



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 adminisztrációs 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 szkennel 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 utaló jelek) alapján pontozza a levél tartalmát, fejlécét, stb.

ClamAV

Teljes nevén Clam AntiVirus. GPL licenz 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. Állítsa be a ClamAV felhasználóját amavis csoportra:

```
adduser clamav amavis
```

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

```
# Change to one to enable spamd  
ENABLED=1  
SAHOME="/var/lib/spamassassin/"  
OPTIONS="--create-prefs --max-children 5 --helper-home-dir ${SAHOME} -s  
${SAHOME}spamd.log"
```



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

```
use_bayes 1
bayes_auto_learn 1
bayes_ignore_header X-Bogosity
bayes_ignore_header X-Spam-Flag
bayes_ignore_header X-Spam-Status
```

5. 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
```

6. Módosítsa a `/etc/postfix/main.cf` állományt a következők szerint (#-ek eltávolítása, + utolsó két sor beírása):

```
smtps      inet  n       -       -       -       -       smtpd
-o syslog_name=postfix/smtps
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
-o milter_macro_daemon_name=ORIGINATING
-o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
-o content_filter=spamassassin
```

7. Írja a `/etc/postfix/main.cf` állomány végére a következőket:

```
smtp-amavis unix  -       -       n       -       2       smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
-o max_use=20

127.0.0.1:10025 inet  n       -       -       -       -       smtpd
```



```
-o content_filter=  
-o local_recipient_maps=  
-o relay_recipient_maps=  
-o smtpd_restriction_classes=  
-o smtpd_delay_reject=no  
-o smtpd_client_restrictions=permit_mynetworks,reject  
-o smtpd_helo_restrictions=  
-o smtpd_sender_restrictions=  
-o smtpd_recipient_restrictions=permit_mynetworks,reject  
-o smtpd_data_restrictions=reject_unauth_pipelining  
-o smtpd_end_of_data_restrictions=  
-o mynetworks=127.0.0.0/8  
-o smtpd_error_sleep_time=0  
-o smtpd_soft_error_limit=1001  
-o smtpd_hard_error_limit=1000  
-o smtpd_client_connection_count_limit=0  
-o smtpd_client_connection_rate_limit=0  
-o  
receive_override_options=no_header_body_checks,no_unknown_recipient_checks  
-o local_header_rewrite_clients=  
  
spamassassin unix -      n      n      -      -      pipe  
      user=debian-spamd argv=/usr/bin/spamc -f -e  
      /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

8. Telepítse fel az imap daemont:

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

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

```
maildirmake Maildir  
maildirmake -f Sent Maildir
```



```
maildirmake -f Junk Maildir  
maildirmake -f Trash Maildir  
maildirmake -f Drafts Maildir
```

SASL autentikáció 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 libsasl2-2 libsasl2-modules sasl2-bin openssl  
mkdir -p /var/spool/postfix/var/run/saslauthd  
chgrp sasl /var/spool/postfix/var/run/saslauthd/  
adduser postfix sasl
```

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 következők szerint:

```
START=yes
```

5. Módosítsa az új állományt a következők 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 autentikáció:

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

Működés vizsgálata

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

	Server hostname	Port	SSL	Authentication
Incoming: IMAP	s6.repas.hu	993	SSL/TLS	Normal password
Outgoing: SMTP	s6.repas.hu	465	SSL/TLS	Normal password

Username: Incoming: student Outgoing: student

2. Küldjön magának egy e-mailt tetszőleges, de értelmes tartalommal, és közben nézze a `/var/lib/spamassassin/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: „Viagra, SEX, Free, Money, Extra size, Cialis, Bonus, Earn, Million, Weight losing, Drug”, és közben nézze a `/var/lib/spamassassin/spamd.log` tartalmát. (less parancs és „F” billentyű) Hány pontot kapott az e-mail, és hány ponttól szűri ki a rendszer?