Network Services Report

Haji Akhundzada[1] and Arzuman Hasanov[1]

[1]UFAZ French Azerbaijani University, Baku, Azerbaijan

May 19, 2024

Abstract

This paper describes a user-friendly, safe, and efficient email system that meets the needs of modern email communications while retaining centralized control over user management and data integrity. By combining these technologies, businesses may create a secure, scalable, and effective textitemail infrastructure that offers secure communication, centralized management, and dependable email distribution. LDAP Account Manager (LAM) is a web-based administrative tool that manages directory entries. The LAM is built around a unified user administration tool that maintains entries in a LAM directory.

1 Network Topology

The network topology for this project is designed to ensure secure and efficient communication between various components. Below is a detailed representation of the network topology:
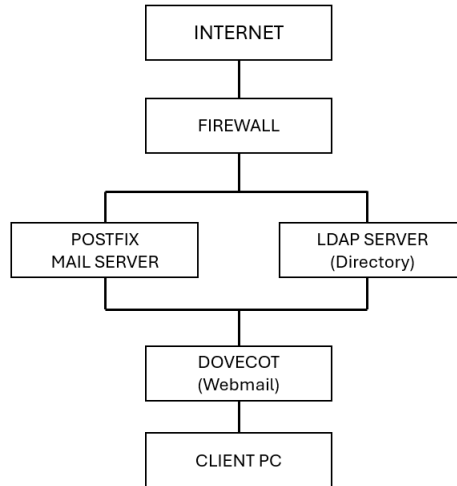
This email system architecture diagram shows how emails travel from the internet, through a firewall for security, to the Postfix mail server for processing. The LDAP server manages user information, Dovecot enables webmail access, and ultimately, emails are delivered to the client's PC.
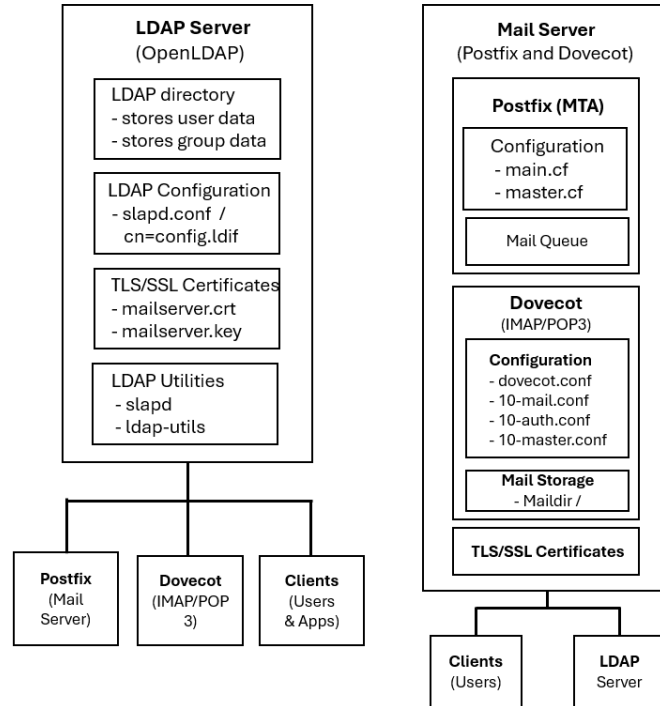
Figure 1: Network Topology

Figure 2: LDAP and Mail Server Architecture

2 Installation and Configurating steps

2.1 Install LDAP Server

Install LDAP Server (OpenLDAP):
Use your Linux distribution's package manager to install OpenLDAP. On Ubuntu, you can run:

```
sudo apt update
sudo apt install slapd ldap-utils
```

2.1.1 Configure LDAP Server

During installation, you'll be prompted to set up an initial LDAP configuration. Choose a domain name (e.g., ufaz.az) and an organization name (e.g., ufaz Corp). Set the LDAP administrator password. During installation, you need to choose the following options :

- Omit openldap server configuration : **No**
- DNS domain name : **ufaz.lab**
- Administrator password : **your secret passwd**

- Database backend to use : **MDB**
- Do you want the database to be removed when slapd is purged?: **No**
- Move old database : **Yes**

You can confirm that your installation was successful using the command '**slapcat**' to output **slapd** database contents.

2.1.2   LDAP client configuration

```
apt install libnss-ldapd
```

Manage your configuration with respect to your domain :

– **LDAP server's URI**: `ldap://mail.ufaz.lab`

– **Suffix**: `dc=ufaz,dc=lab`

Edit the `/etc/ldap/ldap.conf` file, if it's not done, uncomment and update the **BASE** and **URI** variables. Execute the following command and enable **'Create home directory on login'**.
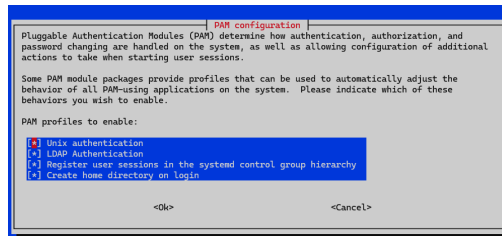
```
pam-auth-update
```


Figure 3: PAM Configuration

Then you reconfigure the **libnss-ldapd** to enable **'passwd, group, shadow'**.
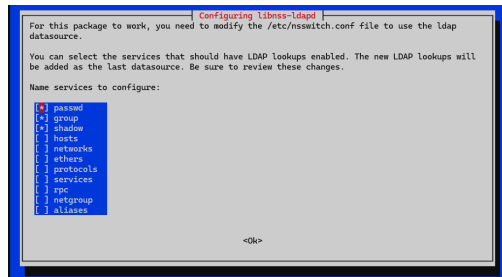
```
dpkg-reconfigure libnss-ldapd
```


Figure 4: libnss-ldapd Configuration

The last configuration is to update the `/etc/pam.d/common-session` update the following line :
Add '`skel=/etc/skel`' and '`umask=022`' end of the '`session optional`'. Atfer the all configurations are done; restart the service **'libnss-ldapd'**.

```
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session [success=ok default=ignore]     pam_ldap.so minimum_uid=1000
session optional        pam_systemd.so
session optional        pam_mkhomedir.so skel=/etc/skel umask=022
# end of pam-auth-update config
```

Figure 5: common-session update

```
systemctl restart nslcd
systemctl restart nscd
```

2.2 Installing Postfix

```
apt-get install postfix mailutils
```

2.2.1 Configure Postfix for LDAP

Postfix was already using the **"Maildir"** format. It is thus set with the home **mailbox = Maildir/** parameter in **'/etc/postfix/main.cf'**. Open **main.cf** file and make the following changes in it.

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.ufaz.lab
mydomain = ufaz.lab
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.ufaz.lab, localhost.ufaz.lab, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
home_mailbox = Maildir/
                        [ Read 49 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File   ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

Figure 6: Configuring main.cf

- To check errors use : **postconf −n**
- Restart the service with : **systemctl restart postfix**
- Check if it works : **systemctl status postfix**
- Be sure that is the wright process : **netstat −tlpn**

2.3 Set Up Dovecot for Webmail

```
apt-get install dovecot-imapd dovecot-core
```

2.3.1 Configure Dovecot

All Dovecot configuration files are present in the **'/etc/dovecot/'** directory

- In `/etc/devcot/devcot.conf` file:
  uncomment: `listen = *, ::`
- In the `/etc/dovecot/conf.d/10-mail.conf` file:

  - `mail_location = maildir:~/Maildir`
    (uncomment this line and comment on the mbox line)

- In the `/etc/dovecot/conf.d/10-auth.conf` file:
  Update: `disable_plaintext_auth = no`
  Change: `auth_mechanisms = plain login`
- In the `/etc/dovecot/conf.d/10-master.conf` file:
  Search: *'Postfix smtp-auth'* Add the following changes or uncomment

```
  unix_listener auth-userdb {
#  unix_listner /varspool/postfix/private/auth {
#    mode = 0666
#    user = postfix
#    group = postfix
#    }
  }

  #Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }

  # Auth process is run as this user.
  #user = $default_internal_user
}
```

Figure 7: Configuring /etc/dovecot/conf.d/10-master.conf

- Restart the service : **systemctl dovecot restart**
- Check if it has the wright process : **netstat -nlpn**

2.4 Obtain SSL/TLS Certificates

Generate Self-Signed Certificates (for Testing). If you don't have SSL/TLS certificates from a trusted CA (Certificate Authority), you can generate self-signed certificates for testing purposes:

```
sudo openssl req −x509 −nodes −days 365 −newkey rsa:2048−
keyout/etc/ssl/private/mailserver.key −out
/etc/ssl/certs/mailserver.crt
```

2.4.1 Configure LDAP Server with TLS

1. Edit the LDAP server configuration (/etc/ldap/slapd.conf or /etc/ldap/slapd.d/cn=config.ldif) to enable TLS.
2. Specify the paths to your SSL/TLS certificate (TLSCertificateFile) and private key (TLSCertificateKeyFile).
3. Ensure that the LDAP server listens on the LDAPS (LDAP over TLS) port (ldaps://).

2.4.2 Configure Postfix with TLS

Edit Postfix configuration file (/etc/postfix/main.cf) to enable TLS

```
smtpd_tls_cert_file = /etc/ssl/certs/mailserver.crt
smtpd_tls_key_file = /etc/ssl/private/mailserver.key
smtpd_use_tls = yes
smtpd_tls_security_level = may
```

2.4.3 Configure Dovecot with TLS

Edit Dovecot configuration file (/etc/dovecot/conf.d/10-ssl.conf) to enable TLS.

```
ssl = yes
ssl_cert = </etc/ssl/certs/mailserver.crt
ssl_key = </etc/ssl/private/mailserver.key
```

2.4.4 Restart Services and Test

```
sudo systemctl restart slapd
sudo systemctl restart postfix
sudo systemctl restart dovecot

openssl s\_client −connect mail.ufaz.lab:636
openssl s\_client −connect mail.ufaz.lab:25 −starttls smtp
openssl s\_client −connect mail.ufaz.lab:993
```

3   Results and tests
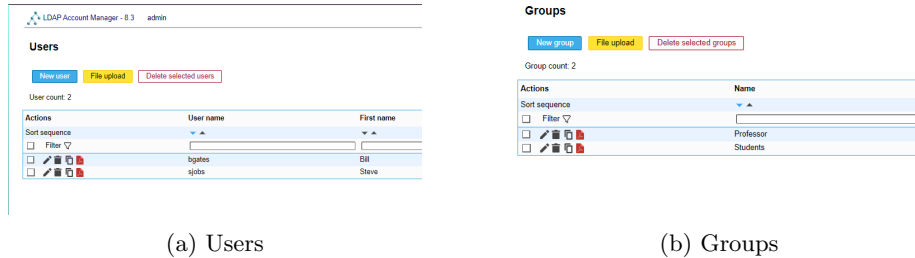
(a) Users   (b) Groups

Figure 8: LDAP

LDAP Account Manager (LAM) is a web-based administration tool for managing entries stored in an LDAP directory. It provides a user-friendly interface for managing LDAP entries, making it easier to handle users, groups, and other directory objects. In LDAP Account Manager, We have two users: Bill Gates and Steve Jobs. Bill Gates is a student, and Steve Jobs is a professor.
As you can see in the picture, there is a user named 'bgates' linking Bill Gates and

Figure 9: Users in Ubuntu server

another user linking Steve Jobs. In addition, it is possible to switch the user from the local user 'user' to 'bgates' within the system. Similarly, the process is the same for Steve Jobs. You can switch the user from the local user 'user' to 'sjobs' for Steve Jobs as well.

To test your server, send an email to the local user (user). To check if the server has sent your mail, use the mail queue, enter this command : `mailq`

Figure 10: Sending test mail

Now, if the server has sent your message correctly, the local user must receive it. Enter the local user session; then you can access the 'Maildir/' directory in 'new/' directory and read your new email.

Figure 11: Mail attachment

To send mail to the new users, you connect with **'nc' or 'telnet'** to your postfix server. If these applications are not installed, you do it with `apt-get install`.

```
sudo apt-get install netcat telnet
```


Figure 12: Sending email with Netcat

Troubleshooting
If you encounter any issues, check the **'Postfix'** and **'Dovecot'** logs for detailed error messages:

```
sudo tail -f /var/log/mail.log
sudo tail -f /var/log/dovecot.log
```

To verify that the email delivery is working correctly, follow these steps to check the `~/Maildir/new/` folder for received emails. This guide assumes you have successfully sent an email with the subject 'Hello Lab.'

Figure 13: Displaying the message

RainLoop is a web-based email client designed to provide a fast, modern, and user-friendly interface for accessing and managing email accounts.
Run the following command in Ubuntu to install Rainloop.

```
apt-get install php8.3 libapache2-mod-php8.3
php8.3-curl php8.3-xml curl apache2
```

In the `var/www/html` folder move the `index.html` to `index.html.old`, and run the following command.

```
curl -sL https://repository.rainloop.net/installer.php
| sudo php
```
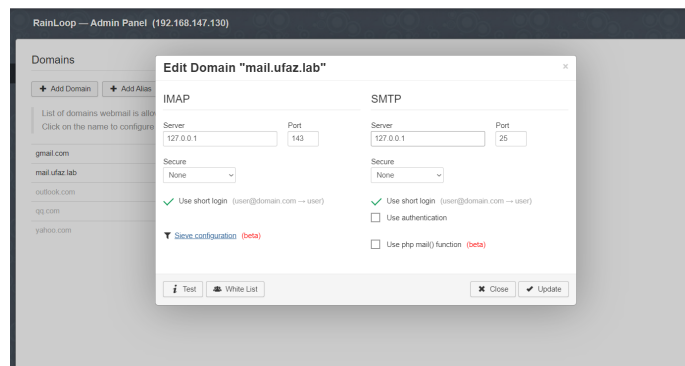

Figure 14: Rainloop

Access Rainloop Admin Panel:
Open a web browser and navigate to the RainLoop admin panel at http://yourip/?admin or http://localhost/?admin. In this situation **'yourip' = '192.168.147.130'**.

- Default login: **admin**
- Default password: **12345**

Change the default admin password immediately after logging in for the first time.

9

4 Conclusion

Creating an email system with Postfix, Dovecot, and LDAP requires numerous steps to provide efficient and secure email handling, user authentication, and centralized user management.

Postfix is the Mail Transfer Agent, which sends and receives emails, integrates with LDAP to precisely route and deliver emails, and uses Dovecot for SASL authentication. Dovecot serves as the IMAP and POP3 server, ensuring secure mailbox access, managing user authentication with LDAP, and enabling webmail access. LDAP is a centralized directory service that stores and manages user account information, mail aliases, and authentication data, guaranteeing consistency throughout the system. Throughout the installation and setup process, it is critical to verify that each component is properly configured and integrated. Configuring LDAP entails installing OpenLDAP, ensuring proper client settings, and enabling TLS for safe connection. Setting the proper parameters for mail delivery and authentication is required when configuring Postfix. Dovecot must be configured to offer secure mailbox access while integrating seamlessly with Postfix and LDAP.

Furthermore, getting and setting SSL/TLS certificates is critical for ensuring secure connection between clients and the server. Sending and receiving emails, checking good operation, and using tools like RainLoop to create a user-friendly webmail interface are all part of the setup testing process.

Contact Information

If you have any questions or need further assistance, please feel free to reach out:

- **Email: Send email to us:** h.akhundzada@ufaz.az **or** a.hasanov@ufaz.az
- **GitHub:** haJye **or** arzuman-hasanov