-Create admin user useradd postman -p P@ssw0rd

-Check /etc/sudoers.d or /etc/sudoers for visudo or NOPASSWD

-Add postman to sudoers file usermod -aG wheel postman

-ps or top to see running processes.

-Kill [PID] to kill process

-Check cron jobs /etc

-Verify permissions on postfix ls -la /etc/postfix

-list all installed packages rpm -qa | less

-View all users less /etc/passwd

-Check DNS nameserver vi /etc/resolv.conf

-should only be accessible by root store PASSWORDS /etc/shadow

-/etc/pam.d/passwd << add >> password required pam\_cracklib.so retry=3 minlen=8 minclass=4 maxsequence=3 maxrepeat=3

-chage -E YYYY-MM-DD {username} << date account is locked

-pam\_lastlog or lastlog displays last login for users from /var/log/lastlog and /var/log/wtmp

-config file for login section /etc/pam.d/login

- display the failed login attempts prior to last login session optional pam\_lastlog.so silent noupdate showfailed

-review active services systemctl list-units | grep service

-checking security updates yum check-update --security

-lsmod | grep kvm

-modprobe -r [module] remove module

-modprobe -a [module] add module

-lsof [library]

-update-crypto-policies to show active cryptographic functions.

-yum install usbguard

-usbguard generate-policy > /etc/usbguard/rules.conf

-systemctl enable --now usbguard

-usbguard list-devices

-usbguard allow-device [ID]

#WE need to make a SSL dir first

mkdir /etc/postfix/ssl

cd /etc/postfix/ssl

#To install openssl

yum -y install openssl

#Create cert and key

openssl req -x509 -nodes -newkey rsa:2048 -keyout server.key -out server.crt -nodes -days 365

#Install postfix

[dnf](https://www.server-world.info/en/command/html/dnf.html) -y install postfix

# :set number

#Use VI to get into config file

[vi](https://www.server-world.info/en/command/html/vi.html) /etc/postfix/main.cf

# line 95: uncomment and specify hostname

myhostname = mail.srv.world

# line 102: uncomment and specify domain name

mydomain = srv.world

# line 118: uncomment

myorigin = $mydomain

# line 135: change

inet\_interfaces = all

# line 138: change it if use only IPv4

inet\_protocols = ipv4

# line 183: add

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

# line 283: uncomment and specify your local network

mynetworks = 127.0.0.0/8,10.0.0.0/24

# line 438: uncomment (use Maildir)

home\_mailbox = Maildir/

# line 593: add

smtpd\_banner = $myhostname ESMTP

# add follows to the end

# limit an email size for 10M

message\_size\_limit = 10485760

# limit a mailbox for 1G

mailbox\_size\_limit = 1073741824

# SMTP-Auth settings

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

smtpd\_sasl\_security\_options = noanonymous

smtpd\_sasl\_local\_domain = $myhostname

#i'm not sure what the diff between permit\_auth\_destination,reject, and reject\_unauth\_destination for the time use the green.

smtpd\_recipient\_restrictions = permit\_mynetworks,permit\_auth\_destination, permit\_sasl\_authenticated, reject

smtpd\_recipient\_restrictions = permit\_sasl\_authenticated,permit\_mynetworks,reject\_unauth\_destination

smtp\_tls\_security\_level = may

smtpd\_tls\_security\_level = may

smtp\_tls\_note\_starttls\_offer = yes

smtpd\_tls\_loglevel = 1

smtpd\_tls\_key\_file = /etc/postfix/ssl/server.key

smtpd\_tls\_cert\_file = /etc/postfix/ssl/server.crt

smtpd\_tls\_received\_header = yes

smtpd\_tls\_session\_cache\_timeout = 3600s

tls\_random\_source = dev:/dev/urandom

#Postfix master conf file process

/etc/postfix/master.cf

#Change the following after smtp inet n – n – – smtpd line\

submission inet n - n - - smtpd

-o syslog\_name=postfix/submission

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_recipient\_restrictions=permit\_sasl\_authenticated,reject

-o milter\_macro\_daemon\_name=ORIGINATING

smtps inet n - n - - smtpd

-o syslog\_name=postfix/smtps

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_recipient\_restrictions=permit\_sasl\_authenticated,reject

-o milter\_macro\_daemon\_name=ORIGINATING

#Start and enable on boot-up

systemctl start postfix

systemctl enable postfix

#Config DIR postfix

/etc/postfix

/etc/postfix/main.configuration or /etc/postfix/main.conf

/etc/postfix/master.cf

#Important NOTES:

#myhostname declares the mail server’s hostname. Hostnames normally #have prefixes in them, like this:

myhostname = mail.sinisterriot.com

#mydomain declares the domain that is actually handling mail, like #this:

mydomain = sinisterriot.com

#mail\_spool\_directory declares the directory where mailbox files are #placed, like so:

mail\_spool\_directory = /var/mail

#mynetworks declares a list of trusted remote SMTP servers that can #relay through the server, like this:

mynetworks = 127.0.0.0/8, 168.100.189.0/28

smtpd\_client\_connection\_rate\_limit — The maximum number of connection attempts any client is allowed to make to this service per time unit (described below). The default value is 0, which means a client can make as many connections per time unit as Postfix can accept. By default, clients in trusted networks are excluded.

anvil\_rate\_time\_unit — This time unit is used for rate limit calculations. The default value is 60 seconds.

smtpd\_client\_event\_limit\_exceptions — Clients that are excluded from the connection and rate limit commands. By default, clients in trusted networks are excluded.

smtpd\_client\_message\_rate\_limit — The maximum number of message deliveries a client is allowed to request per time unit (regardless of whether or not Postfix actually accepts those messages).

default\_process\_limit — The default maximum number of Postfix child processes that provide a given service. This limit can be overruled for specific services in the master.cf file. By default the value is 100.

queue\_minfree — The minimum amount of free space in bytes in the queue file system that is needed to receive mail. This is currently used by the Postfix SMTP server to decide if it will accept any mail at all. By default, the Postfix SMTP server rejects MAIL FROM commands when the amount of free space is less than 1.5 times the message\_size\_limit. To specify a higher minimum free space limit, specify a queue\_minfree value that is at least 1.5 times the message\_size\_limit. By default the queue\_minfree value is 0.

header\_size\_limit — The maximum amount of memory in bytes for storing a message header. If a header is larger, the excess is discarded. By default the value is 102400.

message\_size\_limit — The maximum size in bytes of a message, including envelope information. By default the value is 10240000.

[vi](https://www.server-world.info/en/command/html/vi.html) /etc/postfix/main.cf

# 106 Uncomment

# Postfix smtp-auth

unix\_listener /var/spool/postfix/private/auth {

mode = 0660

user = postfix

group = postfix

}

#19 Uncomment IMAP login port

Port = 143

#22&23 Uncomment IMAPS login port

Port = 993

Ssl = yes

#40 Uncomment POP3 login

Port = 110

#43&44 Uncomment POP3S login

Port = 995

Ssl = yes

#50 Uncomment submission login

Port = 587

#73 Uncomment sets MAX IMAP (connections)

Process\_limit = 1024

#78 Uncomment sets MAX POP3 (connections)

Process\_limit = 1024

#83 Uncomment sets MAX SMTP submission (connections)

Process\_limit = 1024

# authentication config file

Vi /etc/dovecot/conf.d/10-auth.conf

# 40 Uncomment

Auth\_username\_chars =

# 100 Uncomment

Auth\_mechanisms = plain login

# mail conf file for dovecot

Vi /etc/dovecot/conf.d/10-mail.conf

#30 Uncomment

mail\_location = maildir:~/mail

# pop3 conf file

Vi /etc/dovecot/conf.d/20-pop3.conf

# 50 Uncomment

pop3\_uidl\_format = %08Xu%08Xv

# restart and enable on boot up

systemctl restart dovecot

systemctl enable dovecot