**Mail Server Configuration Scripts and Commands**

**1. Installing and Configuring Postfix**

**Installing Postfix**

sudo dnf update -y

sudo dnf install postfix -y

sudo systemctl start postfix

sudo systemctl enable postfix

sudo systemctl status postfix

**Basic Postfix Configuration**

Edit the configuration file:

sudo nano /etc/postfix/main.cf

Modify the following parameters:

myhostname = mail.example.com

mydomain = example.com

myorigin = $mydomain

**Configuring Relay Host for AWS SES**

relayhost = [email-smtp.us-east-1.amazonaws.com]:587

smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_sasl\_security\_options = noanonymous

smtp\_use\_tls = yes

Create the password file:

echo "[email-smtp.us-east-1.amazonaws.com]:587 username:password" | sudo tee /etc/postfix/sasl\_passwd

sudo postmap /etc/postfix/sasl\_passwd

sudo chmod 600 /etc/postfix/sasl\_passwd /etc/postfix/sasl\_passwd.db

sudo systemctl restart postfix

**Testing Postfix with Thunderbird**

Install Thunderbird:

sudo dnf install thunderbird -y

Send a test email:

echo 'Test Email from Postfix' | mail -s 'Test Email' user@example.com

**2. Managing Mail Domains and Users**

**Configuring Multiple Mail Domains**

Edit Postfix main configuration file:

sudo nano /etc/postfix/main.cf

Add the following line:

mydestination = $myhostname, localhost.$mydomain, localhost, example.com, example.net

**Adding New Users**

sudo useradd john

sudo passwd john

**Creating Mail Aliases**

Edit alias file:

sudo nano /etc/aliases

Add an alias:

sales: sales@example.net

Update the aliases database:

sudo newaliases

**Setting Up Maildir Format**

sudo nano /etc/postfix/main.cf

Add or modify:

home\_mailbox = Maildir/

**3. Security and Anti-Spam Measures**

**Enabling TLS Encryption**

smtpd\_use\_tls = yes

smtpd\_tls\_cert\_file = /etc/ssl/certs/your\_domain\_cert.pem

smtpd\_tls\_key\_file = /etc/ssl/private/your\_domain\_key.pem

**Installing and Configuring SpamAssassin**

sudo dnf install spamassassin -y

sudo systemctl enable --now spamassassin

Configure Postfix to use SpamAssassin:

content\_filter = smtp:[127.0.0.1]:10024

**Setting Up Fail2Ban for Brute Force Protection**

sudo dnf install fail2ban -y

sudo systemctl enable --now fail2ban

Edit configuration file:

sudo nano /etc/fail2ban/jail.local

Add Postfix protection:

[postfix]

enabled = true

port = smtp,ssmtp

filter = postfix

logpath = /var/log/mail.log

maxretry = 5

bantime = 3600

Restart Fail2Ban:

sudo systemctl restart fail2ban

sudo systemctl status fail2ban

**4. Monitoring and Troubleshooting**

**Checking Email Delivery Logs**

sudo tail -f /var/log/maillog

**Viewing the Mail Queue**

postqueue -p

**Flushing the Mail Queue**

sudo postqueue -f

**Testing Mail Server Connectivity**

telnet mail.example.com 25

**5. AWS SES Integration**

**Configuring Postfix for AWS SES**

Edit the main configuration file:

sudo nano /etc/postfix/main.cf

Add the SES SMTP settings:

relayhost = email-smtp.us-east-1.amazonaws.com:587

smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_sasl\_security\_options = noanonymous

smtp\_tls\_security\_level = encrypt

smtp\_tls\_CAfile = /etc/ssl/certs/ca-certificates.crt

**Setting Up SMTP Authentication**

Create authentication file:

echo "[email-smtp.us-east-1.amazonaws.com]:587 AWS\_ACCESS\_KEY\_ID:AWS\_SECRET\_ACCESS\_KEY" | sudo tee /etc/postfix/sasl\_passwd

sudo postmap /etc/postfix/sasl\_passwd

sudo chmod 600 /etc/postfix/sasl\_passwd /etc/postfix/sasl\_passwd.db

sudo systemctl reload postfix

**Sending a Test Email via AWS SES**

echo 'Test Email from Postfix using AWS SES' | mail -s 'Test Email' recipient@example.com

**Conclusion**

This document provides essential scripts and commands for setting up and managing a mail server using Postfix on Rocky Linux, securing it with TLS, SpamAssassin, and Fail2Ban, and integrating with AWS SES for scalable email management.