Virtual Mail Sever Report

Aniyah Pena, Tyra Baxter, Caroline Adeloye, & Glory Imo

Department of Computer Technology

CTEC 435: UNIX Administration

Professor Anthony Adedoyin

September 26, 2025

Abstract

This report will cover how our team was able to set up a virtual mail server on a Linux Ubuntu Server. On our virtual mail server, we were able to configure services like Postfix, Dovecot, MySQL, Amvis, and Clam AV. This allowed us to create the foundation for our virtual mail server. These steps established groundwork for integrating security protocols and spam protection for systems. Below are screenshots and a description of each part of the project to showcase what was completed.

Research Approach

History

The origins of virtual mail servers began in 1971 when the first email was sent across the ARPANET by Ray Tomlinson. He introduced using the "@" symbol to distinguish between the users and the host name. As time went on protocols like the Simple Mail Transfer Protocol (SMTP) were created and implemented on ARPNET to build a framework on how emails should be delivered in 1983. Then by the 1990's the internet began to expand quickly, and businesses needed a scalable solution to manage emails for multiple domains and users. This led to the development of virtual mail servers, these systems where able to host emails services for multiple domains on a single physical server. These servers also used virtual domains to seperate email traffic which allows hosting systems without having to deploy separate hardware for each domain. Over time as threats like viruses and spam grew in the early 2000's virtual email servers evolved to included advanced security features like SMTP authentication and Transport Layer Security (TLS). Tools like Amavis and ClamAV were created to scan systems for viruses and

filter spam messages. Today, virtual mail servers are essential infrastructure for hosting email for different industries.

How it was gotten

For our UNIX Administration class, our team was assigned to set up a virtual mail server. We chose this project because it ties together core system admin skills like DNS setup, mail transport protocols, database integration, and security tools. We worked with Postfix, Dovecot, MySQL, Amavis, and ClamAV. It wasn't just about installing packages. We had to troubleshoot real issues like authentication errors and missing dependencies, and figure out how each component fits into the bigger picture. This gave us practical experience and helped us understand how to build a secure, working mail system from the ground up.

Results

Virtual mail servers perform the same functions as traditional mail servers, but they operate within a virtualized environment. Despite not running directly on physical hardware, virtual mail servers maintain comparable performance and reliability. They offer societal benefits due to their low maintenance requirements and high functionality. According to Faizan et al. (2020), "The main advantage of virtual mail servers is that they are scalable, and they have their dedicated core and memory allocation. They bring down the installation and maintenance costs. They significantly reduce downtime. They can also be completely customized." These features benefit companies by reducing costs and simplifying installation, thanks to scalability. Users also benefit from minimal downtime, which ensures consistent access to email services.

Below are the screenshots of the process we followed to configure the virtual mail server.

Part 1: Checking Prerequisites

Before configuring the mail server, the server software and system packages were updated. This ensures the system is equipped with the latest security patches, maintains compatibility with mail services, and operates efficiently to support reliable email delivery. After the upgrades and updates were completed, the server was manually configured for DNS. This included configuring an A record to point *mail.themays.com* to the server's public IP address, and an MX record to designate it as the mail handler for the domain.

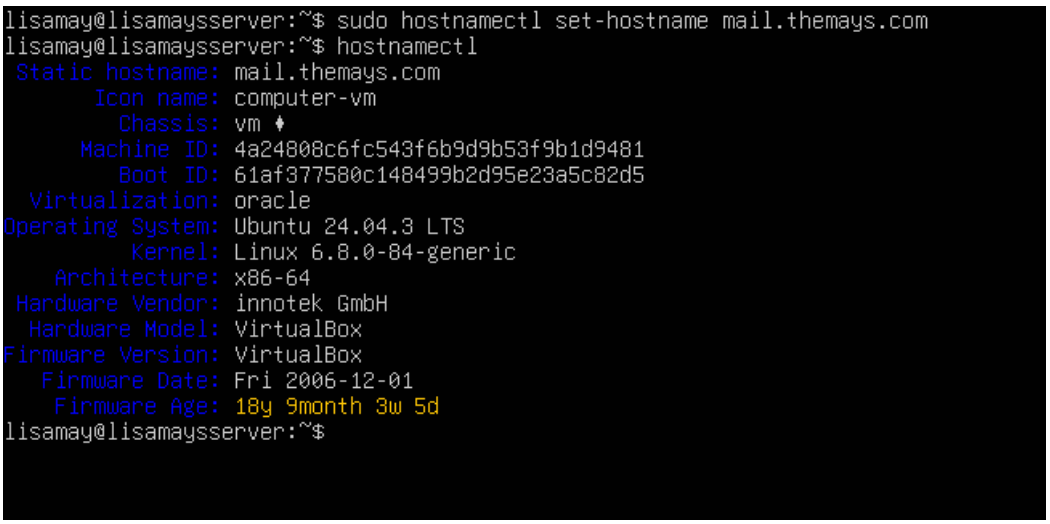


Figure 1- Hostname

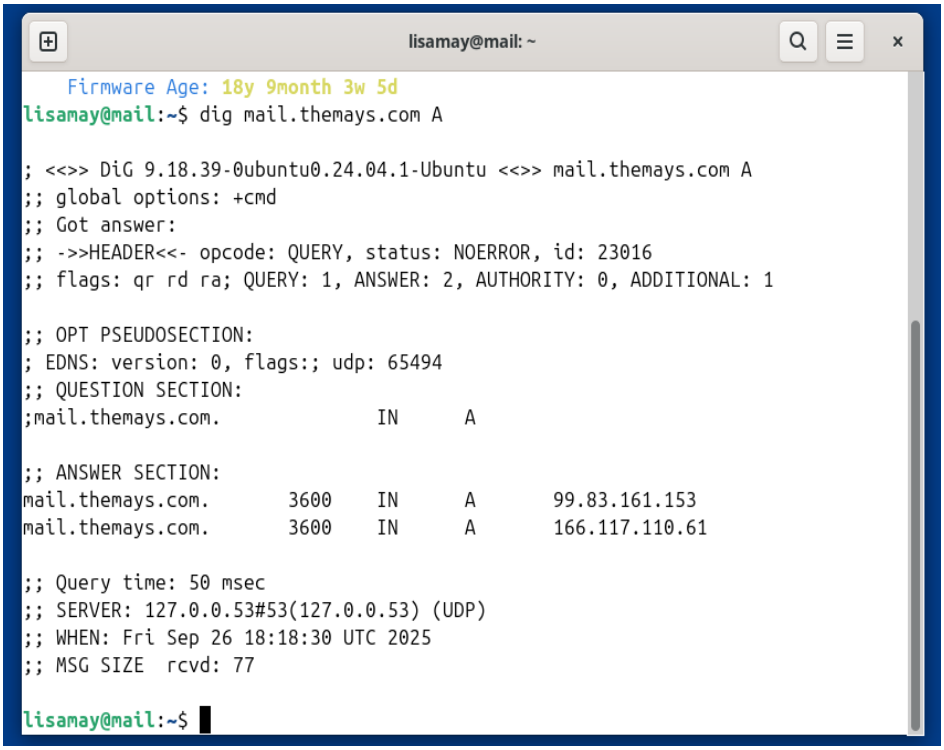


Figure 2- A record

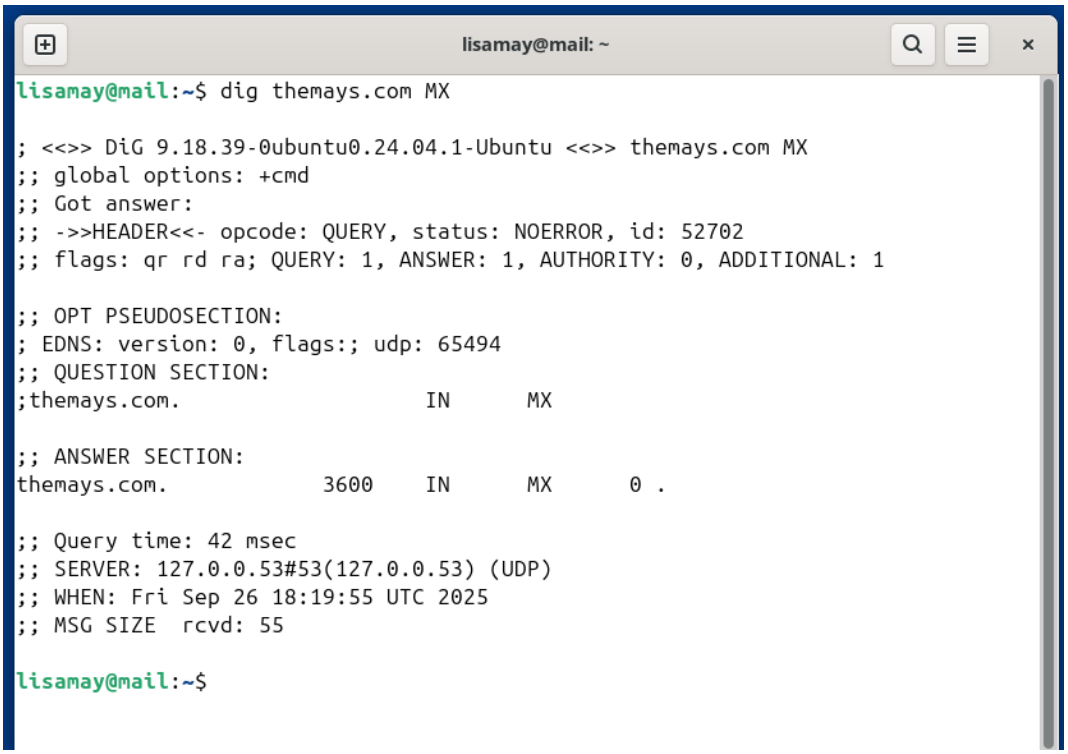


Figure 3 - MX records

Part 2: Installing Required Software Packages

Once DNS was configured and the system was updated, the following software packages were installed to support the mail server: Postfix, MySQL, Dovecot, ClamAV Daemon, and Amavisd. These components work to allow for mail transport, user authentication, spam filtering, and virus scanning. To check if the service was active and enabled, the command ***systemctl status*** was used.

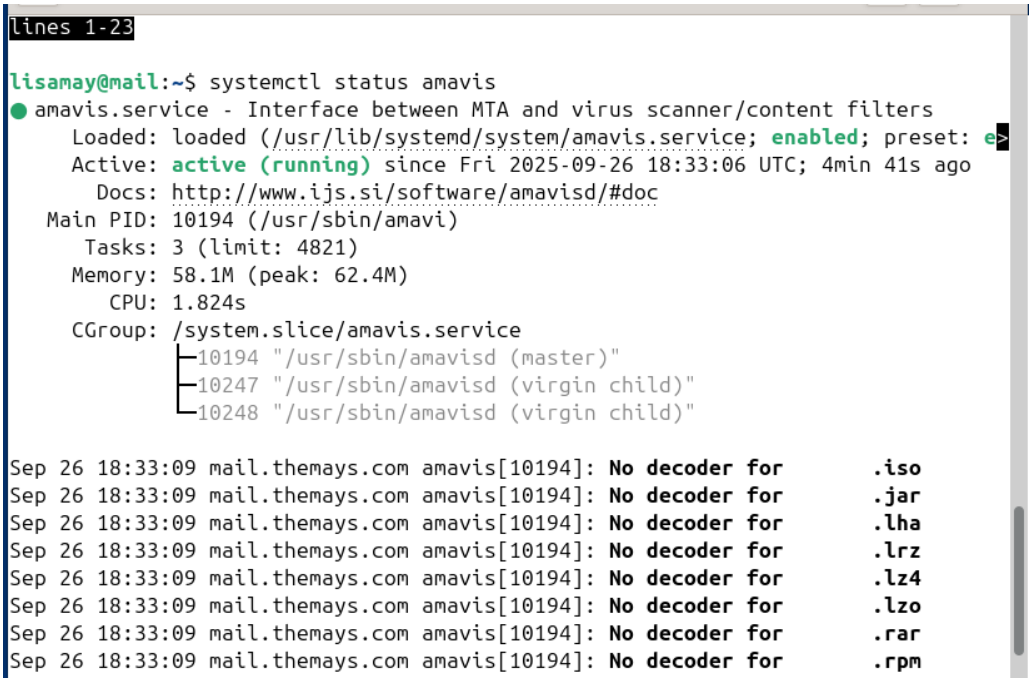


Figure 4 - Status of Amavis

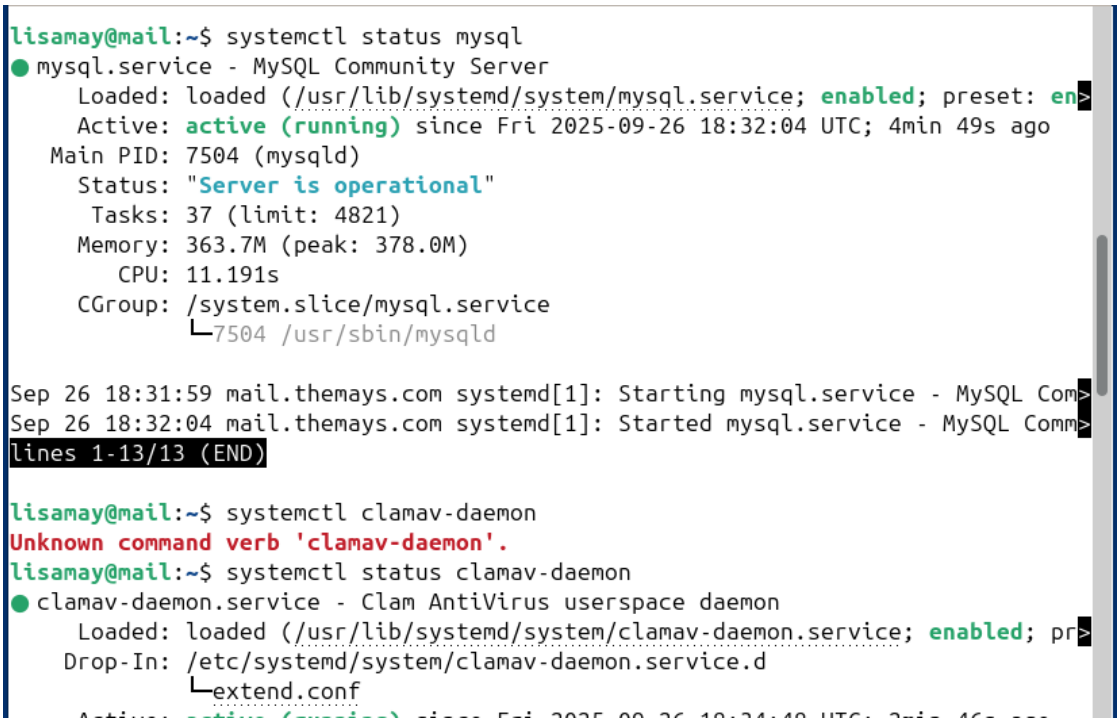


Figure 5- Status of MySQL and Clamav

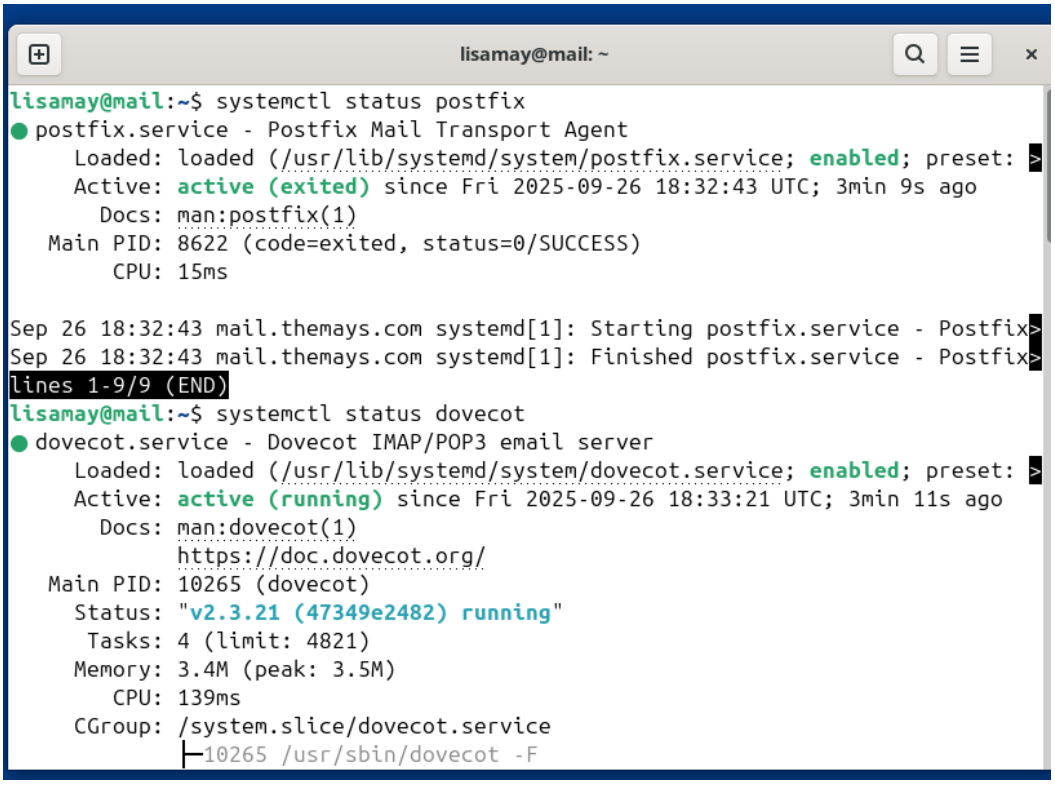


Figure 6- Status of Postfix and Dovecot

Part 3: Configuring MySQL and Connecting it with Postfix

To manage virtual domains and users, MySQL was configured and integrated with Postfix. A database named ***mailserver*** was created, along with the following tables: ***virtual_domains, users***, and ***aliases***. These tables will ensure that domain routing works properly, users can authenticate through the database, and aliases handle any mail forwarding or redirection.

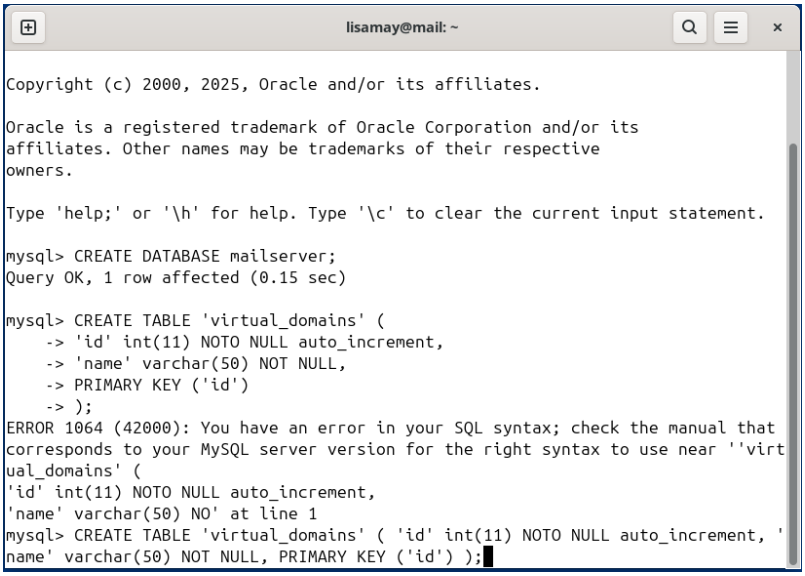


Figure 7 - DB creation and Virtual Domain

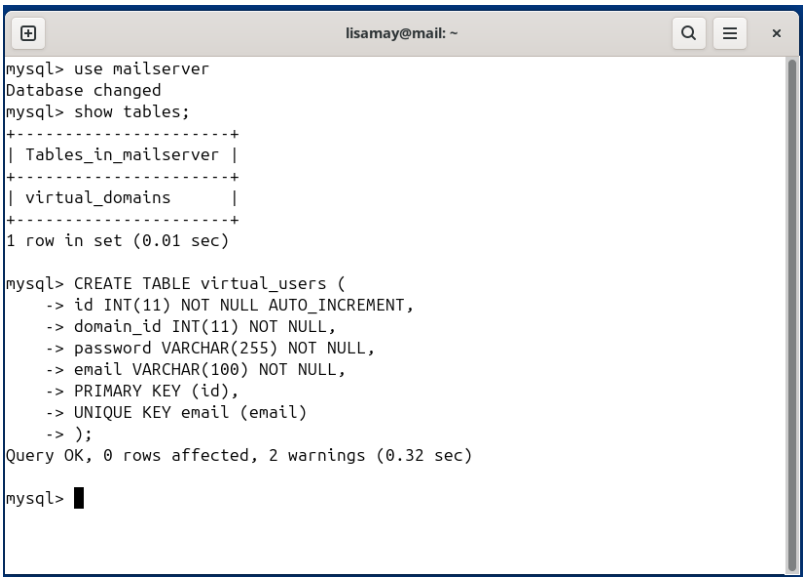


Figure 8- Table for Virtual Users

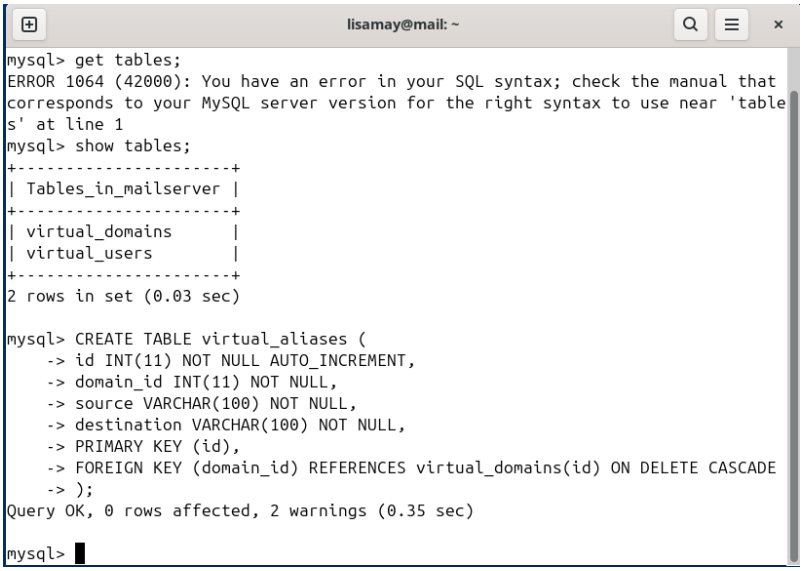


Figure 9 - Table for Virtual Aliases

Afterwards, a user was created for the purpose of interacting with the database. Doing so will allow Postfix to query MySQL for information about the domain, users, and aliases. Without a user, it would not be able to connect to the mail server database to query or verify anything.

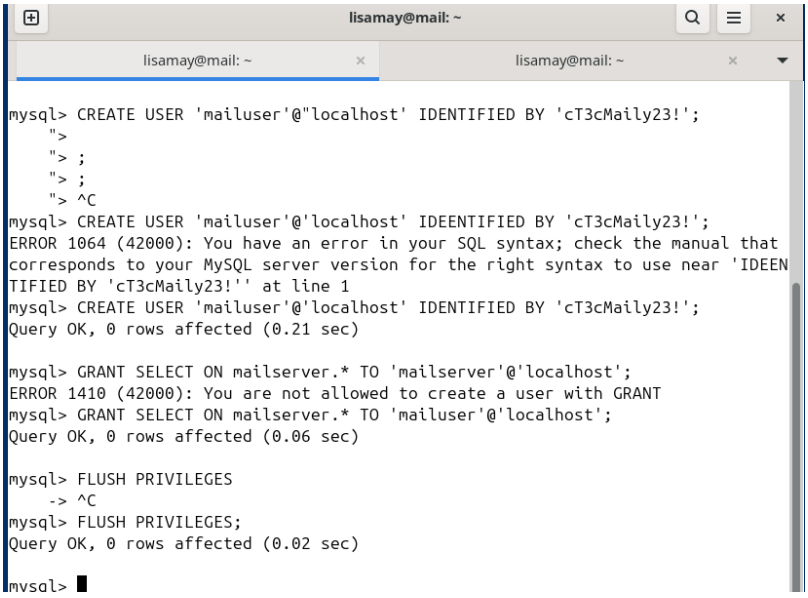


Figure 10 - User creation

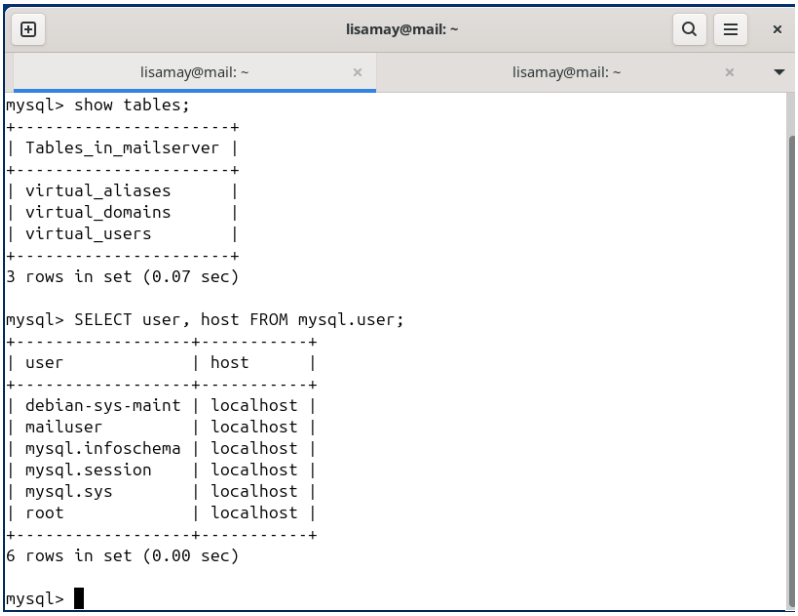
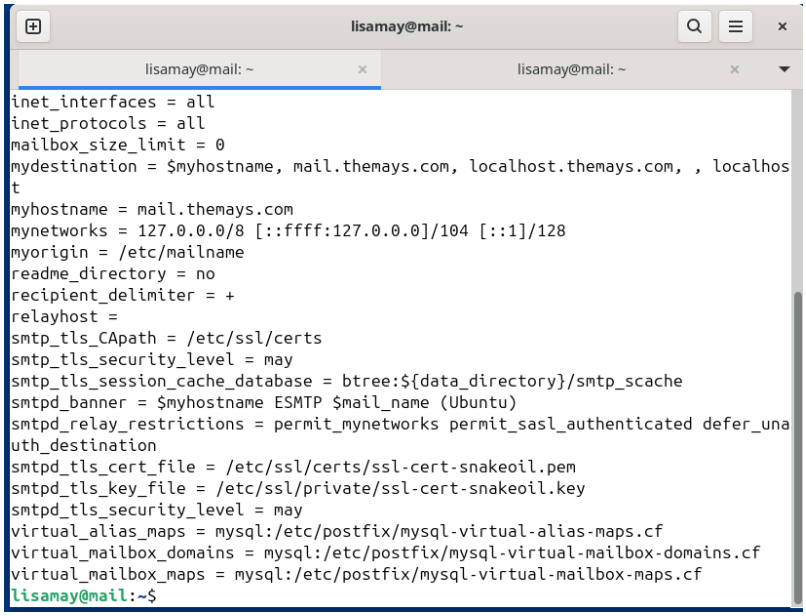
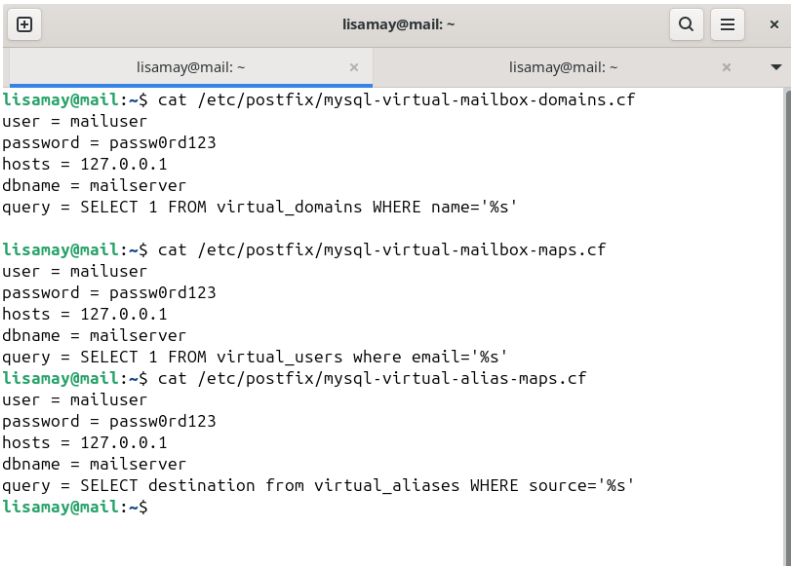


Figure 11 - Tables and Users

Part 4: Configuring Postfix Using Postconfig Command

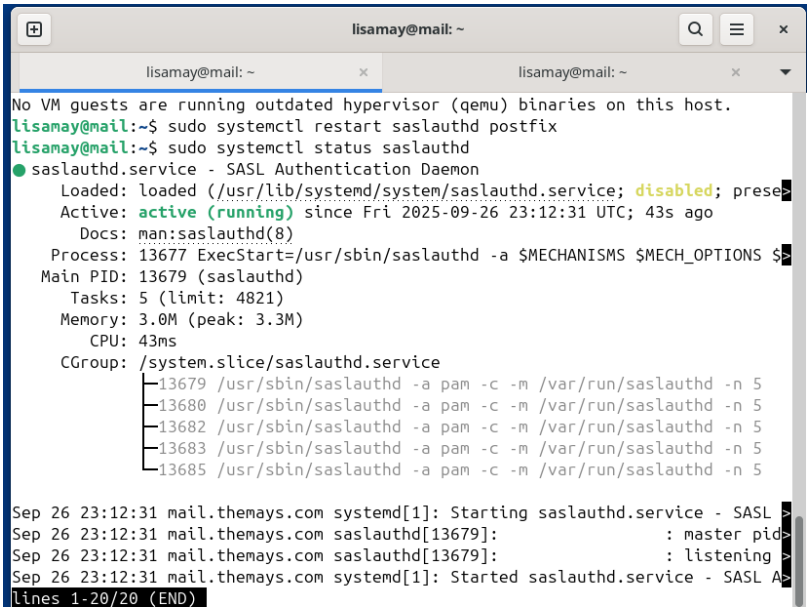
To configure Postfix to handle virtual domains and users, the ***postconf*** command was used to point Postfix to MySQL lookup files. These files contain the queries and credentials needed to pull domain, user, and alias data from the mailserver database.





Part 5: Configuring SMTP AUTH (SASLAUTHD and MySQL)

Enabling SMTP authentication prevents unauthorized users from sending mail through the server. Without SMTP authentication, unwanted mail, such as spam, may get through. This will require users to sign in before they are able to send mail. If the user does not have valid credentials, they will not be able to send mail through the server.



Future Work

This project builds a solid foundation for learning how to build a virtual mail server using a Linux based system. But there are still a number of opportunities for further research and advancement. This could include incorporating advanced threat protection in systems. Maybe implementing AI to help with spam and virus filtering. Especially at universities since college students are targeted frequently. Email systems automatically have banners that alert you saying this email originated outside of the organization. But those banners are applied to almost all of student's emails. So, students tend to disregard those messages. The software is also not accurate when it comes to categorizing or filtering out malicious emails. Students are often misled by emails focused on refund checks and financial aid. More research could be done to help prevent these types of attacks, so students won't even see these types of emails. Then AI models could also be incorporated to categorize emails based on the user's interest. This would reduce clutter and focus on important messages in the user's email.

Conclusion

With the help of essential components like Postfix, Dovecot, MySQL, Amavis, and ClamAV, in this project, we successfully deployed and configured a virtual mail server on a Linux Ubuntu platform, guaranteeing reliable mail delivery and security. Through practical troubleshooting and system integration, our team gained important real-world experience in user authentication, virtual domain management, and virus and spam prevention. This work not only achieves important technical goals but also emphasizes the growing significance of virtual mail servers in the current digital communication.

References

KHAJI, F. A. ., POTLURI, S. V. ., & KAKELLI, A. K. . (2021). A Performance Analysis of Virtual Mail Server on Type-2 Hypervisors. *Walailak Journal of Science and Technology (WJST)*, *18*(13), Article 9845 (10 pages). https://doi.org/10.48048/wjst.2021.9845

Mohindroo, Sanjay K. “A Journey through Time: The History of Email SystemsA Journey through Time: The History of Email Systems.” *Medium*, Oct. 2023, medium.com/@sanjay.mohindroo66/a-journey-through-time-the-history-of-email-systemsa-journey-through-time-the-history-of-email-4efc8b3d2816.

“What Is a Mail Server?” *Cloudflare.com*, 2023, www.cloudflare.com/learning/email-security/what-is-a-mail-server/.