryption added an important layer of security in terms that all the emails were encrypted while sending and received.

The third-party email client tested this project completely, and everything worked just perfectly, secure operation of the server. This hands-on experience was particularly insightful in terms of network and system administration, especially for configuring and securing Linux-based servers. The skills acquired in the setup and troubleshooting of secure email communication systems will be applied to all future work involving network administration in high-security environments.

# Certificate of red head

A certificate of attendance with a red and white background

Description automatically generated

# Proof of video



This is proof of the video.

# References

Zhou, J., Fu, W., Hu, W., Sun, Z., He, T., & Zhang, Z. (2024). Challenges and Advances in Analyzing TLS 1.3-Encrypted Traffic: A Comprehensive Survey. *Electronics*, *13*(20), 4000.

Matharu, S. K. (2021). Exploiting SSL/TLS Vulnerabilities in Modern Technologies.

Sharp, R. (2023). Network Security. In *Introduction to Cybersecurity: A Multidisciplinary Challenge* (pp. 171-233). Cham: Springer Nature Switzerland.

Gaminara, A. (2022). *Performance and Security Evaluation of TLS, DTLS and QUIC Security Protocols* (Doctoral dissertation, Politecnico di Torino).

Petraglia, G. (2023). *TLS-Monitor: An Intrusion Detection-based Monitoring Tool for countering TLS Attacks* (Doctoral dissertation, Politecnico di Torino).

Fisher, T. (2020, 13 December). *What is DHCP? (Dynamic Host Configuration Protocol)*. Lifewire. <https://www.lifewire.com/what-is-dhcp-2625848>

Küçükkarakurt, F. (2022, 9 mei). *Introduction to Linux Postfix Architecture for Beginners*. MUO. <https://www.makeuseof.com/postfix-architecture-linux/>

GeeksforGeeks. (2024c, August 20). *Difference Between Secure Socket Layer (SSL) and Transport Layer Security (TLS)* . GeeksforGeeks. <https://www.geeksforgeeks.org/difference-between-secure-socket-layer-ssl-and-transport-layer-security-tls/>

GeeksforGeeks. (2024b, June 19). *Secure Socket Layer (SSL)* . GeeksforGeeks. <https://www.geeksforgeeks.org/secure-socket-layer-ssl/>

GeeksforGeeks. (2024a, May 23). *Transport Layer Security (TLS)* . GeeksforGeeks. <https://www.geeksforgeeks.org/transport-layer-security-tls/>

*What is DHCP?* (z.d.). https://www.iplocation.net/dhcp