SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési Utasítás PASC – Postfix- Amavis – Spamassassin - Clamav

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 Third-party Vírus szkenner Linux/Unix környezetbe. Nagy előnye, hogy gyakorlatilag bármilyen MTA-val képes együtt dolgozni.

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 licensz alatt fejlesztett széleskörben elterjedt antivírus programcsomag, ami egyaránt alkalmas email szerver forgalmának vírus-szűrésére és otthoni használatra. Gyakran (akár naponta többször) frissítik a vírus definiációs állományait.

Telepítési útmutató (2011.02.14/Debian Squeeze)

Feltelepítjük a csomagokat

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

A clamav felhasználóját átállítjuk amavis group-ra

```
adduser clamav amavis
```

Létrehozzuk a spamassassin felhasználóját

```
adduser --system --home /var/lib/spamassassin --disabled-login --disabled-
password spamd
```

Spamassassin konfiguráció

Szerkesszük a **/etc/default/spamassassin** fájlt!

```
# Change to one to enable spamd
ENABLED=1

SAHOME="/var/lib/spamassassin/"
OPTIONS="--create-prefs --max-children 5 --helper-home-dir --username spamd
--helper-home-dir ${SAHOME} -s ${SAHOME}spamd.log"
```

Majd a **/etc/spamassassin/local.cf-et**

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

Ha ezzel megvagyunk újraindítjuk a vírus és spamszűrőket:

```
/etc/init.d/spamassassin restart
/etc/init.d/amavis restart
/etc/init.d/clamav-freshclam restart
/etc/init.d/clamav-daemon restart
```

Postfix konfiguráció

Szerkesszük a **/etc/postfix/main.cf** fájlt!

```
smtpd tls auth only = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom


mailbox_command = /usr/bin/maildrop
home_mailbox = Maildir/

smtpd sasl auth enable = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,
permit_mynetworks, reject_unauth_destination
broken_sasl_auth_clients = yes
smtpd sasl path = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = cyrus

content_filter = smtp-amavis:[127.0.0.1]:10024
```

Majd jöhet a master.cf (az alábbi szöveget a konfigurációs állomány végére kell beírni)
Először a következő sorokat kell kikommentezni:

```
smtps     inet  n       -       -       -       -       smtpd
  -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
```

```
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=spamd argv=/usr/bin/spamc -f -e
    /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

Ha ezzel megvagyunk fel kell telepítenünk az imap szolgáltatásért felelős daemon-okat!

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

(a következő parancsokat a userek $HOME könyvtárában kell kiadni!)

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

Autentikáció beállítás

SASL

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

Egy lista a teljesség igénye nélkül:

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

Telepítsük fel a hozzá tartozó csomagokat!

```
apt-get install postfix-tls 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
```

Majd a /etc/default/saslauthd fájlban a START=no-t yes-re állítani!

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

Probáljuk ki, működik-e a SASL réteggel kiegészített autentikáció!

```
fekete4:/home/root# testsaslauthd -u root -p labor
0: OK "Success."
fekete4:/home/root#
```

Következik a kulcsgenerálás

```
#mkdir /etc/postfix/ssl
#cd /etc/postfix/ssl/
```

Az smtpd.key legenerálásánál meg kell adnunk egy jelszó, melyet később a tanusítványok létrehozásánál meg kell adnunk, hogy hivatkozhassunk a kulcsra

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 1830 -in smtpd.csr -signkey smtpd.key -out
smtpd.crt
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
cp smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem
-days 1830
```

Már csak az IMAP protokollt kell SSL tanúsítvánnyal ellátni!

```
apt-get install courier-imap-ssl
cd /etc/courier
openssl req -new -x509 -nodes -out imapd.pem -keyout imapd.pem -days 1830
```

Ezzel meg is volnánk!

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

/etc/init.d/courier-imap-ssl restart
```

Teszteléshez használhatjuk a Mozilla Thunderbird programot, vagy Linux portját a Icedove-ot.