

# Die eierlegende Wollmilchsau?

Vorgestellt: qmail in Kombination mit einem Virens Scanner, Spamfilter und datenbankbasierten Benutzern

"Enlarge your..." - Dutzende solcher E-Mails landen täglich in meinem Posteingang. Spielzeugautos soll ich kaufen, der Präsident einer Bank in Nigeria will Geld von mir und ein Anwalt sendet eine Mahnung und hofft, dass ich dadurch mit teuren Dialern heisse Mädels anrufe. Eines Tages platzte mir der Kragen, und ich beschloss, für meinen Mailserver einen Spamfilter und einen Virens Scanner zu installieren. Einmal am Werk, erweiterte ich den Server direkt um virtuelle, d.h. datenbankbasierte Benutzer und viele weitere nützliche Zusätze.

Qmail wurde 1997 durch D. J. Bernstein (<http://cr.yip.to/djb.html>) entwickelt und ist ein freier Mail Transfer Agent. Die Software zeichnet sich durch ihre Flexibilität, ihre beeindruckende Performance und durch ihre hohe Sicherheit aus und ist nicht umsonst die am zweithäufigsten eingesetzte Mailserversoftware überhaupt. Leider gestaltet sich die Installation und Konfiguration etwas umständlich und eine für Systemadministratoren täglich anfallende Arbeit, wie die Einrichtung von neuen Usern oder Domains, ist äußerst arbeits- und zeitintensiv. Dieser Artikel stellt den freien Zusatz vpopmail vor, der die Administration von qmail sehr vereinfacht, in dem er die Verwaltung und Authentifikation von Benutzern aus (My-) SQL-Datenbanken ermöglicht und gleichzeitig mit einigen vielversprechenden Erweiterungen aufwartet. Zum Schutz vor bösen Viren und fast ebenso bösen Werbemails zeige ich außerdem die Implementierung eines Virens Scanners und des bekannten Spamfilters Spamassassin (<http://www.spamassassin.org>).

Bevor wir nun mit der Installation beginnen, möchte ich noch darauf hinweisen, dass ich als Basis für diesen Artikel ein Debian Linux (Sarge)-System mit einer Minimalinstallation benutzt habe. Als Basisverzeichnis für vpopmail habe ich mir `/home/vpopmail` ausgesucht, als Virens Scanner verwende ich AntiVir von H+BEDV (<http://www.antivir.de>). Sollten Sie eine andere Distribution und/oder Software verwenden, so sind gegebenenfalls die Verzeichnisse und Einstellungen den entsprechenden Gegebenheiten anzupassen. Bitte beachten Sie außerdem, dass auf dem jeweiligen System neben einem Basissystem (z.B. gcc, make, patch etc.) auch Perl 5.6.1 (inkl. Headerdateien), zlib, MySQL (inkl. Headerdateien und Bibliotheken) und unzip installiert sein müssen. Sofern diese Programme nicht vorhanden sind, müssen Sie diese vor der Installation von qmail, vpopmail etc. installieren.

## Installation von qmail

Auf der offiziellen Seite zu qmail (<http://www.qmail.org>) finden Sie viele Informationen, Dokumentationen und bekannte Erweiterungen für das Programm. Laden Sie sich von <http://cr.yip.to/software/qmail-1.03.tar.gz> die aktuelle Version herunter und entpacken Sie diese mit `tar xvfz qmail-1.03.tar.gz`. Damit später bei der Ausführung von qmail unser Virens Scanner bzw. Spamfilter aktiv werden kann, müssen wir den Quellcode von qmail durch einen Patch verändern. Laden Sie sich deshalb z.B. mit `wget http://www.qmail.org/qmailqueue-patch` den entsprechenden Patch herunter und führen Sie diesen mit `patch -p0 < qmailqueue-patch` aus. Erzeugen Sie nun das Installationsverzeichnis für qmail mit `mkdir /var/qmail`. Da qmail über ein ausgeklügeltes Sicherheits- und Rechtesystem verfügt, müssen Sie vor der eigentlichen Installation zahlreiche Benutzer und Gruppen anlegen. Diese legen Sie mit folgenden Befehlen an:

```
groupadd nofiles
useradd -g nofiles -d /var/qmail/alias alias
useradd -g nofiles -d /var/qmail qmaild
useradd -g nofiles -d /var/qmail qmailf
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
```

Wechseln Sie in das Verzeichnis der entpackten Quellen von qmail (`cd qmail-1.03`) und rufen Sie zur Vorbereitung der Installation den Befehl `make setup check` auf. Danach müssen Sie den Rechnernamen und die

Domain für Ihr System definieren, in dem Sie den Befehl `./config` ausführen. Sollte Ihr Rechner- bzw. Domainname durch das Programm nicht vollständig aufgelöst werden können, werden Sie eine Fehlermeldung erhalten, die Sie jedoch vernachlässigen können. Definieren Sie Ihren Rechner- und Domainnamen manuell durch den Befehl `./config-fast rechnername.domain.tld`, wobei Sie `rechnername.domain.tld` selbstverständlich durch Ihre Werte ersetzen müssen (z.B. `wunderwaffe.wolfgarten.com`). Dieser Domainname wird von `qmail` in diversen Konfigurationsdateien eingetragen, die Sie später unter `/var/qmail/control` finden und er wird als Basisname bzw. Hauptdomain benutzt. Das Hinzufügen weiterer, virtueller Domains ist natürlich auch nach der Installation ohne Probleme möglich und wird im Laufe dieses Artikels noch eingehend vorgestellt. Sie können nun die eigentliche Installation von `qmail` durch Eingabe von `./install` und `./instcheck` abschließen.

### Der erste Start von `qmail`

Vor dem ersten Start von `qmail` müssen Sie einige Aliase anlegen, die festlegen, an welche E-Mailadresse das System fehlgeleitete oder ungültige E-Mails senden soll. Ebenso müssen Sie eine E-Mailadresse definieren, an die die für den Systemadministrator gedachten E-Mails gesendet werden, da bei `qmail` der `root`-Benutzer niemals direkt E-Mails bekommt. Legen Sie diese Aliase durch folgende Befehle an (E-Mailadresse entsprechend Ihren Gegebenheiten anpassen):

```
echo "sebastian@wolfgarten.com" > /var/qmail/alias/.qmail-postmaster
echo "sebastian@wolfgarten.com" > /var/qmail/alias/.qmail-mailer-daemon
echo "sebastian@wolfgarten.com" > /var/qmail/alias/.qmail-root
echo "sebastian@wolfgarten.com" > /var/qmail/alias/.qmail-default
```

Beenden und entfernen Sie desweiteren eventuell vorhandene Programme wie `sendmail`, `exim`, `postfix` etc. und deinstallieren Sie diese. Da einige Programme das Vorhandensein eines MTA wie `sendmail` voraussetzen, können Sie durch die folgenden Befehle entsprechende Verweise auf `qmail` vornehmen:

```
killall sendmail
mv /usr/lib/sendmail /usr/lib/sendmail.orig
mv /usr/sbin/sendmail /usr/sbin/sendmail.orig
ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

Hinweis: Entfernen Sie auch eventuell vorhandene Startskripte für `sendmail` und Konsorten. Sollten Sie PHP verwenden, sei an dieser Stelle darauf hingewiesen, dass Sie bei Verwendung von `qmail` als Pfad zu `sendmail` nicht den soeben verlinkten Wrapper, sondern den Pfad `/var/qmail/bin/qmail-inject` eintragen sollten.

Vor dem ersten Start von `qmail` müssen wir ein mitgeliefertes Startskript verändern, damit `qmail` das vorteilhafte Maildir-Verfahren zur Speicherung der E-Mails auf der Festplatte des Servers benutzt. Dazu kopieren wir ein mitgeliefertes Skript von `qmail` in das Hauptverzeichnis `/var/qmail` mit `cp /var/qmail/boot/home /var/qmail/rc` und editieren dieses. In dieser Datei ersetzen Sie den Ausdruck `./Mailbox` durch `./Maildir`, so dass das vollständige Startskript wie folgt aussieht:

```
#!/bin/sh

# Using splogger to send the log through syslog.
# Using qmail-local to deliver messages to ~/Mailbox by default.
```

```
exec env - PATH="/var/qmail/bin:$PATH" \
qmail-start ./Maildir splogger qmail
```

Speichern Sie die Datei und starten Sie `qmail` durch die Eingabe von `sh /var/qmail/rc &`. Schicken Sie zu Testzwecken eine erste E-Mail (ohne Inhalt) mit dem Befehl `echo to: sebastian@beispiel.de | /var/qmail/bin/qmail-inject` (E-Mailadresse anpassen). Verfolgen Sie die Auslieferung Ihrer Testmail durch Eingabe von `tail -f /var/log/mail` (oder `mail.info`, je nach Konfiguration von `/etc/syslog.conf`) und folgende Einträge sollten etwa in Ihrer Logdatei auftauchen:

```
Jan 4 16:41:19 wunderwaffe qmail: 1041694879.329055 new msg 1343557
```

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.329234 info msg 1343557: bytes 1701 from <root@wunderwaffe.wolfgarten.com> qp 32288 uid 1004

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.332736 starting delivery 22880: msg 1343557 to remote sebastian@beispiel.de

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.332835 status: local 0/10 remote 1/20

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.811156 delivery 22880: success:

63.131.11.7\_accepted\_message./Remote\_host\_said:\_250\_ok\_1041695677\_qp\_5581/

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.811319 status: local 0/10 remote 0/20

Jan 4 16:41:19 wunderwaffe qmail: 1041694879.811345 end msg 1343557

Hinweis: Sofern Ihre Domain noch nicht vollständig im DNS eingetragen ist, kann es unter Umständen passieren, dass die von Ihnen gesendete E-Mail nicht ankommt bzw. durch die Gegenseite des Empfängers abgelehnt wird, da Ihr Domainname nicht aufgelöst werden kann oder ungültig ist. Gerade beim Versenden einer E-Mail an Freemail-Anbieter wie z.B. GMX kann dieser Fall eintreten, der nur durch Korrektur der DNS-Einstellungen seitens des Providers behoben werden kann.

Wenn der Test erfolgreich war, müssen Sie qmail durch Eingabe von `killall qmail-send` beenden und damit die Installation von qmail abschließen. Widmen wir uns nun der Installation von vpopmail.

### Installation von vpopmail

Inter7, eine aus der Nähe von Chicago stammende Firma, hat die Software vpopmail ([www.inter7.com/vpopmail/](http://www.inter7.com/vpopmail/)) entwickelt. Das Softwarepaket, welches unter der GPL-Lizenz veröffentlicht worden ist, soll die Administration von virtuellen Domains und Usern unter qmail (und Postfix!) erheblich vereinfachen. Besonders zu erwähnen ist dabei die Tatsache, dass die Software mit nur einem real existierenden Benutzer bis zu 23 Millionen virtuelle Domains und bis zu 23 Millionen virtuelle User je Domain verwalten kann. Außerdem kann die Authentifizierung der User gegen zahlreiche SQL-Datenbanken (u.a. MySQL, Oracle) oder den Verzeichnisdienst LDAP erfolgen. Zudem bietet vpopmail, das früher unter dem unaussprechlichen Namen vchkw bekannt war, eine hervorragende Unterstützung von SMTP-after-POP und Selective Relaying. Vor der Installation von vpopmail müssen Sie das Programm tcpserver installieren, welches ebenfalls durch den Autor von qmail, D. J. Bernstein, entwickelt worden ist. Laden Sie sich deshalb von <http://cr.yip.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz> die aktuelle Version herunter, entpacken Sie diese mit `tar xvzf ucspi-tcp-0.88.tar.gz` und wechseln Sie in das neu erzeugte Verzeichnis `ucspi-tcp-0.88` (`cd ucspi-tcp-0.88`). Führen Sie die Befehle `make`, `make setup check` und `./install` sowie `./instcheck` hintereinander aus, um die Software nach `/usr/local/bin` zu installieren.

Die aktuellste Version von vpopmail finden Sie unter <http://www.inter7.com/vpopmail/>, wobei ich mich bei diesem Artikel auf die Version 5.2.1 (<http://www.inter7.com/vpopmail/vpopmail-5.2.1.tar.gz>) beziehe. Laden Sie die Software herunter und entpacken Sie diese mit `tar xvzf vpopmail-5.2.1.tar.gz`. Erstellen Sie nun durch die Eingabe von `groupadd vchkw` eine neue Gruppe für vpopmail namens vchkw. Zusätzlich müssen Sie durch Eingabe von `useradd -g vchkw -d /home/vpopmail -s /bin/false vpopmail` einen Benutzer namens vpopmail erstellen. Schließlich erzeugen Sie das Homeverzeichnis für diesen Benutzer durch die Eingabe von `mkdir /home/vpopmail` sowie `mkdir /home/vpopmail/etc`. In diesen Verzeichnissen werden später alle von vpopmail benötigten Programmteile abgelegt. Zusätzlich müssen Sie eine Datei anlegen, in der vpopmail die IP-Adressen der Clients speichert, die E-Mails über diesen Mailserver versenden dürfen (sog. Relaying). Erstellen Sie diese Datei durch die Eingabe von `touch /home/vpopmail/etc/tcp.smtp` und erlauben Sie dem lokalen PC (localhost mit IP 127.0.0.1) durch die Eingabe von `echo "127.0.0.:allow,RELAYCLIENT=\"\" > /home/vpopmail/etc/tcp.smtp` den Zugriff. Dies ist die minimalste Konfiguration und erlaubt nur dem Server selbst, E-Mails zu verschicken. Neben dieser einen IP-Adresse können in dieser Datei noch weitere IP-Adressen des Mailservers oder auch fremde (statische) IP-Adressen eingetragen werden, denen das Relaying, d.h. das Versenden von E-Mails über den Server, erlaubt sein soll. In der Regel müssen Sie jedoch keine weiteren IP-Adressen mehr eintragen, da die Software die dynamische Verwaltung dieser Liste automatisch übernimmt.

Der Sinn in der Benutzung der Software vpopmail liegt u.a. darin, dass die Software qmail um die Möglichkeit

erweitert, die Speicherung und Authentifikation von Benutzer u.a. gegen eine MySQL-Datenbank laufen zu lassen und somit virtuelle, d.h. nicht real existierende und in einer MySQL-Datenbank gespeicherte Benutzer innerhalb des E-Mailsystems zu verwenden. Dazu müssen Sie MySQL starten und eine neue Datenbank sowie einen neuen Benutzer mit exklusivem Zugriff auf diese anlegen. Starten Sie MySQL durch Eingabe von *mysql* und erzeugen Sie mit *create database vpopmail*; eine neue Datenbank namens vpopmail. Verwenden Sie die MySQL-interne Datenbank mysql mit *use mysql*; und führen Sie die folgenden SQL-Befehle aus, um einen neuen Benutzer anzulegen, der exklusiven Zugriff auf die neu angelegte Datenbank vpopmail hat (Passwort geheim, bitte ändern):

```
INSERT INTO user (Host, User, Password, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv,
Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, References_priv, Index_priv,
Alter_priv) VALUES ('localhost', 'vpopmail', PASSWORD('geheim'), 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N', 'N');
```

```
INSERT INTO db (Host, Db, User, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv,
Grant_priv, References_priv, Index_priv, Alter_priv) VALUES ('localhost', 'vpopmail', 'vpopmail', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y', 'Y');
```

Beenden Sie MySQL durch die Eingabe von *quit* und initialisieren Sie das Rechtesystem von MySQL mit *mysqladmin reload* neu. Hinweis: Sofern Sie den passwortlosen Zugriff durch den Benutzer root auf MySQL deaktiviert haben, müssen Sie gegebenenfalls beim Aufruf von MySQL zusätzlich die Optionen *-u root* und *-p* verwenden, um den Zugriff auf die Datenbank zu erhalten. Weitere Informationen erhalten Sie durch Eingabe von *mysql --help*.

Wechseln Sie in das Verzeichnis der entpackten vpopmail-Quellen (*cd vpopmail-5.2.1*), editieren Sie die Datei *vmysql.h* und ändern Sie die Zeilen 25-31 wie folgt (Passwort geheim bitte gemäß Ihrer vorherigen Eingaben ändern):

```
/* Edit to match your set up */
#define MYSQL_UPDATE_SERVER "localhost"
#define MYSQL_UPDATE_USER "vpopmail"
#define MYSQL_UPDATE_PASSWD "geheim"

#define MYSQL_READ_SERVER "localhost"
#define MYSQL_READ_USER "vpopmail"
#define MYSQL_READ_PASSWD "geheim"
/* End of setup section*/
```

Speichern Sie die Datei und rufen Sie den Befehl *./configure --help* auf, um eine Übersicht der zur Verfügung stehenden Optionen zu erhalten. Ich habe mich nach Durchsicht der Optionen für den folgenden Befehl entschieden (ggfs. an Ihre Gegebenheiten anpassen): *./configure --enable-qmaildir=/var/qmail --enable-vpopuser=vpopmail --enable-vpopgroup=vchkpw --enable-roaming-users=y --enable-relay-clear-minutes=30 --enable-auth-logging=y --enable-logging=y --enable-log-name=vpopmail --enable-default-domain=wolfgarten.com --enable-mysql=y --enable-passwd=n --enable-valias=y --enable-md5-passwords=y --enable-incdir=/usr/include --enable-libdir=/lib --enable-clear-passwd=n --enable-defaultquota=100M*

Die Optionen bedeuten im Einzelnen folgendes: *--enable-qmaildir* gibt das Basisverzeichnis von qmail an, hier also */var/qmail*. Die zwei nächsten Parameter (*--enable-vpopuser=vpopmail* und *--enable-vpopgroup=vchkpw*) definieren die Gruppe und den Benutzer, die bei der Installation von vpopmail erstellt worden sind. Die wohl wichtigste Option in dieser Konfiguration ist die folgende Option *--enable-roaming-users=y*, die das sogenannte Selective Relaying aktiviert. Selective Relaying ist eine Technik, die verhindern soll, dass ein Server zum Senden von unerwünschten Spam-Mails missbraucht wird. Es wird einem Client das Senden über einen Server nur ermöglicht, wenn vorher eine erfolgreiche Authentifizierung via POP3 erfolgt ist. Diese Technik ist auch bekannt als SMTP-after-POP (teilweise auch POP-before-SMTP) und wird mittlerweile sehr oft angewendet, weil das SMTP-Protokoll im Gegensatz zum POP3 Protokoll nicht direkt über einen Authentifizierungsmechanismus verfügt. Die drei Optionen *--enable-auth-logging=y*, *--enable-logging=y* und *--enable-log-name=vpopmail* sorgen dafür, dass die Zugriffe (Logins etc.) auf das E-Mailsystem in einer Datei (*/var/log/mail*) gespeichert werden.

Dies kann unter Umständen sehr sinnvoll sein, da so eine relativ einfache Fehlersuche möglich ist. Mit `--enable-default-domain=wolfgarten.com` wird eine Standard- bzw. Hauptdomain für den Server festgelegt, wodurch sich die Benutzer der Standarddomain nur mit ihrem Benutzernamen und ihrem Passwort anmelden können. Die Angabe des Domainnamens braucht im Gegensatz zu allen anderen Domains nicht zu erfolgen. Der Parameter `--enable-mysql=y` schaltet die MySQL-Unterstützung ein, die von uns für die Speicherung und Authentifikation der Benutzer verwendet wird. Mittels `--enable-passwd=n` wird die Authentifikation der Benutzer gegenüber der lokalen Passwortdatei des Systems (`/etc/passwd`) deaktiviert und `--enable-md5-passwords=y` aktiviert die Verschlüsselung der Passwörter in der MySQL-Tabelle nach dem sicheren MD5-Verfahren. Die beiden Optionen `--enable-incdir=/usr/include` und `--enable-libdir=/lib` geben Verzeichnisse an, in denen das Programm nach Bibliotheken und Headerdateien suchen soll, diese müssen Sie gegebenenfalls Ihren Gegebenheiten anpassen. Die beiden letzten Optionen `--enable-clear-passwd=n` und `--enable-defaultquota=100M` sorgen dafür, dass die Passwörter innerhalb der MySQL-Datenbank in verschlüsselter Form gespeichert werden und begrenzen die maximale Speicherplatzmenge, die ein Benutzer mit seinen E-Mails belegen darf, auf 100 MB (optional). Weitere Informationen zu den einzelnen Optionen finden Sie im Internet unter <http://www.inter7.com/vpopmail/vpopmail.html>.

Sobald die Konfiguration abgeschlossen ist, sehen Sie eine Übersicht der von Ihnen gewählten Optionen. Wenn Sie mit diesen Optionen nicht zufrieden sind, können Sie mittels `make clean` die Konfiguration löschen und die oben genannten Schritte wiederholen. Ansonsten können Sie durch den Befehl `make` die Software kompilieren und mit dem Befehl `make install` installieren. Nach der Installation müssen Sie den Befehl `*30 * * * * root /home/vpopmail/bin/clearopensmtp 2>&1 > /dev/null` in die Crontab des Systems (`/etc/crontab`) einfügen, damit die Liste der authentifizierten Clients, die über Server E-Mails senden dürfen, alle 30 Minuten geleert wird. Vor dem ersten Start von vpopmail müssen Sie die Datei `/home/vpopmail/bin/clearopensmtp` einmalig ausführen, um einige u.a. für das Selective Relaying benötigte Dateien zu erstellen. Die Installation von vpopmail ist damit abgeschlossen.

### Bedienung von vpopmail

Nachdem wir die eigentliche Installation abgeschlossen haben, können wir uns der Konfiguration des Systems widmen. Im Basisverzeichnis der vpopmail-Installation findet man ein Verzeichnis (`/home/vpopmail/bin`) namens bin, welches die ausführbaren Programmteile von vpopmail enthält. Eine Übersicht über die wichtigsten Programme von vpopmail bietet Ihnen die nachfolgende Liste, wobei die einzelnen Parameter kursiv angegeben sind:

- `vaddomain domain.tld Passwort`: Wie der Name unweigerlich erkennen lässt, legt dieser Befehl eine neue Domain im System an. Der erste Parameter gibt den eigentlichen Namen der Domain an, der zweite definiert das Passwort für den administrativen Benutzer Postmaster, der standardmäßig als Defaultuser benutzt wird. Beispiel: Der Aufruf `/home/vpopmail/bin/vaddomain wolfgarten.com Df2AxhJ9` würde eine neue Domain namens wolfgarten.com anlegen und dem Benutzer postmaster das Passwort Df2AxhJ9 zuteilen. Eine Übersicht der vorhandenen Domains und Benutzer finden Sie übrigens im Unterverzeichnis domains der vpopmail-Installation. Durch den Parameter `-q` können Sie den maximalen Speicherplatz festlegen, den der administrative Benutzer (postmaster) dieser Domain belegen darf.
- `vaddaliasdomain NeueDomain.tld AlteDomain.tld`: Dieser Befehl legt einen Alias von AlteDomain.tld auf NeueDomain.tld.
- `vdeldomain domain.tld`: Dieser Befehl löscht die angegebene Domain inklusive aller vorhandenen Benutzer (und Mails!).
- `vadduser user@domain.tld Passwort`: Hiermit erstellt man einen neuen Benutzer mit der E-Mailadresse `user@domain.tld` und dem durch den zweiten Parameter übergebenen Passwort. Beispiel: Der Befehl `/home/vpopmail/bin/vadduser sebastian@wolfgarten.com hallo` erstellt einen Benutzer mit der E-Mailadresse `sebastian@wolfgarten.com` und dem Passwort hallo.
- `vdeluser user@domain.tld`: Mit diesem Befehl löscht man einen Benutzer.
- `vpasswd user@domain.tld neuesPasswort`: Dieser Befehl weist einem Benutzer ein neues Passwort zu.

Dies sind die wesentlichen Programme zur Administration des E-Mailsystems. Eine Übersicht über den Syntax aller in vpopmail enthaltenen Programme sowie zahlreiche Hilfetexte finden Sie auf der Internetseite

<http://www.inter7.com/vpopmail/doc/> bzw. <http://www.inter7.com/vpopmail/>. Hinweis: Es sei noch erwähnt, dass die Benutzer sich immer mit dem Benutzernamen `benutzer%domain.tld` und ihrem Passwort am Server anmelden müssen, das `@`-Zeichen wird also durch ein Prozentzeichen ersetzt (aus `sebastian@wolfgarten.com` wird dementsprechend `sebastian%wolfgarten.com`).

### Installation eines Virenschanners

Zum Schutz gegen böse Viren möchte ich das E-Mailsystem mit einem Virenschanner verknüpfen und habe mich für das Programm AntiVir von H+BEDV (<http://www.antivir.de>) entschieden, da ich das Produkt sehr gut finde und es für den privaten Einsatz kostenlos ist. Hinweis: Wenn Sie einen anderen Virenschanner einsetzen möchten, müssen Sie zur Installation die Dokumentation des jeweiligen Programms konsultieren. Außerdem müssen Sie das Produkt AntiVir lizenzieren, wenn Sie es in einem kommerziellen Umfeld einsetzen möchten!

Laden Sie sich von <http://www.antivir.de> die aktuelle Version für Linux herunter (direkter Link: <http://www.antivir.de/dateien/antivir/release/avlxsrv.tgz>) und entpacken Sie die Software mit `tar xvf avlxsrv.tgz`. Wechseln Sie in das entpackte Verzeichnis (`cd antivir-server-2.0.6`) und installieren Sie die Software mit `./install`. Folgen Sie dabei einfach den Anweisungen des komfortablen Installationsprogramms und registrieren Sie sich bei <http://www.antivir.de> (für Privatanwender kostenlos!). Nachdem Sie den Registrierungsschlüssel per E-Mail erhalten haben, müssen Sie diesen in das Verzeichnis `/usr/lib/AntiVir` kopieren. Hinweis: Bitte achten Sie darauf, dass sich der Virenschanner regelmäßig auf den neuesten Stand bringt und aktivieren Sie deshalb in der Software vorhandene Mechanismen (avupdater) zur automatischen Aktualisierung. Nur so kann der Virenschanner wirkungsvoll und effektiv eingesetzt werden.

### Installation des Spamfilters Spamassassin

Die Installation des in Perl geschriebenen Spamfilters Spamassassin (<http://www.spamassassin.org>), der zur Einstufung eingehender E-Mails diese verschiedenen Tests (z.B. Überprüfung des syntaktischen und inhaltlichen Aufbaus einer E-Mail) unterzieht, ist denkbar einfach. Laden Sie sich von der Homepage die aktuelle Version herunter (<http://www.spamassassin.org/released/Mail-SpamAssassin-2.43.tar.gz>) und entpacken Sie diese mit `tar xvf Mail-SpamAssassin-2.43.tar.gz`. Wechseln Sie in das neu entstandene Verzeichnis (`cd Mail-SpamAssassin-2.43/`) und starten Sie die Vorbereitung der Installation mittels `perl Makefile.PL`. Hinweis: Sollte bei der Ausführung dieses Befehls eine Fehlermeldung (z.B. nicht erfüllte Abhängigkeiten etc.) erscheinen, müssen Sie sich vergewissern, dass alle benötigten Perlmodule (siehe Datei `INSTALL` der entpackten Spamassassin-Quellen) auf Ihrem System vorhanden sind.

Sobald dieser Befehl abgeschlossen ist, können Sie die Kompilierung der Software durch das Kommando `make` starten. Der Aufruf `make install` installiert schließlich die Software. Bevor Sie das Programm starten, sollten Sie einige Parameter in einer Konfigurationsdatei von Spamassassin ändern. Editieren Sie dazu die Konfigurationsdatei `/usr/share/spamassassin/10_misc.cf` und fügen Sie folgende Zeilen hinzu:

```
rewrite_subject      1
report_header       1
subject_tag         *****SPAM*****
use_terse_report    0
defang_mime         1
skip_rbl_checks     0
check_mx_attempts   3
check_mx_delay      5
```

Die erste Option bedeutet, dass der Betreff (engl. subject) einer E-Mail besonders gekennzeichnet/umgeschrieben (engl. rewrite) wird, sofern eine E-Mail durch die verschiedenen inhaltlichen Tests als unerwünschte Werbung (Spam) erkannt worden ist. Die folgende Anweisung (`report_header`) sorgt dafür, dass die Ergebnisse der Tests zur Einstufung einer E-Mail als Werbung in den Header einer E-Mail aufgenommen werden. Dadurch können Sie feststellen, warum eine E-Mail als unerwünschte Werbung eingestuft worden ist bzw. warum sie es nicht ist und können gegebenenfalls die durch Spamassassin durchgeführten Überprüfungsmechanismen anpassen. Als nächstes wird festgelegt, dass der Betreff einer E-Mail um den Text `*****SPAM*****` erweitert wird, sofern diese als Werbung eingestuft worden ist. Die vierte Anweisung zwingt Spamassassin, einen langen und ausführlichen Bericht (Report) über die einzelnen E-Mails zu führen. Die Option `defang_mime` ändert aus

Sicherheitsgründen den MIME-Typen einer E-Mail in text/plain, sofern diese als Werbung erkannt worden ist. Dieses Feature wurde entwickelt, da viele E-Mails den MIME-Typen text/html benutzen, der in manchen E-Mailprogrammen ohne Überprüfung angezeigt oder sogar ausgeführt wird (inkl. eventuell vorhandener, böser Skripte/Anhänge) und somit eine echte Sicherheitslücke darstellen kann. Damit Spamassassin den Absender einer E-Mail mit den als Versender von Spam bekannten Adressen vergleicht, gibt es die Option `skip_rbl_checks`, die durch unsere Einstellung aktiviert wird. Die vorletzte Option `check_mx_attempts` definiert die Anzahl der Überprüfungen, die der so genannte MX-Eintrag (Mail Exchange Record) der Domain des Urhebers einer E-Mail unterzogen wird. Der Mail Exchange Record definiert für eine Domain die Adresse eines Servers, an die diejenigen E-Mails geschickt werden müssen, die einen Empfänger innerhalb der lokalen Domain erreichen sollen und dient in diesem Fall dazu, die Gültigkeit der Domain des Urhebers einer E-Mail zu verifizieren. Die letzte Anweisung `check_mx_delay` gibt die Zeitspanne in Sekunden an, die bis zur erneuten Überprüfung des MX-Eintrages der Domain des Absenders einer E-Mail, gewartet werden soll. Speichern Sie die Konfigurationsdatei und starten Sie das Programm testweise mit dem Befehl `/usr/bin/perl /usr/local/bin/spamd -d -c &`. Hinweis: Der Pfad zu Ihrem Perl-Interpreter kann durchaus variieren, Sie erhalten des korrekten Pfad für Ihr System u.a. mit dem Befehl `type perl`. Des weiteren möchte ich, da die Anzahl der verfügbaren Konfigurationsmöglichkeiten von Spamassassin sehr umfangreich ist, an dieser Stelle auf die Dokumentation des Programms (<http://www.spamassassin.org/doc.html>) verweisen. Weitere Informationen zur Anpassung und Bedienung von Spamassassin (inkl. FAQ) finden Sie ebenfalls unter [http://www.spamassassin.org/doc/Mail\\_SpamAssassin\\_Conf.html](http://www.spamassassin.org/doc/Mail_SpamAssassin_Conf.html) bzw. unter <http://spamassassin.taint.org/faq/index.cgi?req=all>. Die eigentliche Installation von Spamassassin ist damit bereits beendet.

#### Vorbereitungen zur Installation von qmail-scanner

Damit ein- und ausgehende E-Mails auch auf Viren und unerwünschte Werbung geprüft werden, ist ein Eingriff in den internen Ablauf von qmail notwendig. Dazu gibt es ein Programm namens qmail-scanner, welches als eine Art Vermittler zwischen qmail und den externen Programmen (Virens Scanner, Spamfilter) auftritt. Bevor wir jedoch mit der eigentlichen Installation von qmail-scanner beginnen können, müssen wir zunächst eine Reihe Drittprogramme und Zusatzmodule installieren, die in der Regel nicht in dem normalen Umfang der marktüblichen Distribution enthalten sind. Zuerst müssen wir die freie Datenbank Berkeley DB installieren, deren aktuelle Version 4.1.25 Sie unter <http://www.sleepycat.com> herunterladen können (<http://www.sleepycat.com/update/snapshot/db-4.1.25.tar.gz>). Entpacken Sie auch diese Software mit `tar xvzf db-4.1.25.tar.gz` und wechseln Sie in das Unterverzeichnis `dist` (`cd db-4.1.25/dist`) des neu entstandenen Verzeichnisses. Starten Sie die Vorbereitung der Software durch Eingabe von `./configure` und rufen Sie nach Beendigung des Skriptes den Befehl `make` auf, der die Kompilierung des Programmes erledigt. Sobald dieser Vorgang abgeschlossen ist, können Sie die Software durch `make install` in das Verzeichnis `/usr/local` installieren. Kopieren Sie danach alle Dateien aus den Unterverzeichnissen `include` und `libs` des soeben installierten Programmes nach `/lib` bzw. `/usr/local/include`. Diese Aufgabe können Sie durch die Befehle `cp /usr/local/BerkeleyDB.4.1/include/* /usr/local/include` und `cp /usr/local/BerkeleyDB.4.1/lib/* /lib` erledigen. Ebenso benötigen Sie ein Programm namens `reformmime`, welches fester Bestandteil des Paketes `maildrop` ist, das Sie unter <http://download.sourceforge.net/courier/> finden. Laden Sie die Software herunter (<http://download.sourceforge.net/courier/maildrop-1.4.0.tar.gz>), entpacken Sie diese durch das Kommando `tar xvzf maildrop-1.4.0.tar.gz` und begeben Sie sich in das neu entstandene Verzeichnis `maildrop-1.4.0` (`cd maildrop-1.4.0`). Wie immer, müssen Sie die Vorbereitung der Software auch hier durch den Befehl `./configure` starten, `make` und `make install` kompilieren und installieren die Software schließlich. Die gleiche Vorgehensweise müssen Sie auch für die Software TNEF unpacker anwenden, die Sie auf der Internetseite <http://world.std.com/~damned/software.html> finden. Laden Sie die Software herunter (<http://belnet.dl.sourceforge.net/sourceforge/tnef/tnef-1.1.4.tar.gz>), entpacken Sie diese mit `tar xvzf tnef-1.1.4.tar.gz`, wechseln Sie in das neu erzeugte Verzeichnis (`cd tnef-1.1.4`) und rufen Sie nacheinander die Befehle `./configure`, `make` sowie `make install` auf. Neben diesen Drittprogrammen benötigen Sie fünf zusätzliche Perlmodule, wovon Sie bei bestehender Internetverbindung vier wie folgt installieren können:

```
perl -e ' use CPAN; install Bundle::CPAN'
```

```
perl -e ' use CPAN; install Time::HiRes'
perl -e ' use CPAN; install Bundle::libnet'
perl -e ' use CPAN; install DB_File'
```

Führen Sie die Befehle nacheinander aus und folgen Sie den Anweisungen der einzelnen Installationsprogramme. Beantworten Sie eventuell gestellte Fragen und wählen Sie nach Möglichkeit überall die Standardeinstellung, die hinter einer Frage meist durch Großbuchstaben angedeutet wird. Neben diesen vier Modulen müssen Sie ein Modul namens Unix::Syslog installieren, welches Sie unter <http://www.cpan.org/authors/id/M/MH/MHARNISCH/Syslog-0.97.tar.gz> finden. Laden Sie das Archiv herunter, entpacken Sie dieses `tar xvzf Syslog-0.97.tar.gz`, wechseln Sie in das Verzeichnis `syslog-0.97` (`cd syslog-0.97`) und führen Sie den Befehl `perl Makefile.PL` aus, der die Kompilierung und spätere Installation des Moduls vorbereitet. Sobald dieser Vorgang abgeschlossen ist, können Sie die Software wie gewohnt mit `make` und `make install` kompilieren bzw. installieren.

### Installation von qmail-scanner

Wir können uns nun endlich der Installation der Software qmail-scanner widmen und benötigen dazu die aktuelle Version 1.15, die Sie unter <http://belnet.dl.sourceforge.net/sourceforge/qmail-scanner/qmail-scanner-1.15.tgz> herunterladen müssen. Entpacken Sie die Software mit `tar xvzf qmail-scanner-1.15.tgz`, wechseln Sie in das neu entstandene Verzeichnis (`cd qmail-scanner-1.15`) und rufen Sie mit `./configure --help` eine Übersicht der zur Verfügung stehenden Optionen auf. Nach Durchsicht der möglichen Optionen habe ich mich für folgenden Aufruf entschieden: `./configure --qmaildir /var/qmail --spooldir /var/spool/qmailscan --bindir /var/qmail/bin --admin sebastian --domain beispiel.de --scanners "antivir,spamassassin" --notify recips,sender,admin --lang de_DE --archive no --redundant yes --log-details yes --fix-mime yes --add-dscr-hdrs yes --unzip yes --install`

Dieser Befehl bereitet die Installation des qmail-scanners vor und definiert das Verzeichnis `/var/qmail` als Basisverzeichnis der lokalen qmail-Installation. Die (Zwischen-) Speicherung der infizierten E-Mails erfolgt im Verzeichnis `/var/spool/qmailscan`, als Administrator habe ich den Benutzer `sebastian@beispiel.de` definiert, wobei hier die Angabe des Benutzer und der zugehörigen Domain durch zwei separate Optionen (`--admin` und `--domain`) erfolgt. Der Administrator ist auch die Person, die per E-Mail benachrichtigt wird, wenn eine E-Mail einen Virus enthält. Die folgende Option `--scanners` ermöglicht die Einbindung externer Programme als Virens Scanner und/oder Spamfilter, wobei neben den vorgestellten Programmen Spamassassin und antivir von H+BEDV zahlreiche andere Produkte unterstützt werden (z.B. Trend Interscan VirusWall, Kaspersky AVPLinux, F-Prot, Clam, Sophos Sweep, F-Secure etc.). Sollten Sie eine dieser Alternativen benutzen wollen, möchte ich Sie an dieser Stelle auf die zahlreichen Dokumentationen verweisen, die dem Quellcode des qmail-scanners beigelegt und in Auszügen ebenfalls unter <http://qmail-scanner.sourceforge.net/> abrufbar sind. Das Programm qmail-scanner kann die installierten Drittprogramme durch die Einstellung `--scanners auto` auf Wunsch auch automatisch erkennen. Die nächste Option (`--notify`) definiert die Personen, die im Falle eines Virenfundes benachrichtigt werden sollen, durch die gewählte Einstellung wird in einem solchen Fall der Empfänger (`recips`), der Absender (`sender`) und der Administrator benachrichtigt, um gegebenenfalls weitere Aktionen einzuleiten. Die beiden nächsten Optionen (`--lang` und `--archive no`) sorgen dafür, dass eine deutsche Spracheinstellung gewählt wird und bereits verarbeitete E-Mails nicht auf der Festplatte des Servers unter `/var/spool/qmailscan/archives` archiviert werden. Die Option `--redundant` ist dafür verantwortlich, dass auch eventuell angehängte Attachments sowie das Rohformat einer E-Mail überprüft werden. Mit Hilfe der Option `--log-details yes` legen Sie fest, dass Informationen über die Struktur jeder E-Mail in einer Logdatei gespeichert werden sollen. Sollte eine E-Mail einen ungültigen oder unbekanntes MIME-Typen enthalten, wird dieser aufgrund der Option `--fix-mime` korrigiert. Des Weiteren fügt qmail-scanner den Eintrag X-Qmail-Scanner zu jeder Nachricht, die er überprüft hat, hinzu (`--add-dscr-hdrs yes`). Die vorletzte Option (`--unzip`) sorgt dafür, dass auch komprimierte Archive entpackt und auf Viren überprüft werden. Schließlich erledigt die letzte Option direkt die Installation der Software, nachdem Sie eine kurze Zusammenfassung der von Ihnen gewählten Einstellungen überprüft und bestätigt haben. Aufgrund der Tatsache, dass das Perl-Skript nach der Installation mit einer speziellen Berechtigung laufen muss, kann es auf einigen Distributionen (z.B. Debian) zu enormen Problemen kommen, da diese den speziellen Modus für Perl-Skripte aus Sicherheitsgründen nicht unterstützen. Wechseln

Sie deshalb nach der Installation in das Unterverzeichnis *contrib* (*cd contrib*), rufen Sie die Befehle *make* sowie *make install* auf und korrigieren Sie die Berechtigung für das Skript */var/qmail/bin/qmail-scanner.pl* mit *chmod 0755 /var/qmail/bin/qmail-scanner-queue.pl*. Sie sollten die Installation des *qmail-scanners* überprüfen, in dem Sie durch das Kommando *su - qmaild* in die Rolle eines für die Installation des MTA *qmail* erzeugten Benutzers schlüpfen, den Pfad des Programms *qmailqueue* mit *export QMAILQUEUE=/var/qmail/bin/qmail-scanner-queue* exportieren und den Befehl */var/qmail/bin/qmail-scanner-queue -g* ausführen. Daraufhin sollten die folgenden Meldungen erscheinen:

```
perlscanner: generate new DB file
perlscanner: total of 8 entries.
```

Hinweis: Auf manchen Systemen erscheint zusätzlich zu den genannten Meldungen eine Fehlermeldung (ERROR: incorrect format on line 82 – skipped) und der Test wird abgebrochen. Editieren Sie in diesem Fall (als root) die Datei */var/spool/qmailscan/quarantine-attachments.txt* und ersetzen Sie in Zeile 82 die Leerzeichen zwischen *Virus-Content-Type:* und *Message/partial* durch einen Tab, so dass die besagte Zeile wie folgt aussieht: *message/partial Virus-Content-Type: Message/partial MIME attachments blocked by policy*. Speichern Sie die Datei und führen Sie als Benutzer *qmaild* den Test (*/var/qmail/bin/qmail-scanner-queue -g*) erneut durch. Falls wider Erwarten weitere Fehlermeldungen erscheinen, haben Sie bei der Installation des Programmes etwas falsch gemacht. Gehen Sie in diesem Fall die einzelnen Schritte erneut durch und konsultieren Sie im Zweifel die Hilfe/FAQ des *qmail-scanners* (siehe <http://qmail-scanner.sourceforge.net/FAQ.php>). Andernfalls können Sie jetzt durch den Befehl *exit* zurück in die Rolle des Benutzers *root* wechseln und *qmail* durch *sh /var/qmail/rc &* starten. Im Unterverzeichnis *contrib* (*cd qmail-scanner-1.13/contrib*) der entpackten Quellen des *qmail-scanners* können Sie durch den Befehl *./test\_installation.sh -doit* einen Test ausführen lassen, der eine Nachricht mit einem ungefährlichen Testvirus versendet. Wenn Ihr System korrekt installiert worden ist, wird die Nachricht abgefangen, der Administrator erhält insgesamt vier E-Mails (saubere und „verseuchte“ Ursprungsmail sowie Benachrichtigung über Viren- und Spamfund) und Sie können sicher sein, dass die Software ordentlich funktioniert. Fügen Sie außerdem folgende Zeilen zur Datei */etc/profile* hinzu:

```
QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue"
export QMAILQUEUE
```

Speichern Sie die Datei, loggen Sie sich aus und direkt wieder in Ihr System ein, damit die Änderungen aktiv werden. Zu guter Letzt müssen Sie *qmail* und *Spamassassin* durch die Kommandos *killall qmail-send* sowie *killall perl* beenden, damit wir uns der Entwicklung eines Startskriptes zuwenden können.

### Entwicklung eines Startskriptes

Da die Installation der benötigten Softwarekomponenten endlich beendet ist, können wir uns nun der Entwicklung eines Startskriptes widmen. Prinzipiell müssen wir drei verschiedene Programme starten, *qmail*, *vpopmail* und *Spamassassin*, wobei für *vpopmail* zwei verschiedene Prozesse (SMTP und POP3) gestartet werden müssen. Erzeugen Sie durch den Befehl *touch /etc/init.d/vqmail* das entsprechende Skript und schreiben Sie folgenden Code in diese Datei (Wichtiger Hinweis: Alle Pfadangaben wie z.B. */usr/bin/perl* müssen ggfs. an Ihre lokalen Gegebenheiten angepasst werden!):

```
#!/bin/bash
# Copyright (c) 2002 by Sebastian Wolfgarten
#
# homepage: http://www.wolfgarten.com
# e-mail: sebastian@wolfgarten.com
#
# Dieses Skript startet qmail (inkl. qmail-scanner), vpopmail
# und den Spamfilter SpamAssassin.
#
# Entwickelt wurde dieses Skript unter Debian Sarge, es sollte aber
# auf allen Unix/Linux-Systemen funktionieren (eventuell mit
# kleinen Anpassungen).
```

#

*# Definition des Pfades*

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*# Deklaration und Export der Umgebungsvariablen QMAILQUEUE*

QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue"

export QMAILQUEUE

*# Name des Programms*

NAME="qmail+vpopmail"

*# Kurze Beschreibung*

DESC="qmail mit vpopmail und SpamAssassin..."

*# Deklaration einiger Variablen*

QMAILHOME="/var/qmail"

VPOPMAILHOME="/home/vpopmail"

*# Welche Benutzer- bzw. Gruppen-ID hat der Benutzer qmaild bzw. die Gruppe nofiles?**# Habe ich jetzt den „useless use of cat“-Award gewonnen?*

USERID=`cat /etc/passwd | grep qmaild | awk -F: ' {print \$3}' `

GROUPID=`cat /etc/group | grep nofiles | awk -F: ' {print \$3}' `

*# Wichtiger Hinweis: Passen Sie die folgende Variable, die den vollständigen Namen**# Ihres Systems definiert, unbedingt an Ihre lokalen Gegebenheiten an! Bitte lesen Sie**# dazu auch die Kommentare am Ende dieses Skriptes.*

FQDN="server.beispiel.de"

*# Dieser Aufruf ueberprueft, ob das eigentliche Startskript von qmail (/var/qmail/rc)**# vorhanden ist. Falls nicht, wird das Skript beendet.*

QMAIL\_BIN="/var/qmail/rc"

test -x \$QMAIL\_BIN || exit 5

*# Dieser Aufruf ueberprueft, ob das Programm tcpserver installiert ist, welches fuer vpopmail**# dringend benoetigt wird. Falls nicht, wird das Skript beendet.*

VPOPMAIL\_BIN="/usr/local/bin/tcpserver"

test -x \$VPOPMAIL\_BIN || exit 5

*# Welche Programme sollen fuer vpopmail und SpamAssassin gestartet werden?**# Hinweis: Pfadangaben muessen ggfs. an Ihre lokalen Gegebenheiten angepasst werden.*DAEMON\_1="\$VPOPMAIL\_BIN -u \$USERID -g \$GROUPID -x \$VPOPMAILHOME/etc/tcp.smtp.cdb 0 \  
smtp \$QMAILHOME/bin/qmail-smtpd"DAEMON\_2="\$VPOPMAIL\_BIN -H -R 0 pop3 \$QMAILHOME/bin/qmail-popup \$FQDN \  
\$VPOPMAILHOME/bin/vchkpw \$QMAILHOME/bin/qmail-pop3d Maildir"

DAEMON\_3="/usr/bin/perl /usr/local/bin/spamd -d -c"

*# Welche Distribution wird benutzt? (Eigentlich ueberfluessig!)*

if [ -d /etc/rc2.d ]

then

```

# Wohl ein Debian-System
DIST=Debian

else

# Hierbei handelt es sich offensichtlich um ein SuSE oder sogar RedHat-System
DIST=SuSE

fi

set -e

# Der wichtigste Teil des Skriptes folgt nun, hier werden die einzelnen
# Programme gestartet bzw. gestoppt.
case "$1" in
    start)
        echo -n "Starte $DESC"
        echo "und ein bisschen mehr :-)"
        # Starte die Programme (z.B. qmail)
        $DAEMON_1 &
        $DAEMON_2 &
        $DAEMON_3 &
        $QMAIL_BIN &

        ;;
    stop)
        echo -n "Stoppe $DESC"
        # Sende ein killall
        # Hinweis: Sofern Sie andere Programme ausführen, die dauerhaft einen Perl-Interpreter
        # benutzen, müssen Sie den Befehl killall perl unbedingt anpassen und nur SpamAssassin
        # gezielt beenden (z.B. kill ProzessID).
        killall perl
        killall -TERM qmail-send
        killall -TERM tcpserver
        echo "Fertig!"

        ;;
    restart)
        $0 stop
        $0 start

        ;;
    *)
        echo "Benutzung: $0 {start|stop|restart}";
        exit 1
esac

```

Hinweis: Bitte modifizieren Sie den Ausdruck `FQDN="server.beispiel.de"` an die Gegebenheiten Ihres lokalen Systems und tragen Sie die vollständigen Domainnamen (rechnernamen.domain.tld) ein. Wenn der vollständige Name Ihres Systems beispielsweise `server1.firma.com` heißt, müssen Sie den Ausdruck in `FQDN="server1.firma.com"` ändern. Des Weiteren müssen Sie unter Umständen Pfadangaben (z.B. `/usr/bin/perl`) an Ihre lokalen Gegebenheiten anpassen. Überprüfen Sie vor dem Start dieses Skriptes unbedingt, ob alle benötigten Programme und Skripte in den jeweiligen Verzeichnissen vorhanden sind.

Das Skript sollte eigentlich sehr leicht verständlich sein, vielleicht noch kurz ein paar Erläuterungen zu folgenden Aufrufen:

```
DAEMON_1="$VPOPMAIL_BIN -u $USERID -g $GROUPID -x $VPOPMAILHOME/etc/tcp.smtp.cdb 0 \
smtp $QMAILHOME/bin/qmail-smtpd"
```

```
DAEMON_2="$VPOPMAIL_BIN -H -R 0 pop3 $QMAILHOME/bin/qmail-popup $FQDN \
$VPOPMAILHOME/bin/vchkpw $QMAILHOME/bin/qmail-pop3d Maildir"
```

Generell werden die Variablen, erkennbar durch ein vorangestelltes Dollar-Zeichen, durch die von uns zu Beginn des Skriptes definierten Werte ersetzt (siehe oben). Die ersten beiden Zeilen sorgen später für den Start des SMTP-Daemon, wobei die einzelnen Parameter die folgende Bedeutung haben:

- -u: Gibt die Userid (numerische Benutzerkennung) des Users qmaild an (wird automatisch ermittelt).
- -g: Gibt die Gruppenid (numerische Gruppenkennung) der Gruppe nofiles an, in der sich u.a. der Benutzer qmaild befindet. Auch dieser Wert wird automatisch ermittelt durch das Skript.
- -x: Startet den SMTP-Daemon unter Verwendung der Angaben aus der CDB-Datenbank. Diese Datei enthält eine Liste aller Hosts, die sich per POP3 authentifiziert haben und nun für eine gewisse Zeit (z.B: 30 Minuten) E-Mails über den lokalen Server versenden dürfen. Diese Datei liegt meist unter /home/vpopmail/etc/tcp.smtp.cdb

Die nächsten beiden Zeilen starten den POP3-Daemon, wobei hier die Parameter folgende Aufgaben erfüllen:

- -H: Durch den Parameter -H wird die Auflösung von Domainnamen durch den TCP-Server zwecks Performancesteigerung unterbunden.
- -R 0: Mit Hilfe dieser Einstellung wird verhindert, dass sich der TCP-Server Informationen über einen entfernten Host holt, der sich soeben mit dem Server verbunden hat. Dadurch sind ebenfalls Performancesteigerungen möglich.

Speichern Sie das Skript, setzen Sie die Ausführberechtigung durch das Kommando `chmod +x /etc/init.d/vqmail` und starten Sie die eierlegende Wollmilchsau mit `/etc/init.d/vqmail start`. Nach dem Start sollte der Befehl `ps aux` u.a. folgende Prozesse zeigen:

```
qmaild 12508 0.0 0.2 2004 620 ? S 2002 0:10 /usr/local/bin/tcpserver -u 1001 -g 103 -x
/home/vpopmail/etc/tcp.smtp.cdb 0 smtp /var/qmail/bin/qmail-smtpd
root 12509 0.0 0.2 2004 608 ? S 2002 0:24 /usr/local/bin/tcpserver -H -R 0 pop3
/var/qmail/bin/qmail-popup server.beispiel.de /home/vpopmail/bin/vchkpw /var/qmail/bin/qmail-pop3d Maildir
qmails 12511 0.0 0.1 1308 368 ? S 2002 0:54 qmail-send
qmail 12512 0.0 0.1 1260 416 ? S 2002 0:41 splogger qmail
root 12513 0.0 0.1 1252 272 ? S 2002 0:17 qmail-lspawn ./Maildir
qmailr 12514 0.0 0.1 1256 304 ? S 2002 0:01 qmail-rspawn
qmailq 12515 0.0 0.1 1244 304 ? S 2002 0:06 qmail-clean
root 12516 0.0 0.6 8788 1768 ? S 2002 1:34 /usr/bin/perl /usr/local/bin/spamd -d -c
```

Sofern dies nicht der Fall ist, müssen Sie das Startskript `/etc/init.d/vqmail`, die Logdateien `/var/log/messages` bzw. `/var/log/mail` sowie die gesamte Installation überprüfen, um die mögliche Ursache zu finden. Andernfalls sage ich herzlichen Glückwunsch zur erfolgreichen Installation von qmail, vpopmail, SpamAssassin und des Virens scanners AntiVir. Damit das Startskript beim Start des Servers ausgeführt wird, sind schließlich folgende Links in den Runleveln notwendig (für SuSE u.ä.):

```
ln -s /etc/init.d/vqmail /etc/init.d/rc3.d/S20vqmail
ln -s /etc/init.d/vqmail /etc/init.d/rc3.d/K03vqmail
```

Für Debian sehen diese Links wie folgt aus:

```
ln -s /etc/init.d/vqmail /etc/rc2.d/S20vqmail
ln -s /etc/init.d/vqmail /etc/rc0.d/K03vqmail
ln -s /etc/init.d/vqmail /etc/rc6.d/K03vqmail
```

Weitere Informationen zum Anlegen der Links in den entsprechenden Runleveln entnehmen Sie bitte der Dokumentation Ihrer Distribution. Sie können alle Dienste durch Eingabe von `/etc/init.d/vqmail start` manuell starten bzw. mit `/etc/init.d/vqmail stop` stoppen, beim Systemstart bzw. `-stop` werden die Dienste automatisch

gestartet und beendet. Die Installation und Konfiguration des Systems ist damit beendet, freuen Sie sich auf eine viren- und spamfreie Zeit :-)

#### Ausblick

Obwohl die Installation von qmail mit den diversen Erweiterungen sicherlich umfangreich und stellenweise schwierig ist, lohnt sich der Aufwand: Das System läuft bei mir seit Monaten ohne Probleme und ich kann von sehr hohen Erkennungsraten durch SpamAssassin berichten (ca. 90-95%). Vorbei die Zeit, in dem ich bösen Viren und unerwünschter Werbung mehr oder weniger schutzlos ausgeliefert war. Zusätzlich vereinfacht vpopmail die Administration sowie Konfiguration von qmail und kann seine Stärke insbesondere in großen (Firmen-) Netzwerken mit einer entsprechend hohen Anzahl von Benutzern bzw. im ISP-Bereich ausspielen. Ich möchte deshalb darauf hinweisen, dass der Hersteller von vpopmail, Inter7, weitere freie Software rund um qmail anbietet. Es lohnt sich also, regelmäßig einen Blick auf die Internetseite <http://www.inter7.com/qmail/> zu werfen und sich in die verschiedenen Mailing-Liste einzutragen. Besonders ans Herz legen möchte ich Ihnen die webbasierte Administrationsoberfläche qmailadmin von Inter7, die eine komfortable Konfiguration des Mailsystems durch die Administratoren und Endbenutzer erlaubt. Wer jedoch Lust hat, sich seine eigene Administrationsoberfläche zu basteln, der sollte einmal bei <http://www.php.net> vorbeischaun: Seit Version 4.05 gibt es eine erste, als experimentell gekennzeichnete Unterstützung von vpopmail in PHP. Dabei muss PHP mit der Option `--with-vpopmail=/home/vpopmail` übersetzt werden. Auch für Perl gibt es unter <http://bluedot.net/projects/vpopmail.html> bereits ein hervorragendes Modul zur Administration von vpopmail durch Perl. Viel Spaß und Erfolg :-)