Elektronikus levelek vírus és SPAM szűrése

Postfix

A Postfix egy MTA (Mail Transfer Agent), mely szabadon elérhető az IBM Public License alatt. Eredetileg Wietse Venema kezdte el fejleszteni az IBM támogatásával Vmailer név alatt, de később nevet kellett változtatni, mivel az említett nevet már más termék használta, így született a Postfix név. Méltán híres teljesítményéről, biztonságosságáról, és igen széles körű konfigurálási lehetőségeiről, ideértve pl. akár LDAP alapú lookup-okat, és különböző spam/UCE szűrési lehetőségeket is. A Postfix fejlesztésénél fő szempont továbbá a "szép" kód, és a kompatibilitás más MTA-kkal, mely jelenti az RFC-k pontos betartását, vagy akár a sendmail-ből, illetve qmail-ből (pl:maildir támogatás) ismert adminisztrálási megoldásokkal való kompatibilitást, lehetővé téve a könnyű átállást Postfix-re.

AMaViS

Az AMaViS (A Mail Virus Scanner) egy illesztő program az MTA és a vírus szkenner között Linux/Unix környezetbe. Nagy előnye, hogy gyakorlatilag bármilyen MTA-val képes együtt dolgozni. Fejlesztése befejeződött, azonban számos fork létezik.

SpamAssassin

A SpamAssassin (SA) egy ún. "pontozásos" rendszerben működő levélszemét szűrő. Használatához át kell rajta hajtani a beérkező leveleket, és a SA különböző szempontok (trágár szavak, csupa nagybetű a tárgyban, nem azonosítható küldő, és egyéb spamra uta ló jelek) alapján pontozza a levél tartalmát, fejlécét, stb.

ClamAV

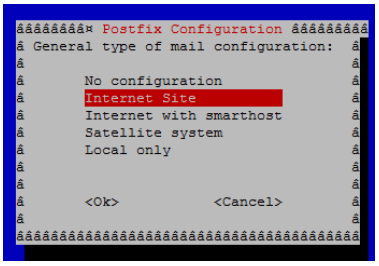
Teljes nevén Clam AntiVirus. GPL licensz alatt fejlesztett széles körben elterjedt antivírus programcsomag, ami egyaránt alkalmas email szerver forgalmának vírus-szűrésére és otthoni használatra. Gyakran (akár naponta többször) frissítik a vírus definíciós állományait.

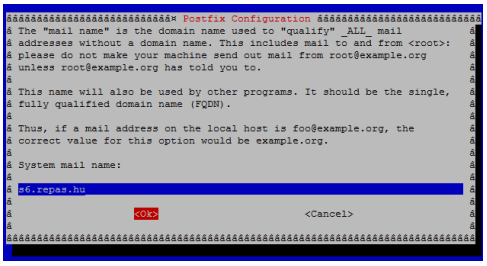
Telepítés

1. Telepítse fel a szükséges csomagokat:

```
apt-get install postfix spamassassin amavisd-new clamav clamav-daemon
libmailtools-perl fam libnet-dns-perl
```

2. A Postfix-et „Internet site”-ként konfigurálja, a rendszer neve pedig sX.repas.hu, ahol X az ön száma:





3. A /etc/hosts állományban adja meg a saját gépe adatait (185.143.48… sX.repas.hu sX):

```
127.0.0.1       localhost
80.64.68.106    debian6.sze.repas.hu    debian6
```

4. Állítsa be a ClamAV felhasználóját amavis csoportra:

```
adduser clamav amavis
```

5. Módosítsa az `/etc/default/spamassassin` állományt a következők szerint:

```
# Change to one to enable spamd

ENABLED=1

OPTIONS="--create-prefs --max-children 5 --helper-home-dir -s
/var/log/spamd.log"
```

6. Módosítsa az `/etc/spamassassin/local.cf` állományt a következők szerint:

```
required_score 1.9

use_bayes 1

bayes_auto_learn 1

bayes_ignore_header X-Bogosity

bayes_ignore_header X-Spam-Flag

bayes_ignore_header X-Spam-Status
```

7. Fordítsa le a SpamAssassin-t:

```
sa-compile
```

8. Indítsa újra a víruskeresőt és a spam szűrőt:

```
/etc/init.d/spamassassin restart

/etc/init.d/amavis restart

/etc/init.d/clamav-freshclam restart

/etc/init.d/clamav-daemon restart
```

9. A következő parancsok segítségével engedélyezze a Postfixnek az SASL authentikációt:

```
postconf -e 'smtpd_sasl_local_domain = $myhostname'

postconf -e 'smtpd_sasl_auth_enable = yes'

postconf -e 'broken_sasl_auth_clients = yes'

postconf -e 'smtpd_sasl_security_options = noanonymous'

postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,
permit_mynetworks, reject_unauth_destination'
```

10. Módosítsa a `/etc/postfix/master.cf` állományt a következők:

```
smtp      inet  n       -       -       -       -       smtpd
    -o content_filter=spamassassin



smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
  -o content_filter=spamassassin
```

11. Írja a `/etc/postfix/master.cf` állomány végére a következőket:

```
spamassassin unix -     n       n       -       -       pipe
      user=debian-spamd argv=/usr/bin/spamc -f -e
      /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

12. Telepítse fel az imap daemont:

```
apt-get install courier-maildrop courier-imap courier-imap-ssl
```

13. Hozza létre a felhasználók levelezési foldereit a felhasználó könyvtárában kiadott parancsokkal (Szükség esetén hozzon létre felhasználói fiókokat is, valamint figyeljen a tulajdonosra is!):

```
cd /home/student
maildirmake Maildir
maildirmake -f Sent Maildir
maildirmake -f Junk Maildir
maildirmake -f Trash Maildir
```

```
maildirmake -f Drafts Maildir

chown student.student * -R
```

14. Állítsa be a postfixet a Maildir használatára, majd indítsa újra:

```
postconf -e "home_mailbox = Maildir/"

postconf -e "mailbox_command = "

/etc/init.d/postfix restart
```

SASL authentikáció beállítása

Simple Authentication and Security Layer, több protokoll képes SASL illetve TLS alapján biztonságos kulcs alapú autentikációval titkosított csatornán kommunikálni. Főként levelező rendszerek használják.

Egy lista a teljesség igénye nélkül:

- IMAP
- LDAP
- IRC
- POP
- SMTP
- IMSP
- ACAP

1. Telepítse fel a szükséges csomagokat:

```
apt-get install libsasl2-modules sasl2-bin

adduser postfix sasl

dpkg-statoverride --add root sasl 710 /var/spool/postfix/var/run/saslauthd
```

2. Hozza létre a /etc/postfix/sasl/smtpd.conf állományt a következő tartalommal:

```
pwcheck_method: saslauthd

mech_list: PLAIN LOGIN
```

3. Készítsen egy másolatot a `/etc/default/saslauthd` állományról `/etc/default/saslauthd-postfix` néven:

```
cp /etc/default/saslauthd /etc/default/saslauthd-postfix
```

4. Módosítsa a régi állományt a következőek szerint:

```
START=yes
```

5. Módosítsa az új állományt a következőek szerint:

```
START=yes

DESC="SASL Authentication Daemon for Postfix"
```

```
NAME="saslauthd-postf"

OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

6. Indítsa újra a sasl és a postfix szolgáltatást:

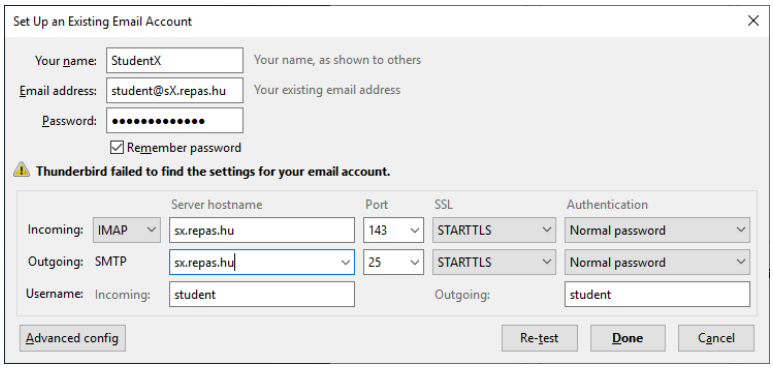
```
/etc/init.d/saslauthd restart

/etc/init.d/postfix restart
```

7. Próbálja ki, hogy működik-e az SASL-el kiegészített authentikáció:

```
testsaslauthd -u Felhasználó -p Jelszó
```

Működés vizsgálata

1. Állítsa be a levelező klienst. Pl. Thunderbird. (Figyeljen a titkosítás módjára és a portszámra!)



2. Küldjön magának egy e-mailt tetszőleges, de értelmes tartalommal, és eközben nézze a `/var/log/spamd.log` tartalmát. (less parancs és „F” billentyű) Hány pontot kapott az e-mail, és hány ponttól szűri ki a rendszer?
3. Küldjön magának egy e-mailt plain text formátumban a következő szavakkal a subjectben és a bodyban: „Reverses aging, Free investment , Auto email removal, Amazing stuff, Cash bonus, Viagra, SEX, Free, Money, Extra size, Cialis, Bonus, Earn, Million, Weight losing, Drug”, és eközben nézze a `/var/log/spamd.log` tartalmát. (less parancs és „F” billentyű) Hány pontot kapott az e-mail, és hány ponttól szűri ki a rendszer?