**SMTP Server:**

1. Harden POSTFIX with /etc/postfix/main.cf:
   1. # line 75: uncomment and specify hostname

myhostname = mail.srv.world

# line 83: uncomment and specify domain name

mydomain = srv.world

# line 99: uncomment

myorigin = $mydomain

# line 116: change

inet\_interfaces = all

# line 164: add

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

# line 264: uncomment and **specify your** local network

**mynetworks = 127.0.0.0/8, 10.0.0.0/24**

# line 419: uncomment (use Maildir)

home\_mailbox = Maildir/

# line 574: 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

**# for SMTP-Auth**

**smtpd\_sasl\_type = dovecot**

**smtpd\_sasl\_path = private/auth**

**smtpd\_sasl\_auth\_enable = yes**

**smtpd\_sasl\_security\_options = noanonymous**

**smtpd\_sasl\_local\_domain = $myhostname**

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

1. Ensure firewall allows smtp:
   1. Firewall-cmd --add-service=smtp --permanent
   2. Firewall-cmd --add-service=smtps --permanent
   3. Firewall-smd --reload

**Harden Dovecot with:**

1. Vim /etc/dovecot/dovecot.conf

# line 24: uncomment

protocols = imaps pop3s lmtp

# line 30: uncomment and change ( if not use IPv6 )

listen = \*

1. Vim /etc/dovecot/conf.d/10-auth.conf

# line 10: uncomment and change ( allow plain text auth )

disable\_plaintext\_auth = no

# line 100: add

auth\_mechanisms = plain login

1. Vim /etc/dovecot/conf.d/10-mail.conf

# line 30: uncomment and add

mail\_location = maildir:~/Maildir

1. Vim /etc/dovecot/conf.d/10-master.conf

# line 96-98: uncomment and add like follows

# Postfix smtp-auth

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

mode = 0666

user = postfix

group = postfix

}

1. Vim /etc/dovecot/conf.d/10-ssl.conf

# line 8: change

**ssl = yes**

# line 14,15: specify certificates, **ensure they are in correct directory**

ssl\_cert = </etc/pki/tls/certs/server.crt

ssl\_key = </etc/pki/tls/certs/server.key

1. Firewall:
   1. Firewall-cmd --add-service=imaps --permanent
   2. Firewall-cmd --add-service=pop3s --permanent
   3. Firewall-cmd --reload

**Mail log report**:

1. Yum install postfix-perl-scripts
2. Perl /usr/sbin/pflogsumm -d yesterday /var/log/maillog
   1. Generates log summary for yesterday
3. Yum --enablerepo+epel install awstats
4. Vim /etc/awstats/awstats.(hostname).conf

###awstats automatically creates the .conf file

# line 50: change

LogFile="/usr/share/awstats/tools/maillogconvert.pl standard < /var/log/maillog |"

# line 62: change

LogType=M

# line 122: comment out and add like follows

#LogFormat=1

LogFormat="%time2 %email %email\_r %host %host\_r %method %url %code %bytesd"

# line 848: change like follows

LevelForBrowsersDetection=0

LevelForOSDetection=0

LevelForRefererAnalyze=0

LevelForRobotsDetection=0

LevelForSearchEnginesDetection=0

LevelForKeywordsDetection=0

LevelForFileTypesDetection=0

LevelForWormsDetection=0

# line 966: change like follows

ShowMonthStats=UHB

ShowDaysOfMonthStats=HB

ShowDaysOfWeekStats=HB

ShowHoursStats=HB

ShowDomainsStats=0

ShowHostsStats=HBL

ShowRobotsStats=0

ShowEMailSenders=HBML

ShowEMailReceivers=HBML

ShowSessionsStats=0

ShowPagesStats=0

ShowFileTypesStats=0

ShowOSStats=0

ShowBrowsersStats=0

ShowOriginStats=0

ShowKeyphrasesStats=0

ShowKeywordsStats=0

ShowMiscStats=0

ShowHTTPErrorsStats=0

ShowSMTPErrorsStats=1

1. Vim /etc/httpd/conf.d/awstats.conf

# line 30: add IP range you allow to access

Require ip 10.0.0.0/24

1. Access at “http://(hostname)/awstats/awstats.pl