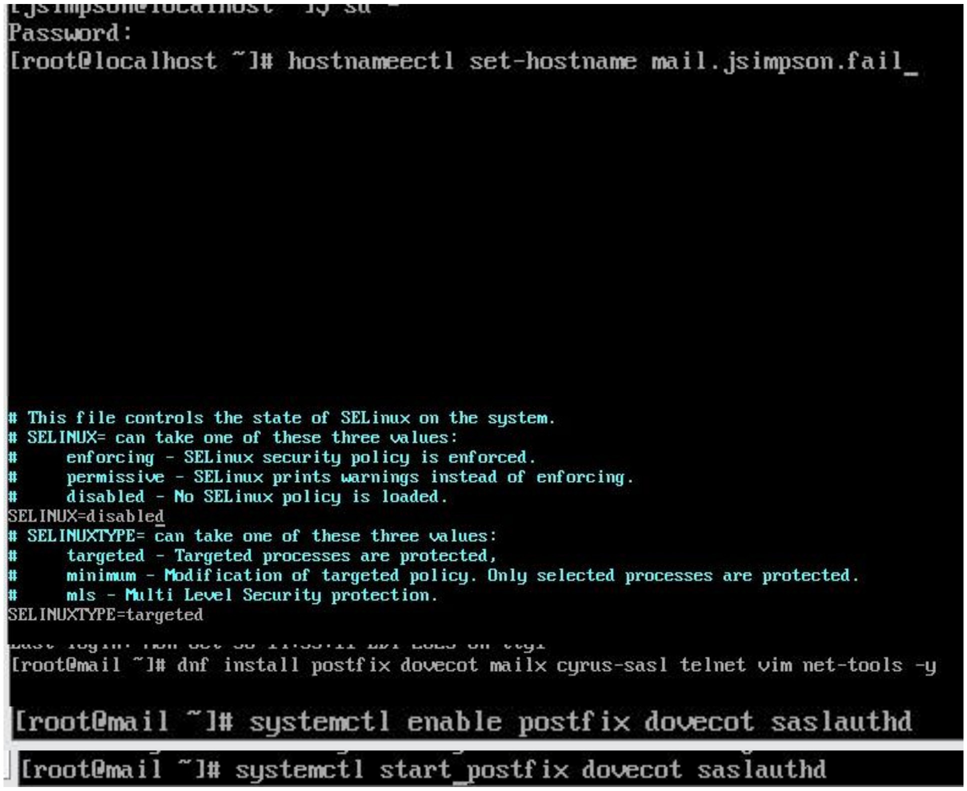
OVERVIEW:

The purpose of this lab was to install and configure an email server using Postfix and Dovecot, enabling users on the system to communicate with each other via email. I started by installing both Postfix and Dovecot, which handle sending and receiving emails, respectively. After setting up the server, I created a second user account to test communication between the two accounts. I also focused on securing the server by ensuring that traffic was encrypted, which helps protect sensitive email data during transmission. This lab helped me gain a better understanding of how to set up and manage a basic email server, a valuable skill for managing email services in real-world environments.

ANALYSIS:



```
[jsimpson@localhost ~]$ su -
Password:
[root@localhost ~]# hostnameectl set-hostname mail.jsimpson.fail_
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

```
[root@mail ~]# dnf install postfix dovecot mailx cyrus-sasl telnet vim net-tools -y
```

```
[root@mail ~]# systemctl enable postfix dovecot saslauthd
```

```
[root@mail ~]# systemctl start postfix dovecot saslauthd
```

The Following commands were changes

- Setup and Configure the POSTFIX service
- various settings (make copy and then edit /etc/postfix/main.cf)
- Uncomment line 94: myhostname = mail.jsimpson.fail
- Uncomment line 102: mydomain = jsimpson.fail
- Uncomment line 118: myorgin = $mydomain

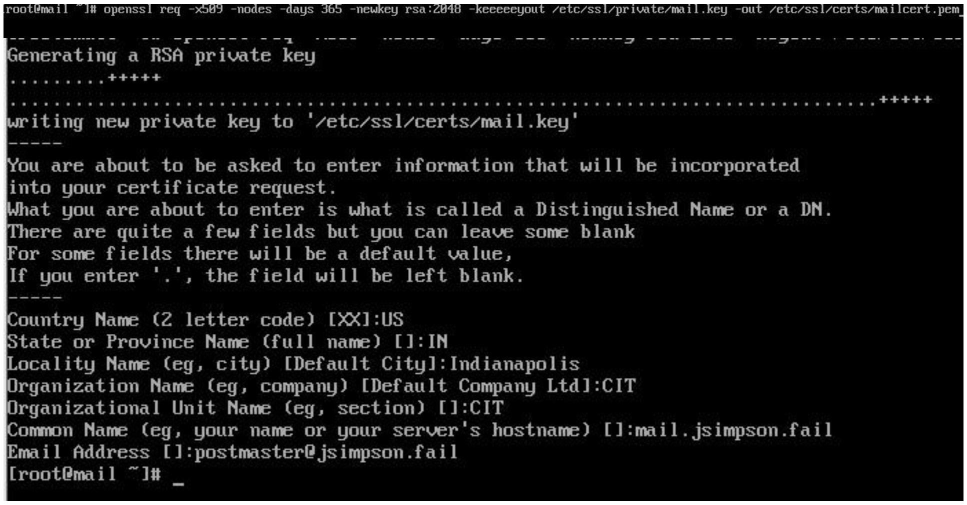
- Uncomment line 132: inet_interfaces = all
- comment line 135: inet_interfaces = localhost
- line 138: inet_protocols = all
- comment line 183: mydestination = $myhostname, localhost.$mydomain, localhost
- Uncomment line 184: mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
- Uncomment line 283: mynetworks = 127.0.0.0/8
- Uncomment line 438: home_mailbox = Maildir/
- Uncomment line 709: smtpd_tls_cert_file
- Uncomment line 715: smtpd_tls_key_file
- Uncomment line 720: smtpd_tls_security_level
- Uncomment line 725: smtpd_tls_CApath
- Uncomment line 731: smtpd_tls_CAfile Uncomment line 736: smtpd_tls_security_level At end of file add:
- smtpd_sasl_auth_enable = yes
- broken_sasl_auth_clients = yes smtpd_sasl_type = dovecot
- smtpd_sasl_path = private/auth
- smtpd_sasl_security_options = noanonymous
- smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated permit_inet_interfaces defer_unauth_destination

- add firewall rule to allow smtp
- firewall-cmd --permanent --add-service=smtp
- firewall-cmd --reload
- Setup and Configure the DOVECOT service

- make copy and then edit /etc/dovecot/dovecot.conf cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.bak dovecot.conf settings:
- Uncomment line 24: protocols = imap pop3 lmtp
- Uncomment line 30: listen = *
- edit files in /etc/dovecot/conf.d/ directory
- 10-mail.conf
- Uncomment line 24: mail_location = maildir:~/Maildir
- 10-auth.conf
- Uncomment line 10: disable_plaintext_auth = no
- line 100: auth_mechanisms = plain login
- 10-master.conf
- Uncomment line 107: unix_listener /var/spool/postfix/private/auth
- line 108: mode = 0660
- line 109: user = postfix

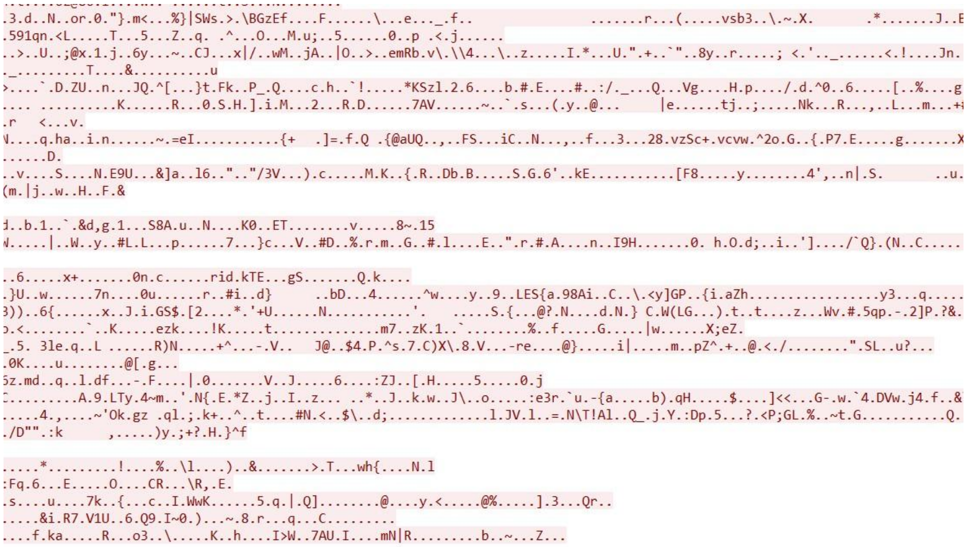
- line 110: group = postfix
- Uncomment line 111
- 10-ssl.conf
- Comment line 8: ssl = required
- line 9: ssl = no
- Comment lines 14 and 15: ssl_cert and ssl_key
- add host firewall rule to allow pop3 and imap
- firewall-cmd --permanent --add-service=pop3 firewall-cmd --permanent --add-service=imap firewall-cmd --reload

I created a certificate for the mail server to enable secure communication. After configuring the server with the certificate.



```
root@mail ~]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keeeeeyout /etc/ssl/private/mail.key -out /etc/ssl/certs/mailcert.pem_
Generating a RSA private key
..........+++++
.................................................................................+++++
writing new private key to '/etc/ssl/certs/mail.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]:US
State or Province Name (full name) []:IN
Locality Name (eg, city) [Default City]:Indianapolis
Organization Name (eg, company) [Default Company Ltd]:CIT
Organizational Unit Name (eg, section) []:CIT
Common Name (eg, your name or your server's hostname) []:mail.jsimpson.fail
Email Address []:postmaster@jsimpson.fail
[root@mail ~]# _
```

I sent a test email between the two user accounts.



```
.3.d..N..or.0."}.m<...%}|SWs.>.\BGzEf....F......\...e..._.f..            .......r...(.....vsb3..\.~.X.       .*.......J..E
.591qn.<L.....T...5...Z..q. .^...O...M.u;..5......0..p .<.j......
..>..U..;@x.1.j..6y...~..CJ...x|/..wM..jA..|O..>..emRb.v\.\\4...\..z.....I.*...U.".+..`"..8y..r.....; <.'.._......<.!....Jn.
._.........T....&.........u
>....`.D.ZU..n...JQ.^[...}t.Fk..P_.Q....c.h..`!.....*KSzl.2.6....b.#.E....#..:/._...Q...Vg....H.p..../.d.^0..6.....[..%....g
.... ..........K......R...0.S.H.].i.M...2...R.D......7AV......~..`.s...(.y..@...     |e......tj..;.....Nk...R...,..L...m...+
.r   <...v.
N....q.ha..i.n......~.=eI...........{+   .]=.f.Q .{@aUQ..,..FS...iC..N...,..f...3...28.vzSc+.vcvw.^2o.G..{.P7.E.....g.......X
......D.
..v....S....N.E9U...&]a..16.."..."/3V...).c.....M.K..{.R..Db.B.....S.G.6'..kE...........[F8.....y........4',..n|.S.       ..u.
(m.|j..w..H..F.&

d..b.1..`.&d,g.1...S8A.u..N....K0..ET........v.....8~.15
N.....|..W..y..#L.L...p......7...}c...V..#D..%.r.m..G..#.l....E..".r.#.A....n..I9H.......0. h.O.d;..i..'].../`Q}.(N..C.....

..6.....x+.......0n.c......rid.kTE...gS.......Q.k....
.}U..w......7n....0u......r..#i..d}      ..bD...4......^w....y..9..LES{a.98Ai..C..\.<y]GP..{i.aZh................y3...q.....
3))..6{......x..J.i.GS$.[2....*.'+U......N...........'.    .....S.{...@?.N....d.N.} C.W(LG...).t..t....z...Wv.#.5qp.-.2]P.?&.
b.<........`..K.....ezk....!K.....t..............m7..zK.1..`........%..f.....G.....|w......X;eZ.
_.5. 3le.q..L ......R)N.....+^...-.V..   J@..$4.P.^s.7.C)X\.8.V...-re....@}.....i|.....m..pZ^.+..@.<./........".SL..u?...
.0K....u........@[.g...
5z.md..q..l.df...-.F....|.0.......V..J.....6....:ZJ..[.H.....5.....0.j
C.........A.9.LTy.4~m..'.N{.E.*Z..j..I..z... ..*..J..k.w..J\..o.....:e3r.`u.-{a.....b).qH.....$....]<<...G-.w.`4.DVw.j4.f..&
.....4.,....~'Ok.gz .ql.;.k+..^..t....#N.<..$\..d;.............l.JV.l..=.N\T!Al..Q_.j.Y.:Dp.5...?.<P;GL.%..~t.G...........Q.
./D"".:k       ,.....)y.;+?.H.}^f

.....*.........!....%..\l....)..&.......>.T...wh{....N.l
:Fq.6...E.....O....CR...\R,.E.
.s....u....7k..{...c..I.WwK......5.q.|.Q]........@....y.<.....@%.....].3...Qr..
.....&i.R7.V1U..6.Q9.I~0.)...~.8.r...q...C.........
....f.ka.....R...o3..\.....K..h....I>W..7AU.I....mN|R.........b..~...Z...
```

To verify the encryption, I used Wireshark to capture the network traffic and observed that the email data was indeed encrypted, ensuring secure transmission. This step confirmed that the server was properly set up to handle encrypted email communication, adding an extra layer of security to the email server configuration.