

# **Poczta w systemie Linux na przykładzie agenta transferu poczty qmail**

Autor: Paweł Malita IVFDS

## STRESZCZENIE

Praca zawiera podstawowe informacje na temat działania poczty elektronicznej w systemie Linux: negocjowanie połączeń i przesyłka przez protokół SMTP. Wyjaśniono w niej podstawowe pojęcia: MTA, MUA. Opisane są zalety agenta pocztowego qmail, sposób pobrania źródeł programu, kompilacja, instalacja i konfiguracja z uwzględnieniem usunięcia najczęściej występującego MTA w systemie Linux - Sendmail. Pokazano jak zmusić qmail do pracy z wirtualnymi domenami jak Omówiono także sposoby zabezpieczania przed użyciem serwera przez spamerów. W ostatnim rozdziale znajduje się lista źródeł, z których można dowiedzieć się więcej na temat MTA qmail a także innych programów wspomagających zarządzanie pocztą w systemie Linux.

## SPIS TREŚCI

STRESZCZENIE .....	1
SPIS TREŚCI .....	2
1. WSTĘP .....	3
1.1 Jak działa poczta w systemie Linux? .....	3
1.2 Dlaczego qmail? .....	3
2. INSTALACJA .....	4
2.1 Dlaczego źródła? .....	4
2.2 Wymagania systemowe .....	4
2.3 Skąd wziąć źródła? .....	5
2.4 Rozpakowanie plików źródłowych .....	5
2.5 Tworzenie użytkowników i grup .....	6
2.6 Budowanie modułów .....	7
2.7 Skrypty sterujące .....	7
2.8 Usunięcie dotychczasowego MTA .....	12
2.9 Testowanie instalacji .....	13
3. KONFIGURACJA .....	13
3.1 Pliki konfiguracyjne .....	13
3.2 Domeny zaufane .....	14
3.3 Domeny wirtualne i różne nazwy hosta .....	14
3.4 Aliasy .....	15
3.5 Filtrowanie spamu .....	15
4. DOKUMENTACJA .....	16
Literatura .....	17

## 1. WSTĘP

### 1.1 Jak działa poczta w systemie Linux?

Poczta w systemie Linux oparta jest o zdefiniowany w dokumencie RFC 821 protokół SMTP (Simple Mail Transfer Protocol). Jest to protokół znakowy pozwalający przysyłać wiadomości zbudowane według standardu RFC 822 przez sieć serwerów pocztowych do adresata.

Proces transportu wiadomości (w dużym uproszczeniu z pominięciem sytuacji awaryjnych) wygląda następująco:

W programie pocztowym (MUA – Mail User Agent) użytkownik *nadawca@domena1* tworzy wiadomość adresowana do *adresat@domena2*

Wiadomość przekazywana jest do kolejki lokalnego agenta pocztowego (MTA – Mail Transfer Agent)

MTA lokalny (klienta) przetwarza kolejkę poczty i natrafiwszy na naszą wiadomość łączy się z serwerem *domena2*

Po połączeniu (najczęściej przez port 25 TCP/IP) MTA klienta wysyła komendę: *HELO domena1*

MTA na zdalnym serwerze odpowiada: *250 domena2 Hello domena1, pleased to meet you*

Teraz MTA – klient wysyła nadawcę wiadomości: *MAIL From:<nadawca@domena1>*

Jeśli serwer przyjmuje pocztę z tej domeny (RELAYING) i nie ma adresu nadawcy na czarnej liście to potwierdza zaakceptowanie nadawcy: *250 <nadawca@domena1>... Sender ok*

Klient pyta o akceptację adresata *RCPT To:<adresat@domena2>*

Jeśli adres jest zaakceptowany serwer odpowiada: *250 <adresat@domena2>... Recipient ok*

Klient sygnalizuje chęć rozpoczęcia transmisji ciała wiadomości: *DATA*

Serwer sygnalizuje oczekiwanie na treść wiadomości: *354 Enter mail, end with "." on a line by itself* – symbol kończący treść wiadomości to sekwencja CR LF . CR LF

Klient MTA transmituje dane i na końcu wysyła sekwencję: .

Serwer powiadamia o przyjęciu wiadomości: *250 Mail accepted*

Klient kończy transmisję: *QUIT*

Serwer potwierdza przesłanie poczty do systemu plików - skrzynki pocztowej użytkownika, lub do kolejnego serwera jeśli była to maszyna typu RELAY HOST: *221 domena2 delivering mail adresat@domena2... Sent*

### 1.2 Dlaczego qmail?

Standardowym MTA w różnych popularnych dystrybucjach systemu Linux jest Sendmail. Jednak ze względu na skomplikowaną konfigurację zajmę się jego zamiennikiem – qmail, napisanym przez dr Dana Bernsteina, wykładowcę matematyki na University of Illinois w Chicago, znanym także z współpracy z rządem Stanów Zjednoczonych w zakresie kryptografii.

O wyborze qmail jako MTA w systemie Linux zdecydowały wyróżniające go ważne cechy:

- Bezpieczeństwo – qmail został napisany w celu zapewnienia bezpiecznego przesyłania poczty; powszechnie używany Sendmail został napisany w czasach gdy Internet nie był w dużym stopniu bezpieczny, a próby jego zabezpieczenia nie zawsze kończyły się powodzeniem. Jedynie zaprojektowanie programu od nowa pozwala na osiągnięcie zadawalającego poziomu bezpieczeństwa
- Wydajność – qmail obsługuje równoległe dostarczanie poczty – standardowo można ustawić do 20 kolejek, co znacznie przyspiesza pracę serwera
- niezawodność – qmail gwarantuje, że wysłana wiadomość nie zaginie w sieci, pozwala również na przesyłanie poczty przez NFS bez zakleszczeń
- prostota – qmail jest jednym z mniejszych MTA oferując przy tym zaawansowane opcje i prostotę konfiguracji

## 2. INSTALACJA

Ponieważ w chwili obecnej posiadam na płytach CD tylko dystrybucję Red Hat Linux 7.2 zostanie opisana instalacja MTA qmail na tym systemie. Instalacje i wszystkie procedury konfiguracyjne (jeśli nie podano inaczej) należy wykonywać jako *super user (root)*.

### 2.1 Dlaczego źródła?

Program najlepiej zainstalować ze źródeł, to znaczy skopiować i następnie skompilować kod źródłowy. Dlaczego? Pozwala to na lepsze dostosowanie programu do systemu na jakim ma pracować, co w efekcie podnosi jego niezawodność i bezpieczeństwo. Skompilowane pliki binarne rozpowszechniane w pakietach muszą być uniwersalne, co pociąga za sobą mniejsze możliwości konfiguracyjne.

### 2.2 Wymagania systemowe

- dowolny system unixowy z systemem plików o tradycyjnej semantyce BSD FFS (synchroniczne wywołania systemowe)
- około 10 MB miejsca na dysku na czas kompilacji – po jej zakończeniu binaria zajmują około 4MB
- kompletny i działający system kompilatora języka C
- kilka MB miejsca na dysku na dokumentację i pliki konfiguracyjne
- wystarczająca ilość miejsca na dysku na kolejkę – od kilku MB dla zastosowań domowych po kilka GB dla profesjonalnego serwera pocztowego
- połączenie sieciowe – zalecane o przepustowości większej niż 28,8kb/s (dla wolnych modemów należy zainstalować pakiet *serialmail*)

## 2.3 Skąd wziąć źródła?

Odnośniki do miejsc, z których można pobrać źródła można znaleźć na stronie <http://www.qmail.org>. Dostępne są polskie mirrory: <http://qmail.skrytka.com/top.html>, <http://qmail.segfault.pl/top.html> i <http://qmail.graff.pl/top.html>.

Do instalacji niezbędne są archiwa:

<ftp://cr.yo.to/software/qmail-1.03.tar.gz> – *qmail* MTA

<ftp://cr.yo.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz> - *ucspi-tcp* – zamiennik *inetd*

<ftp://cr.yo.to/daemontools/daemontools-0.76.tar.gz> - *daemontools* – narzędzie do zarządzania demonami i ich logami

## 2.4 Rozpakowanie plików źródłowych

Najpierw należy utworzyć katalogi na pliki źródłowe. Niech będą to */usr/local/src* dla *qmail* i *ucspi-tcp*, oraz */package* dla pozostałych:

```
mkdir -p /usr/local/src
mkdir -p /package
```

teraz z katalogu, w którym znajdują się pliki należy przenieść je do utworzonych powyżej:

```
mv qmail-1.03.tar.gz ucspi-tcp-0.88.tar.gz /usr/local/src
mv daemontools-0.76.tar.gz
```

i w końcu rozpakowujemy pliki z zachowaniem uprawnień dla każdego pliku z archiwum:

```
cd /usr/local/src
gunzip qmail-1.03.tar.gz
gunzip ucspi-tcp-0.88.tar.gz
tar -xpf qmail-1.03.tar
tar -xpf ucspi-tcp-0.88.tar
rm *.tar
cd /package
gunzip daemontools-0.76.tar.gz
tar -xpf daemontools-0.76.tar
rm *.tar
```

Przed kompilacją trzeba jeszcze utworzyć katalog dla plików binarnych:

```
mkdir /var/qmail
```

Pozostałe katalogi zostaną utworzone automatycznie podczas budowania modułów, przy czym korzeniem całej struktury będzie katalog */var/qmail*. W systemie Red Hat Linux pliki konfiguracyjne znajdują się w katalogu */etc*. Żeby dostosować *qmail* do tego standardu należy stworzyć link symboliczny:

```
mkdir /etc/qmail
ln -s /etc/qmail /var/qmail/control
```

## 2.5 Tworzenie użytkowników i grup

Aby umożliwić demonom MTA *qmail* dostęp do systemu plików (kolejka, skrzynki pocztowe, logi) należy utworzyć odpowiednich użytkowników i grupy użytkowników. W pliku */usr/local/src/qmail-1.03/INSTALL.ids* znajdują się szablony skryptów realizujących tą operację dla danego systemu. Wystarczy skasować niepotrzebne linie i nieco zmodyfikować wpisy aby otrzymać przydatny skrypt powłoki. W przypadku Red Hat Linux 7.2 z powłoką *Bash* wygląda on następująco:

```
#!/bin/bash
groupadd nofiles
useradd -g nofiles -d /var/qmail/alias alias
useradd -g nofiles -d /var/qmail qmaild
useradd -g nofiles -d /var/qmail qmail1
useradd -g nofiles -d /var/qmail qmailp
groupadd qmail
useradd -g qmail -d /var/qmail qmailq
useradd -g qmail -d /var/qmail qmailr
useradd -g qmail -d /var/qmail qmails
```

następnie należy plik oznaczyć jako wykonywalny i uruchomić:

```
chmod 700 /usr/local/src/qmail-1.03/INSTALL.ids
/usr/local/src/qmail-1.03/INSTALL.ids
```

Jeśli na maszynie zainstalowano system dla którego nie ma przygotowanego szablonu należy utworzyć grupy ręcznie. Należy w tym dodać do */etc/group* linie:

```
qmail:*:2107:
nofiles:*:2108:
```

gdzie 2107 i 2108 są identyfikatorami grup i nie mogą być używana przez żadne inne. Jeśli są już zajęte należy wybrać inne z zachowaniem analogii przy dalszej konfiguracji. Analogicznie dokonuje się wpisów użytkowników w */etc/passwd* pamiętając by identyfikatory użytkowników (tutaj 7790-7796) były unikalne:

```
alias:*:7790:2108::/var/qmail/alias:/bin/true
qmaild:*:7791:2108::/var/qmail:/bin/true
qmail1:*:7792:2108::/var/qmail:/bin/true
qmailp:*:7793:2108::/var/qmail:/bin/true
qmailq:*:7794:2107::/var/qmail:/bin/true
qmailr:*:7795:2107::/var/qmail:/bin/true
qmails:*:7796:2107::/var/qmail:/bin/true
```

## 2.6 Budowanie modułów

Skrypt budujący zakłada, że kompilator C uruchamia się poleceniem `cc` i ścieżka do niego dostępu zapisana jest w zmiennej środowiskowej `PATH`. Jeśli tak nie jest należy zmodyfikować zmienną `PATH` lub/i zmienić nazwę pliku kompilatora w plikach `conf-cc` i `conf-ld` w katalogu z plikami źródłowymi – dla `qmail`: `/usr/local/src/qmail-1.03/`, który należy uczynić katalogiem bieżącym. Proces kompilacji uruchamia się poleceniem:

```
make setup check
```

Kompilacja nie powinna być przerwana żadnym komunikatem o błędzie. Po jej zakończeniu należy przeprowadzić wstępną konfigurację `qmail` za pomocą skryptu `config`.

Jeśli w rekordach DNS nie można znaleźć nazwy hosta, należy uruchomić skrypt `config-fast` podając jako argument pełną nazwę hosta z domeną.

`Ucspi-tcp` kompiluje się w taki sam sposób jak `qmail` (bez konfiguracji), natomiast kompilacja `daemontools` wygląda następująco:

```
cd /package/admin/daemontools-0.76
package/install
```

Po tym poleceniu powinien rozpocząć działanie proces `svscan` (system BSD wymaga restartu).

## 2.7 Skrypty sterujące

Teraz należy napisać skrypty sterujące `qmail`. Najpierw skrypt `rc` w katalogu `/var/qmail/`, który uruchamia agenta z odpowiednim parametrem – rodzajem skrzynki pocztowej użytkownika:

```
#!/bin/bash
exec env - PATH="/var/qmail/bin:$PATH: \
qmail-start "`cat /var/qmail/control/defaultdelivery`"
```

Teraz trzeba oznaczyć plik jako wykonywalny, utworzyć katalogi na logi i uczynić ich właścicielem użytkownika `qmail`:

```
chmod 755 /var/qmail/rc
mkdir -p /var/log/qmail/smtpd
chown qmail /var/log/qmail /var/log/qmail/smtpd
```



Następnie należy wpisać do pliku *defaultdelivery* rodzaj skrzynki pocztowej użytkownika. Do wyboru są dwa rodzaje:

- skrzynka formatu mbox – najpowszechniej używana przez programy pocztowe, wiadomości są zapisane w pliku *~/Mailbox*; aby móc jej używać należy wpisać: *./Mailbox*
- skrzynka formatu maildir – bardziej niezawodna, mniej powszechna; wpis ma postać: *./Maildir/*

Trzeci rodzaj skrzynki wykorzystywany np.: w systemie Red Hat Linux i wspierany przez programy *procmail*, *Sendmail* nie jest obsługiwany przez *qmail* – poczta w przechowywana jest w katalogu *\$USER/var/spool/mail*. Aby przystosować system do innego rodzaju skrzynki należy zmienić zmienną środowiskową *MAIL* w pliku */etc/profile* (Red Hat 7.2) na wartość:

```
MAIL="/home/$USER/Mailbox"
```

Programy typu *procmail* wymagają zmian w kodzie i ponownej kompilacji.

Następnym krokiem instalacji jest stworzenie skryptu sterującego opcjami agenta takimi jak: restart, zatrzymanie, wznowienie, wyczyszczenie kolejki, start, zamknięcie procesu MTA. Dla Red Hat Linux używającego programu *chkconfig* gotowy skrypt można pobrać ze strony: <http://www.lifewithqmail.org/qmailctl-script-dt70>:

```
#!/bin/sh
# For Red Hat chkconfig
# chkconfig: - 80 30
# description: the qmail MTA
18 2.8. Start qmail
PATH=/var/qmail/bin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
export PATH
QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
case "$1" in
start)
echo "Starting qmail"
if svok /service/qmail-send ; then
svc -u /service/qmail-send
else
echo qmail-send supervise not running
fi
if svok /service/qmail-smtpd ; then
svc -u /service/qmail-smtpd
else
echo qmail-smtpd supervise not running
fi
if [ -d /var/lock/subsys ]; then
touch /var/lock/subsys/qmail
fi
;;
stop)
echo "Stopping qmail..."
```

```

echo " qmail-smtpd"
svc -d /service/qmail-smtpd
echo " qmail-send"
svc -d /service/qmail-send
if [ -f /var/lock/subsys/qmail ]; then
rm /var/lock/subsys/qmail
fi
;;
stat)
svstat /service/qmail-send
svstat /service/qmail-send/log
svstat /service/qmail-smtpd
svstat /service/qmail-smtpd/log
qmail-qstat
;;
doqueue|alarm|flush)
echo "Flushing timeout table and sending ALRM signal to qmail-send."
/var/qmail/bin/qmail-tcpok
svc -a /service/qmail-send
;;
queue)
qmail-qstat
qmail-qread
;;
reload|hup)
echo "Sending HUP signal to qmail-send."
svc -h /service/qmail-send
;;
pause)
echo "Pausing qmail-send"
svc -p /service/qmail-send
echo "Pausing qmail-smtpd"
svc -p /service/qmail-smtpd
;;
cont)
echo "Continuing qmail-send"
svc -c /service/qmail-send
echo "Continuing qmail-smtpd"
svc -c /service/qmail-smtpd
;;
restart)
echo "Restarting qmail:"
echo "* Stopping qmail-smtpd."
svc -d /service/qmail-smtpd
echo "* Sending qmail-send SIGTERM and restarting."
svc -t /service/qmail-send
echo "* Restarting qmail-smtpd."
svc -u /service/qmail-smtpd
;;
cdb)
tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
chmod 644 /etc/tcp.smtp.cdb

```

```

echo "Reloaded /etc/tcp.smtp."
;;
help)
cat <<HELP
stop -- stops mail service (smtp connections refused, nothing goes
out)
start -- starts mail service (smtp connection accepted, mail can go
out)
pause -- temporarily stops mail service (connections accepted,
nothing leaves)
cont -- continues paused mail service
stat -- displays status of mail service
cdb -- rebuild the tcpserver cdb file for smtp
restart -- stops and restarts smtp, sends qmail-send a TERM &
restarts it
doqueue -- schedules queued messages for immediate delivery
reload -- sends qmail-send HUP, rereading locals and virtualdomains
queue -- shows status of queue
alm -- same as doqueue
flush -- same as doqueue
hup -- same as reload
HELP
;;
*)
echo "Usage: $0
{start|stop|restart|doqueue|flush|reload|stat|pause|cont|cdb|queue|he
lp}"
exit 1
;;
esac
exit 0

```

Należy go nazwać *qmailctl* i umieścić w katalogu */var/qmail/bin/*. Pozostaje tylko wskazać na niego w katalogu *init.d* oraz w katalogach odpowiadających za uruchamianie usług w poszczególnych trybach pracy (errorlevel). Dla Red Hat Linux 7.2 polecenia wyglądają następująco:

```

ln -s /var/qmail/bin/qmailctl /etc/init.d/qmail
ln -s /etc/init.d/qmail /etc/rc0.d/K30qmail
ln -s /etc/init.d/qmail /etc/rc1.d/K30qmail
ln -s /etc/init.d/qmail /etc/rc2.d/S80qmail
ln -s /etc/init.d/qmail /etc/rc3.d/S80qmail
ln -s /etc/init.d/qmail /etc/rc4.d/S80qmail
ln -s /etc/init.d/qmail /etc/rc5.d/S80qmail
ln -s /etc/init.d/qmail /etc/rc6.d/K30qmail

```

Następnie należy utworzyć katalogi dla skryptów zapisujących logi:

```

mkdir -p /var/qmail/supervise/qmail-send/log
mkdir -p /var/qmail/supervise/qmail-smtpd/log

```

i poszczególne skrypty:

```
/var/qmail/supervise/qmail-send/run:
```

```
#!/bin/bash
exec /var/qmail/rc
```

```
/var/qmail/supervise/qmail-send/log/run:
```

```
#!/bin/bash
exec /usr/local/bin/setuidgid qmail1 /usr/local/bin/multilog t \
/var/log/qmail
```

Skrypt ten uruchamia program multilog z identyfikatorem użytkownika qmail1 i ścieżką docelową dla logów utworzoną wcześniej.

```
/var/qmail/supervise/qmail-smtpd/run:
```

```
#!/bin/bash
QMAILUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`
if [ -z "$QMAILUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" \
-o -z "$LOCAL"]; then
echo Brak ustawionych zmiennych QMAILUID, NOFILESGID, MAXSMTPD lub
LOCAL
echo w /var/qmail/supervise/qmail-smtpd/run
exit 1
exec /usr/local/bin/softlimit 2000000 \
/usr/local/bin/tcpserver -v -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c \
"$MAXSMTPD" -u "$QMAILUID" -g "$NOFILESGID" 0 \
smtp /var/qmail/bin/qmail-smtpd 2>&1
```

Skrypt ten sprawdza czy w plikach konfiguracyjnych znajdują się odpowiednie ustawienia a następnie uruchamia program *qmail-smtpd* jako serwer smtp. Szczegóły plików konfiguracyjnych opisane będą w następnym rozdziale. Na razie zapisać trzeba do nich jakieś wartości. W tym momencie nie ustawiony jest tylko plik */var/qmail/control/concurrencyincoming*, który należy utworzyć z wartością 20.

W systemie Solaris program *id* nie działa poprawnie. Należy użyć za miast niego */usr/xpg4/bin/id*.

Limit pamięci ustawiany komendą *softlimit* można zwiększyć, gdy nie można połączyć się z portem 25 lub gdy zdalne systemy nie mogą wysłać poczty.

Po wskazaniu wskazań:

```
ln -s /var/qmail/supervise/qmail-send /service
ln -s /var/qmail/supervise/qmail-smtpd /service
```

system uruchomi automatycznie usługi *qmail*. Na tym etapie jest to jeszcze nie pożądane i aby je zatrzymać należy wywołać polecenie:

```
qmailctl stop
```

Następnym krokiem jest zezwolenie na wysyłanie poczty z maszyny lokalnej. Do pliku `/etc/tcp.smtp` należy dopisać linię:

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

a następnie odbudować bazę poleceniem:

```
qmailctl cdb
```

## 2.8 Usunięcie dotychczasowego MTA

Równoczesne działanie dwóch agentów pocztowych w systemie nie jest wskazane dlatego przed uruchomieniem `qmail` należy usunąć dotychczasowego MTA (w Red Hat 7.2 domyślnie instalowany jest *Sendmail*).

Pierwszym krokiem jest zatrzymanie procesów *Sendmail* poleceniem:

```
sendmail stop
```

Jeśli z jakichś względów polecenie nie funkcjonuje (w moim przypadku spowodowało zawieszenie wirtualnej konsoli) proces najlepiej ubić. Teraz można usunąć program (jeśli był instalowany z pakietu):

```
rpm -e --nodeps sendmail
```

a następnie, aby programy współpracowały z *qmail* wykonać odnośniki:

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

Ostatni krok instalacji *qmail* to stworzenie aliasów. Ze względów bezpieczeństwa pocztę z uprzywilejowanego konta musi otrzymywać zwykły użytkownik (proces *qmail* nie może działać jako uprzywilejowany). Także RFC 2821 narzuca utworzenie aliasu administratora systemu (*postmaster*) oraz odbiorcy dla zwrotów poczty (*mailer-daemon*). Aliasy tworzy się przez utworzenie plików o odpowiednich nazwach w katalogu `/var/qmail/aliases/`. Dla przykładu niech użytkownik *pawel* będzie administratorem poczty i systemu, a także odbiorcą zwrotów. Wówczas pliki można utworzyć następująco:

```
echo pawel > /var/qmail/alias/.qmail-root
echo pawel > /var/qmail/alias/.qmail-postmaster
ln -s /var/qmail/alias/.qmail-postmaster /var/qmail/alias/.qmail-
mailer-daemon
```

## 2.9 Testowanie instalacji

Po zakończeniu instalacji należy przetestować działanie agenta i ewentualnie poprawić błędy. Uruchamiamy usługi i wyświetlamy status:

```
qmailctl start
qmailctl stat
```

Status powinien zawierać cztery uruchomione procesy: *qmail-send*, *qmail-send/log*, *qmail-smtpd* i *qmail-smtpd/log* działające dłużej niż jedną sekundę. Jeśli po powtórным wyświetleniu statusu procesy mają inne identyfikatory i czas działania nie większy od 1, trzeba poszukać błędu. Najprościej spróbować każdą z usług qmail z katalogu */service* próbować uruchomić ręcznie np.:

```
cd /service/qmail-smtpd/log
./run
```

W przypadku błędu zostanie wyświetlony komunikat. W przeciwnym razie należy zakończyć przesyłanie do strumienia (Ctrl-d) i próbować w innym katalogu. W przypadku braku powodzenia prześledzić proces instalacji od początku.

Jeśli procesy działają poprawnie, można przetestować program i wysłać pocztę do użytkownika *root* np. poleceniem *mail*. Pocztę powinien otrzymać użytkownik wskazany jako administrator systemu w aliasach.

## 3. KONFIGURACJA

### 3.1 Pliki konfiguracyjne

Wszystkie pliki konfiguracyjne (za wyjątkiem aliasów) znajdują się w katalogu */var/qmail/control/* (lub */etc/qmail/*). W przypadku braku któregoś z nich qmail przyjmuje opcje domyślne. Poniżej przedstawiona jest lista plików i ich funkcji:

*badmailfrom* – zawiera listę zakazanych adresów w nagłówku *From* – filtr antyspamowy; domyślnie lista pusta

*bouncefrom* – nazwa użytkownika wysyłającego zwroty; domyślnie *MAILER-DAEMON*

*bouncehost* – nazwa hosta wysyłającego zwroty; domyślnie host zapisany w *me*

*concurrencyincoming* – liczba równoczesnych przychodzących połączeń SMTP; wpis w pliku musi istnieć

*concurrencylocal* – maksymalna ilość równoczesnych lokalnych przesyłek; domyślnie 10

*concurrencyremote* – maksymalna ilość równoległych zdalnych przesyłek; domyślnie 20

*defaultdelivery* – skrzynka pocztowa użytkowników; wpis musi istnieć

*defaultdomain* – nazwa domeny; domyślnie wartość z pliku *me*

*defaulthost* – nazwa hosta; domyślnie wartość z pliku *me*

*databytes* – limit wielkości wiadomości w bajtach; domyślnie 0 czyli brak limitu

*doublebouncehost* – nazwa hosta dla podwójnych zwrotów; domyślnie wpis z *me*

*doublebounceto* – odbiorca podwójnych zwrotów; domyślnie postmaster  
*envnoathost* – host dla adresów bez @; domyślnie wpis z *me*  
*helohost* – nazwa używana przez komendę HELO; domyślnie wpis z *me*  
*idhost* – nazwa dołączana do identyfikatora wiadomości; domyślnie wpis z *me*  
*localiphost* – nazwa przypisana do lokalnego adresu IP; domyślnie wpis z *me*  
*locals* – nazwa domeny dla lokalnych przesyłek; domyślnie wpis z *me*  
*me* – pełna nazwa domeny; wpis musi istnieć  
*morercphosts* – druga baza domen akceptowanych przez MTA; domyślnie pusta  
*percenthack* - lista akceptowanych domen z % w nazwie (adresowanie UUCP);  
domyślnie pusta  
*plusdomain* – nazwa dodawana do domen zakończonych znakiem +; domyślnie wpis z *me*  
*qmqpservers* – adresy IP serwerów QMQP (obsługujących Quick Mail Queuing Protocol); domyślnie pusty  
*queuelifetime* – liczba sekund po której wiadomość jest usuwana z kolejki (z odpowiednim komunikatem); domyślnie 604800  
*rcphosts* – lista domen akceptowanych przez MTA; domyślnie pusta  
*smtpgreeting* – wiadomość powitalna protokołu SMTP; domyślnie wpis z *me*  
*smtproutes* – wymuszane drogi dla SMTP; domyślnie brak  
*timeoutconnect* – czas oczekiwania (w sekundach) na połączenie SMTP; domyślnie 60  
*timeoutremote* – czas oczekiwania na zdalny serwer w sekundach; domyślnie 1200  
*timeoutsmtpd* – czas oczekiwania w sekundach na klienta SMTP; domyślnie 1200  
*virtualdomains* – baza wirtualnych domen i użytkowników; domyślnie pusta

### 3.2 Domeny zaufane

Aby zabezpieczyć się przed spamowaniem należy utworzyć listy zaufanych domen, dla których poczta będzie akceptowana przez MTA. Dokonuje się tego przez wpisy do pliku *rcphosts*.

Co jednak jeśli chcemy akceptować pocztę od maszyn z zakresu IP (np.: sieci lokalnej)? Do tego służy zmienna systemowa *RELAYCLIENT*, jednak ustawiana tylko dla połączenia z danego adresu IP. Odpowiedni wpis umieszcza się w pliku */etc/tcp.smtp*. Dla przykładu założmy, że chcemy akceptować wszystkie maszyny z podsieci *192.168.0.0/24*. Wówczas do *tcp.smtp* dopisujemy:

```
192.168.0.:allow,RELAYCLIENT=""
```

i następnie odbudowujemy bazę poleceniem:

```
qmailctl cdb
```

### 3.3 Domeny wirtualne i różne nazwy hosta

Domeny wirtualne konfigurowane są w pliku *virtualdomains*. Wpisy mają postać:

```
uzytkownik@wirtualna.domena:dodatek
wirtualna.domena:dodatek
```

co w rezultacie powoduje przetłumaczenie przez qmail adresu

*uzytkownik@wirtualna.domena* na *dodatek-uzytkownik@wirtualna.domena* i traktowanie przesyłki jako lokalnej. Niezbędne jest dodanie do *rcphosts* wpisu *wirtualna.domena*. Aby wiadomość mogła trafić do odpowiedniego użytkownika trzeba odpowiednio skonfigurować serwer DNS.

Aby lokalna maszyna posiadająca więcej niż jedną nazwę akceptowała odpowiednie połączenia, oprócz wpisów w *rcphosts* należy dodać odpowiednie linie w pliku *locals*. Po wszelkich modyfikacjach należy odbudować bazę tak jak w rozdziale 3.3.

### 3.4 Aliasy

Aliasy są to wirtualni użytkownicy przypisani do rzeczywistych użytkowników systemu Linux. Jeśli adresat wiadomości nie istnieje *qmail* przeszukuje bazę aliasów aby przyporządkować odpowiedniego użytkownika. Aliasy są konfigurowane wpisami do plików w katalogu */var/qmail/aliases/*. Dla przykładu chcemy aby w domenie *mojafirma.com* pocztę zaadresowaną do *biuro@mojafirma.com* otrzymywał użytkownik *kowalski* (który ma już swoje konto w systemie o adresie: *kowalski@mojafirma.com*). Aby to osiągnąć tworzymy plik */var/qmail/aliases/.qmail-biuro* i wpisujemy do niego tekst *kowalski*.

Jeśli utworzono alias o nazwie takiej jak rzeczywiste konto użytkownika, to nie będzie on nigdy używany.

### 3.5 Filtrowanie spamu

Podstawowe narzędzia w walce ze spamem dostarczane przez *qmail* to domeny zaufane i czarna lista nadawców (*badmailfrom*). Dodatkowym zabezpieczeniem może być sprawdzanie wpisów w serwerach DNS. Można to wykonać modyfikując skrypt */service/qmail-smtpd/run*:

```
#!/bin/bash
QMAILUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`
if [ -z "$QMAILUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" \
  -o -z "$LOCAL"]; then
echo Brak ustawionych zmiennych QMAILUID, NOFILESGID, MAXSMTPD lub
LOCAL
echo w /var/qmail/supervise/qmail-smtpd/run
exit 1
exec /usr/local/bin/softlimit 2000000 \
/usr/local/bin/tcpserver -v -p -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c \
  "$MAXSMTPD" -u "$QMAILUID" -g "$NOFILESGID" 0 \
smtp sh -c 'test -z "$TCPREMOTEHOST" \
&& echo "451 zly reverse DNS" \
|/var/qmail/bin/qmail-smtpd' 2>&1
```

Modyfikacja wykorzystuje opcję *-p* programu *tcpserver*, która usuwa zmienną systemową *TCPREMOTEHOST* w przypadku braku wpisu w DNS. Jeśli zmienna nie istnieje wyświetlany jest odpowiedni komunikat i demon *qmail-smtpd* nie startuje.



## 4. DOKUMENTACJA

Lista źródeł dokładniejszych informacji o MTA *qmail*:

1. Instrukcje MAN, dostępne również w Internecie:  
<http://www.qmail.org/man/index.html>
2. Dokumentacja qmail – po instalacji dostępna w katalogu `/var/qmail/doc/`
3. Najczęściej zadawane pytania (FAQ) dostępne w katalogu `/var/qmail/doc/FAQ/` lub on-line: <http://cr.yp.to/qmail/faq.html>
4. Archiwa mailingowej listy dyskusyjnej – wyszukiwarka pod adresem <http://www-archive.ornl.gov:8000/>
5. Archiwa Securepoint - <http://msgs.securepoint.com/qmail/>

## LITERATURA

- [1] "The qmail home page" - <http://www.qmail.org/top.html>
- [2] Dave Still "Life with qmail" - <http://www.lifewithqmail.org/>
- [3] Chris Hardie " qmail Anti-Spam HOWTO" –  
<http://www.summersault.com/chris/techno/qmail/qmail-antispam.html>
- [4] Ben-Dayana Maor, Ben-Shimon Sonny, Efron Niv, Kuperman Idan, Meller Tal "SMTP Simple Mail Transfer Protocol" - <http://www2.rad.com/networks/1998/sntp/sntp.htm>