Qmail – Öreg ember, nem vén ember

Már nem is emlékszem pontosan mikor, talán még 1998-ban telepítettem először a Qmail-t. Noha sok év eltelt már azóta, de még ma is jól használható SMTP kiszolgálót írt D.J. Berstein. A legújabb funkciók (például DSN, TLS, …) némelyike ugyan hiányzik belőle, de az alapfeladatát, a levelek biztonságos továbbítását, még mindig ugyanolyan jól végzi.

Szerencsére a *Qmail* lelkes tábora különböző foltokat (***patch***) írt, amelyekkel felokosítható a program, hogy a jelen kor igényeinek is megfelelhessen. A támogatott ***RFC***-k listája a http://cr.yp.to/qmail.html címen olvasható. Ebben az írásban egy vírus- és spam védelemmel ellátott levelező kiszolgáló kialakítását mutatom be. Szükségünk lesz az ***ucspi-tcp*** csomagra, amely egy ***inetd*** alternatíva, illetve tartalmazza az ***rblsmtpd*** programot, amellyel feketelistákat (***RBL***) használhatunk. Ennek telepítése részletesen le van írva a http://cr.yp.to/ucspi-tcp/install.html címen.

Hogy a telepítés és a használat minél kényelmesebb legyen, néhány önkéntes elkészítette a ***netqmail-1.05*** csomagot, amelyben a gyári ***qmail-1.03*** szerepel néhány ajánlott folt társaságában. Töltsük ezt le a http://www.qmail.org/netqmail/ címről, majd telepítsük az *1. listában* látható parancsokkal, amelyek létrehozzák a szükséges felhasználókat és csoportokat, beállítják az alapértelmezett hosztnevet és azt a felhasználót, aki a ***root***, a ***postmaster*** és a ***MAILER-DAEMON*** leveleit olvassa. A telepítés részletei az ***INSTALL*** dokumentációban vannak.

A ***Qmail*** alapértelmezett könyvtára a ***/var/qmail***. Ha ezt módosítani akarjuk, akkor fordítás előtt szerkesszük a ***conf-qmail*** állományt, illetve ennek megfelelően módosítani szükséges az imént létrehozott felhasználók könyvtárait.

1. Lista A qmail telepítése

```
# a szükséges csoportok és felhasználók létrehozása
groupadd nofiles
useradd -g nofiles -s /nonexistent -d /var/qmail/alias alias
useradd -g nofiles -s /nonexistent -d /var/qmail qmaild
useradd -g nofiles -s /nonexistent -d /var/qmail qmaill
useradd -g nofiles -s /nonexistent -d /var/qmail qmailp
groupadd qmail
useradd -g qmail -s /nonexistent -d /var/qmail qmailq
useradd -g qmail -s /nonexistent -d /var/qmail qmailr
useradd -g qmail -s /nonexistent -d /var/qmail qmails

tar zxvf netqmail-1.05.tar.gz
cd netqmail-1.05
mkdir /var/qmail
./collate.sh

make setup check

# ez az FQDN nevünk
./config-fast mail.aaaa.hu

# bela kapja meg a postmaster, a MAILER-DAEMON és a root leveleit
cd ~alias
echo bela > .qmail-postmaster
echo bela > .qmail-mailer-daemon
echo bela > .qmail-root
chmod 644 ~alias/.qmail*
```

A ***Qmail*** indításához készítsük el a *2. Listában* látható ***/etc/rc.d/rc.qmail*** héjprogramot (***shell script***), amely elindítja mind a helyi levéltovábbítást, mind pedig a ***qmail-smtpd*** programot. A ***qmail-smtpd root*** felhasználóként fog futni, legfeljebb 100 (alapértelmezésben 40) konkurens kapcsolatot tud kiszolgálni, az ***sbl-xbl.spamhaus.org*** és a helyi ***rbl.aaaa.hu*** feketelisták adatbázisával veti össze a kliens IP-címét, illetve a ***syslog*** naplóba kerül minden üzenet. A ***softlimit*** paraméter után

megadott szám (20 M) a ***Qmail*** számára elérhető memória méretét korlátozza. Az eredeti értéket (2 M) azért növeltem meg, hogy a később ismertetett vírusellenőrzés se üsse be a fejét memória limitbe.
Ha ***Maildir*** formátumú postafiókot akarunk, akkor a */etc/rc.d/rc.qmail* állományban a cseréljük le a „*./Mailbox*” sztringet „*./Maildir/*”-re, és adjuk ki minden felhasználó nevében a

```
cd ~;/var/qmail/bin/maildirmake
➥Maildir
```

utasítást.
Ha mindent jól csináltunk, akkor a programot lefuttatva, a *3. Listában* felsorolt folyamatokat (***process***) láthatjuk. Ne felejtsünk el kedvenc ***Linux*** disztribúciónk valamelyik indító szkriptjében hivatkozni rá, például ***Slackware*** esetében a */etc/rc.d/rc.local* állományban.
A figyelmes olvasónak bizonyára feltűnt a `-x` kapcsoló után szereplő ***cdb*** fájl. Ezzel adhatjuk meg azt a hálózatot és/vagy ***IP***-címet, amelyek számára ***relay*** szolgáltatást nyújtunk.
A *4. listában* egy lehetséges megoldást láthatunk, amely a ***localhost*** illetve a 192.168.1.0/24 hálózat számára engedi a levél továbbítását, és amelyből a

```
tcprules /etc/tcp.smtp.cdb
➥/etc/tcp.smtp.tmp < /etc/
➥tcp.smtp
```

utasítással hozható létre a szükséges ***cdb*** állomány.
A ***Unix*** programok egy része a ***sendmail*** programot használja levélküldésre. A ***Qmail*** rendelkezik egy burkoló (***wrapper***) programmal, amelyet az

```
ln -s /var/qmail/bin/sendmail
➥/usr/lib/sendmail
```

és az

```
ln -s /var/qmail/bin/sendmail
➥/usr/sbin/sendmail
```

parancsokkal tehetünk például a ***pine*** számára elérhetővé.
Az *5. Listában* egy levél nyomát láthatjuk a naplóban. A bejegyzésből azt tudhatjuk meg, hogy sj@aaaa.hu 2765 byte hosszú levelet küldött a bela@mail.aaaa.hu címre. A levél a 219962 (ez valójában egy ***i-node*** száma) sorszámot kapta meg ***queue*** azonosítóként, ill. hogy a levél küldése sikeres volt.
Ha a levél küldője rajta van az ***RBL*** listáink valamelyikén, akkor az ***rblsmtpd*** program 451-es hibával elutasítja a levelet az ***RCPT TO*** fázisban, amint az a *6. Listában* is látható, ill. az esemény a naplóba is bekerül – lásd a *7. Listát*, az adott ***IP***-címhez tartozó ***TXT*** rekorddal együtt.

2. Lista A /etc/rc.d/rc.qmail tartalma

```
#!/bin/sh

QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=100
LOCAL=`head -1 /var/qmail/control/me`

exec /usr/local/bin/softlimit -m 20000000 \
    /usr/local/bin/tcpserver -v -R -l "$LOCAL" -x
/etc/tcp.smtp.cdb -c "$MAXSMTPD" \
        -u "$QMAILDUID" -g "$NOFILESGID" 0 25
➥/usr/local/bin/rblsmtpd -r sbl-xbl.spamhaus.org \
        -r rbl.aaaa.hu /var/qmail/bin/qmail-smtpd 2>&1 |
➥/var/qmail/bin/splogger smtpd 3 &

exec env - PATH="/var/qmail/bin:$PATH" qmail-start ./Mailbox
➥splogger qmail &
```

3. Lista Ezeknek a qmail programoknak kell futniuk

```
qmaild    8311  0.0  0.2   1356   292 pts/0    S    15:04   0:00
➥/usr/local/bin/tcpserver -v -R -l mail.aaaa.hu -x /etc/
➥tcp.smtp.cdb -c 100 -u 1000 -g 102 0 25 /usr/local/bin/
➥rblsmtpd -r rbl.aaaa.hu -r sbl-x
root      8312  0.0  0.3   1472   444 pts/0    S    15:04   0:00
➥/var/qmail/bin/splogger smtpd 3
qmails    2657  0.0  0.2   1500   360 pts/0    S    12:17   0:00
➥qmail-send
qmaill    2658  0.0  0.3   1468   440 pts/0    S    12:17   0:00
➥splogger qmail
root      2659  0.0  0.2   1468   304 pts/0    S    12:17   0:00
➥qmail-lspawn ./Mailbox
qmailr    2660  0.0  0.2   1464   304 pts/0    S    12:17   0:00
➥qmail-rspawn
qmailq    2661  0.0  0.2   1456   316 pts/0    S    12:17   0:00
➥qmail-clean
```

4. Lista A /etc/tcp.smtp fájl tartalma

```
192.168.1.:allow,RELAYCLIENT=""
127.:allow,RELAYCLIENT=""
```

Ha ***tinydns***-t használunk, a *8. Listában* szereplő bejegyzésekre lesz szükség.
A ***Qmail*** nem rendelkezik hagyományos konfigurációs állománnyal, hanem környezeti változók, ill. a */var/qmail/control* könyvtárban

5. Lista Egy levélhez tartozó naplóbejegyzések

```
Mar 21 14:25:30 aaa qmail: 1174519530.809151 new msg 219962
Mar 21 14:25:30 aaa qmail: 1174519530.809802 info msg 219962:
➥bytes 4769 from <sj@aaaa.hu> qp 2765 uid 1000
Mar 21 14:25:30 aaa qmail: 1174519530.837840 starting delivery
➥2: msg 219962 to local bela@mail.aaaa.hu
Mar 21 14:25:30 aaa qmail: 1174519530.838335 status: local 1/10
➥remote 0/20
Mar 21 14:25:30 aaa qmail: 1174519530.890881 delivery 2:
➥success: did_1+0+0/
Mar 21 14:25:30 aaa qmail: 1174519530.891472 status: local 0/10
➥remote 0/20
Mar 21 14:25:30 aaa qmail: 1174519530.891820 end msg 219962
```

6. Lista Az rblsmtpd elutasított egy spammert

```
220 rblsmtpd.local
HELO aaaa.hu
250 rblsmtpd.local
MAIL FROM: <sj@aaaa.hu>
250 rblsmtpd.local
RCPT TO: <sj@aaa.acts.hu>
451 spammer vagy
```

7. Lista Az rblsmtpd épp megfogott egy spammert

```
Mar 21 14:35:38 aaa smtpd:
➥1174520138.145382 rblsmtpd:
➥192.168.1.22 pid 2795: 451
➥spammer vagy
```

8. Lista DNS rekordok a tinydns-ben

```
+22.1.168.192.rbl.aaaa.hu:
➥127.0.0.2:1800
'22.1.168.192.rbl.aaaa.hu:
➥spammer vagy:1800
```

található egyszerű szöveges fájlok segítségével hangolhatjuk a működését, amelyek részletes leírása a http://www.lifewithqmail.org/lwq.html#config-files címen található. Ezek segítségével beállíthatjuk például

9. Lista A checkpassword telepítése

```
tar zxvf checkpassword-0.90.
➥tar.gz
cd checkpassword-0.90
echo cc -O2 -include
➥/usr/include/errno.h >
➥conf-cc
make setup check
```

virtuális domaineket, az üzenetek max. méretét, mennyi ideig várjon a távoli *SMTP* ügyfélre, a *HELO* paraméter értékét, stb.

POP3 szolgáltatás

A *Qmail* csomagban egy teljes értékű *POP3* démon (*qmail-popup*) is található, amely (csak) M*aildir* formátumú postafiókkal tud együtt működni. A használat előtt telepítsük a *checkpassword* programot, amelyet a http://cr.yp.to/checkpwd/install.html címről tölthetünk le, telepíteni pedig a *Berstein* programjainál megszokott, a *9. Listában* látható módon lehet.
A http://cr.yp.to/qmail/toaster.html címen egyéb jelszó ellenőrző programokat is találunk, amelyekkel – ha úgy kívánjuk – a *checkpassword* kiváltható.
Futtassuk a

```
tcpserver 0 110 /var/
➥qmail/bin/qmail-popup
➥mail.aaaa.hu /bin/
➥checkpassword /var/qmail/bin/
➥qmail-pop3d Maildir
```

utasítást, ahol 0 a root felhasználó numerikus azonosítója (*userid*), a 110 pedig a *POP3* szolgáltatás *TCP* portja. Ezután a levelező ügyfelek rögtön elérhetik postafiókjukat. Természetesen más *POP3* (sőt *IMAP4*, *webmail*, stb.) kiszolgáló is használható, ha úgy akarjuk. Szerencsére nem kell érvényes héjprogramot (*shell*) beállítani a csak *POP3* szolgáltatást használó felhasználók számára.

Statisztika

Egyetlen alkalmazás sem lehet meg kimutatások nélkül, amelyből kiderül, hogy ki, kinek, mikor és mennyit küldött. A *qmailanalog* program segítségével (http://cr.yp.to/qmailanalog.html) részletes statisztikát készíthetünk mindezekről.
Nézzünk meg először egy általános statisztikát a

```
grep qmail /var/log/maillog |
➥awk '{$1="";$2="";$3="";
➥$4="";$5="";print}' |
➥/usr/local/qmailanalog/bin/
➥matchup | /usr/local/
➥qmailanalog/bin/zoverall
```

parancs segítségével, amely a *10. Listához* hasonló eredményt ad, ahol láthatjuk a továbbított üzenetek számát, hogy abból mennyi volt sikeres, illetve sikertelen, meddig tartott átlagosan egy üzenet továbbítása, illetve a különböző késleltetések, méretek stb. is szerepelnek a jelentésben.
A *zsuids* parancs táblázatos formában mutat meg statisztikát az egyes felhasználókról, amint az a *11. Listában* látható.
A `zrecipients` parancs a címzettekről mutat meg összesítést, lásd a *12. Listát*.
A további parancsokról az előbbi web oldal közöl információkat.

Biztonság

Ma már egy magára valamit is adó levelező rendszernek biztosítania kell a vírusok- és spam elleni védelmet.
A *Qmail-Scanner* egy lehetséges megoldás, amelyet a http://qmail-scanner.sourceforge.net/ címről tölthetünk le. Az alkalmazás többféle vírusirtóval is együtt tud működni, például *Clamav, Sophos, McAfee*, stb. ill. a *SpamAssassin* spamszűrővel.

10. lista Általános információk a qmail futásáról

```
Completed messages: 4010
Recipients for completed messages: 3955
Total delivery attempts for completed messages: 3963
Average delivery attempts per completed message: 0.988279
Bytes in completed messages: 46955358
Bytes weighted by success: 46738103
Average message qtime (s): 0.582822

Total delivery attempts: 3963
  success: 3940
  failure: 15
  deferral: 8
Total ddelay (s): 2326.556067
Average ddelay per success (s): 0.590496
Total xdelay (s): 798.067730
Average xdelay per delivery attempt (s): 0.201380
Time span (days): 2.07719
Average concurrency: 0.00444682
```

11. Lista Az egyes felhasználói azonosítók tevékenysége

```
mess     bytes    sbytes    rbytes  recips  tries      xdelay  uid
   2       388       388       388       2      4    0.373292  0
  90    407842    338807    338807      63     67    4.335345  1000
   1       294       294       294       1      3    0.275610  1003
  10     41879         0     41879      10     10    0.763050  1006
   1      3496         0      3496       1      1    0.080386  1009
3593  42561854  42459009  42472581    3565   3565  733.164487  1010
```

12. Lista Statisztika címek szerinti bontásban

```
  sbytes  mess  tries  xdelay  recipient
    7009     2      3    0.12  local.bela@aaa.acts.hu
46413806  3878   3878  792.39  local.bela@mail.aaaa.hu
       0     1      1    0.08  local.maildir@mail.aaaa.hu
       0     5      5    0.31  local.postmaster@mail.aaaa.hu
       0     5      5    0.46  remote.sj@aaaa.hu
```

13. Lista A qmail-scanner telepítése

```
groupadd qscand
useradd -g qscand -s /bin/
➥false -d /nonexistent
➥qscand
tar zxvf qmail-scanner-
➥2.01.tgz
cd qmail-scanner-2.01
./configure --log-details
➥syslog --domain mail.aaaa.hu
```

14. Lista Setuid wrapper program telepítése

```
gcc -O2 -o qmail-scanner-
➥queue qmail-scanner-queue.c
cp qmail-scanner-queue /var/
➥qmail/bin/qmail-scanner-queue
chown qscand:qscand
➥/var/qmail/bin/
➥qmail-scanner-queue
chmod 6755 /var/qmail/bin/
➥qmail-scanner-queue
chmod -s /var/qmail/
➥bin/qmail-scanner-queue.pl
chown -R qscand:qscand
➥/var/spool/qscan
```

15. Lista A /etc/tcp.smtp fájl tartalma módosítás után

```
192.168.1.:allow,RELAYCLIENT=
➥"",QMAILQUEUE="/var/qmail/
➥bin/qmail-queue"
127.:allow,RELAYCLIENT="",
➥QMAILQUEUE="/var/qmail/bin/
➥qmail-queue"
```

A példában feltételezzük, hogy a ***clamav*** antivírus csomag már telepítve van, és gépünkön fut a ***clamd***. Adjuk ki az *13. Listában* szereplő utasításokat, majd kövessük a megjelenő instrukciókat.
Ha minden rendben ment, akkor a `./configure --install` következik, és kövessük ismét az utasításokat. A telepítő létrehozza a */var/spool/qscan* könyvtár alatt a szükséges állományokat és könyvtárszerkezetet, illetve a `qmail-scanner-queue.pl` programot a */var/qmail/bin* alá másolja.
Ha a telepítő arra panaszkodik, hogy a ***Perl*** nem tud ***setuid*** programot futtatni, akkor telepítsük a ***contrib*** könyvtárban található ***qmail-scanner-queue.c*** programot az *14. Listában* látható utasításokkal, majd a */var/qmail/bin/qmail-scanner-queue.pl* első sorából töröljük a `-T` kapcsolót.
Már csak azt kell tudatni a ***Qmail***-lel, hogy ne a gyári ***qmail-queue*** programot használja, hanem a mi ***setuid*** programunkat – amely a */var/qmail/bin/qmail-scanner-queue.pl* programot futtatja, hogy az elvégezze a vírusellenőrzést, majd átadja a levelet a ***qmail-queue*** programnak, hogy aztán a levél tovább

16. Lista Egy vírusmentes levél naplóbejegyzése

```
Mar 22 09:21:03 aaa qmail: 1174587663.700520 new msg 64906
Mar 22 09:21:03 aaa qmail: 1174587663.701110 info msg 64906:
➥bytes 2932 from <sj@aaaa.hu> qp 31739 uid 1000
Mar 22 09:21:03 aaa qmail: 1174587663.731470 starting delivery
➥40: msg 64906 to local sj@mail.aaaa.hu
Mar 22 09:21:03 aaa qmail: 1174587663.732095 status: local 1/10
➥remote 0/20
Mar 22 09:21:03 aaa qmail-scanner[31732]:
➥Clear:RC:1(192.168.1.22): 0.221937 2642 sj@aaaa.hu
➥sj@mail.aaaa.hu RE:_torles
➥<E8C8116587EBD6119ACB00508B63C4DD0A65003B@bxxxxx01.xxxx.xxx.h
➥1174587663.31734-0.aaa:424 orig-aaa117458766354031732:2642
Mar 22 09:21:03 aaa qmail: 1174587663.843804 delivery 40:
➥success: did_1+0+0/
Mar 22 09:21:03 aaa qmail: 1174587663.844481 status: local 0/10
➥remote 0/20
Mar 22 09:21:03 aaa qmail: 1174587663.844789 end msg 64906
```

17. Lista Egy vírusos levélhez tartozó naplórészlet

```
Mar 22 19:28:24 aaa clamd[31833]:
➥/var/spool/qscan/tmp/aaa117458810454031841/photo-9502.zip:
➥Worm.Sober.G FOUND
Mar 22 19:28:25 aaa clamd[31833]:
➥/var/spool/qscan/tmp/aaa117458810454031841/
➥orig-aaa117458810454031841: Worm.Sober.G FOUND
Mar 22 19:28:25 aaa qmail-scanner[31841]: Clear:RC:1(127.0.0.1):
➥0 1100 sj@mail.aaaa.hu <>
➥virus_found_in_sent_message_"FwD:_hey_dude!_(fwd)"
➥aaa117458810554031841-sj@mail.aaaa.hu quarantine-
➥event.txt:1000
Mar 22 19:28:25 aaa qmail-scanner[31841]:
➥CLAMDSCAN:Worm.Sober.G:RC:1(192.168.1.22): 0.935775 69075
➥sj@aaaa.hu sj@mail.aaaa.hu FwD:_hey_dude!_(fwd)
➥<ab.20609153921.K49148@aaaabbbb.xxxx.hu> photo-9502.zip:49821
```

18. Lista A /var/spool/qscan/quarantine.log-ba írt bejegyzés

```
Thu, 22 Mar 2007 19:31:52
➥AKST  sj@aaaa.hu
➥sj@mail.aaaa.hu FwD: hey
➥dude! (fwd)    Worm.Sober.G
➥clamdscan: 0.90.1/2892.
```

mehessen. Ehhez állítsuk be a `QMAILQUEUE` környezeti változót a */etc/tcp.smtp* állományban, a *15. Lista* szerint, majd frissítsük a hozzá tartozó ***cdb*** fájlt a korábban leírt módon.

Ha egy vírusmentes levél érkezik, akkor a *16. Listában* látható bejegyzés kerül a naplóba

Ha vírust talál a levélben, akkor azt karanténba helyezi, és a *17. Listában* látható bejegyzés kerül a naplóba (csak a lényeges részt mutatva), ill. a *18. Listában* a */var/spool/qscan/quarantine.log* fájlba írt bejegyzés látható. Bár véleményem szerint jobb lenne, ha a levelet az ***SMTP*** párbeszéd során 55x hibával eldobná. Egy kis módosítással azonban ez is elérhető.

Vírusos levél esetén – ha a ***debug*** opciót engedélyezzük (alapértelemzésben be van kapcsolva) – a */var/spool/qscan/qmail-queue.log* állományba egy igen részletes bejegyzés kerül, ahol mindent megtudhatunk, hogy a levél feldolgozása során pontosan mi történik.

Ami a spam elleni védelmet illeti, ha már telepítettük a ***SpamAssassin***-t, akkor azt felismeri és használja a ***qmail-scanner***. Ha még nem, akkor érdemes egy olyan statisztikai elven működő programot választani, amely használható a ***maildrop*** vagy ***procmail*** programokon keresztül.

Hogyan tovább?

A ➲ http://www.lifewithqmail.org/lwq.html#related-packages címen további hasznos kiegészítő programokat találunk. Bizonyára telepíteni akarjuk a ***dot-forward*** csomagot, amely ***sendmail***-kompatibilis ***.forward*** támogatást biztosít.

Ha nem akarunk megbarátkozni a ***qmail*** saját álnév (***alias***) mechanizmusával, akkor a ➲ http://cr.yp.to/fastforward.html címről töltsük le a ***fastforward*** csomagot.

Ajánlom még az Olvasó figyelmébe a http://www.qmail.org/top.html és a ➲ http://www.lifewithqmail.org/lwq.html címeket, ahol részletes információk, leírások, foltok ill. segédprogramok találhatóak, amelyek megkönnyítik életünket.

A ***Qmail*** nagy teljesítményű, biztonságos, a többi ***djbware*** programhoz hasonlóan moduláris, és néhány segédprogram segítségével ***sendmail*** kompatibilissé tehető. ***Berstein*** a ***TODO*** részben felveti, hogy esetleg az egészet újraírja a nulláról. Hátha akkor már belekerülnek a hiányolt-, ill. azok a funkciók is, amelyeket jelenleg csak kissé körülményesen lehet biztosítani.

Sütő János
(jsuto@freemail.hu)

1997 óta használ Slack ware Linux-ot. Szabadidejében a postfix clapf nevű vírus- és spam szűrőjét polírozza.