



QMAIL

ein effizienter und sicherer
sendmail Ersatz

Dr. Erwin Hoffmann

feh@fehcom.de

<http://www.fehcom.de>

OSIE - Offene Systeme im Einsatz
Köln, 2001-3-2

Was ist QMAIL ?

QMAIL ist ein von Dan Bernstein entwickelter UNIX (E)SMTP- und QMTP- MTA.

- Die erste Beta-Version 0.70 wurde Januar 1996 zur Verfügung gestellt.
- Die Version 0.99 wurde von mir Anfang 1997 bei einem grossen Kölner Kunden eingerichtet.
- Aktuelle QMAIL-Version ist 1.03.

- QMAIL sollte auf jedem nur einigermaßen sauberen UNIX-Derivat laufen.
- QMAIL ist Bestandteil vieler Ports für populäre LINUX-Distributionen mit Ausnahme von SUSE.
- QMAIL ersetzt mittlerweile bei vielen ISPs sendmail, verlangt aber aufgrund seiner Philosophie gewisse Kenntnisse bei der Konfiguration.

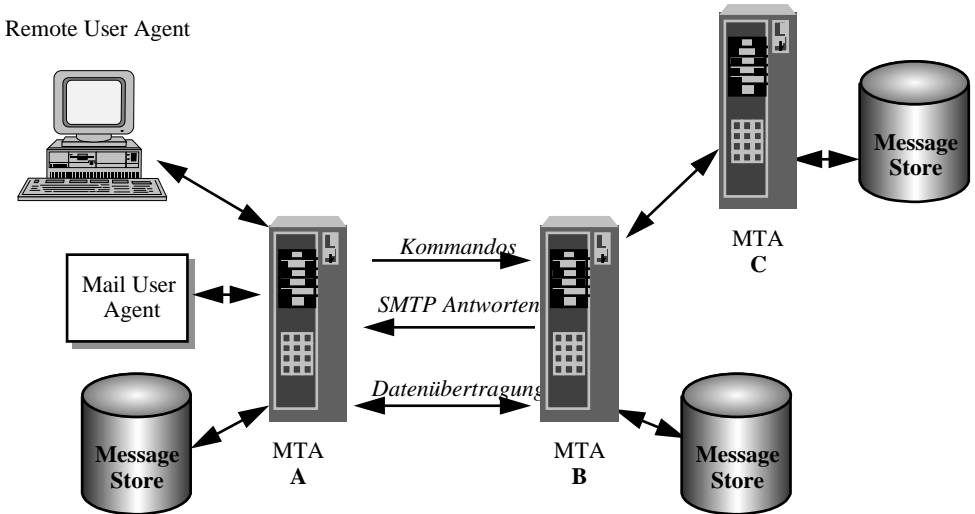
Warum QMAIL ?

QMAIL ist Teil von Dan J. Bernsteins' UNIX System-Software.

- Statt einer Server-Installation "Out-of-the-Box", wie sie z.B. bei SuSE-Linux vorliegt, verlangen die DJB-Alternativen einiges an SysAdmin-Know-How.
- Verfügbare Software-Pakete:
 - *qmail* statt *sendmail*
 - *ezmlm* statt *Majordomo*
 - *djbdns* statt *BIND*
 - *tcpserver* statt *INETD*
 - *multilog* statt *SYSLOG*
 - *daemontools* statt *rc-Skripte*
- Alle Pakete sind unter dem besonderen Vorsatz der Sicherheit, der Einhaltung der Standards, sowie der Geschwindigkeit entwickelt worden. Für QMAIL und djbdns gibt es \$\$\$ für gefundene Sicherheitslücken!

Philosophie von QMAIL

MTA, MS, UA



QMAIL besitzt im Gegensatz zu sendmail eine segmentierte Architektur und entspricht damit dem MTA-Modell.

- Jeder Prozess läuft unter einer anderen UID.
- Einziger SETUID-Prozess ist *qmail-queue*.
- Einziger Root-Prozess ist *qmail-lspawn*.
 - *qmail-lspawn* ändert seine effektive UID (=> Empfänger), bevor ein benutzerspezifisches Programm aufgerufen wird.

Philosophie von QMAIL

Umfang

QMAIL entspricht allen aktuellen (E)SMTP-RFCs und ist 8-Bit "clean".

- SMTP-Authentisierung wird durch einige QMAIL-Patche gewährleistet:
 - STARTTLS: RFC 2487
 - AUTH: RFC 2554 (login, plain, CRAM-MD5)
 - POP3-Login vor SMTP
- QMAIL bietet Unterstützung für
 - POP3-Server (nativ)
 - IMAP4
 - LDAP
 - MySQL/Postgresql/Oracle
- QMAIL bringt seinen eigenen E-Mail Listenmanager EZMLM mit.
- QMAIL setzt in der Regel auf einem eigenen *tcpserver*-Prozess auf und vermeidet daher Probleme mit *inetd*.
- Dan Bernstein hat ausserdem einen Ersatz für den *syslog*-Daemon und einige weitere daemon-tools.

Philosophie von QMAIL

Prozesse

QMAIL arbeitet modular:

- *qmail-smtpd* wird von inetd/xinetd/tcpserver aufgerufen.
- *qmail-send* mit mehreren Prozessen zum Versenden auslaufender Mail.
- *qmail-rspawn* Queue-Manager für auslaufende Mail
- *qmail-remote* versendet E-Mail an entfernte MTAs
- *qmail-lspawn* Queue-Manager für einlaufende Mails
- *qmail-local* liefert E-Mail an lokale Empfänger aus
- *qmail-clean* Aufräumprozess für die Queues
- *qmail-pop3d* POP3-Serverprozess
- *splogger* QMAIL Log-Daemon

```
qmail1 123 0.0 0.4 824 292 ? S 07:26 0:00 splogger qmail
qmailq 126 0.0 0.3 816 220 ? S 07:26 0:00 qmail-clean
qmailr 125 0.0 0.3 820 232 ? S 07:26 0:00 qmail-rspawn
qmails 112 0.0 0.4 860 264 ? S 07:26 0:00 qmail-send
root 124 0.0 0.3 820 232 ? S 07:26 0:00 qmail-lspawn ./Mailbox
```

Philosophie von QMAIL

Interne Sicherheit

	lines	words	chars	files
qmail-1.03	16617	44780	395243	279
sendmail-8.9.1	55059	179376	1229121	54
zmailer-2.2e10	57595	205524	1423624	227
smail-3.2	62331	246140	1701112	151
exim-2.02	70102	283295	2172786	128

Anzahl und Größe der *.c und *.h Dateien
(von Peter Samuel - AUUG 1998-09-15)

QMAIL "Keep It Simple" Prinzip:

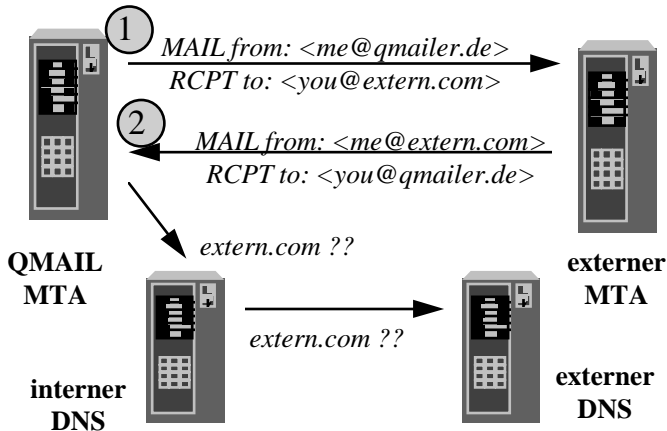
- QMAIL hat die kleinste Codebasis aller MTAs, mit gleichzeitig der größten Anzahl von Dateien.
- QMAIL Source-Dateien sind kompakt.
- QMAIL vermeidet C-Lib, speziell *stdio* und ersetzt diese durch eigene robuste Funktionen (auch z.B. *syslog*).

QMAIL vermeidet das Standard `sendmail` /`var/mail`-Verzeichnis. Jeder Anwender hat eine personalisierte Mailbox/Maildir:

- `~/Mailbox`, `~/mbox`
- `~/Maildir/`

Philosophie von QMAIL

SMTP und DNS/MX



Zwei Szenarien:

- *qmail-remote* (1) überprüft beim Senden den A/MX-Record des Empfänger-MTAs (RCPT To:)
 - ausser der MTA ist per SMTP-Route eingetragen
- *qmail-smtpd* (2) ermöglicht einen Check des Absenders (MAIL from:)
 - ausser für spezielle MTAs/Domänen (SPAMCONTROL Patch)

Philosophie von QMAIL

Sendeprozess

QMAIL arbeitet beim Versenden von E-Mail multitasking und asynchron:

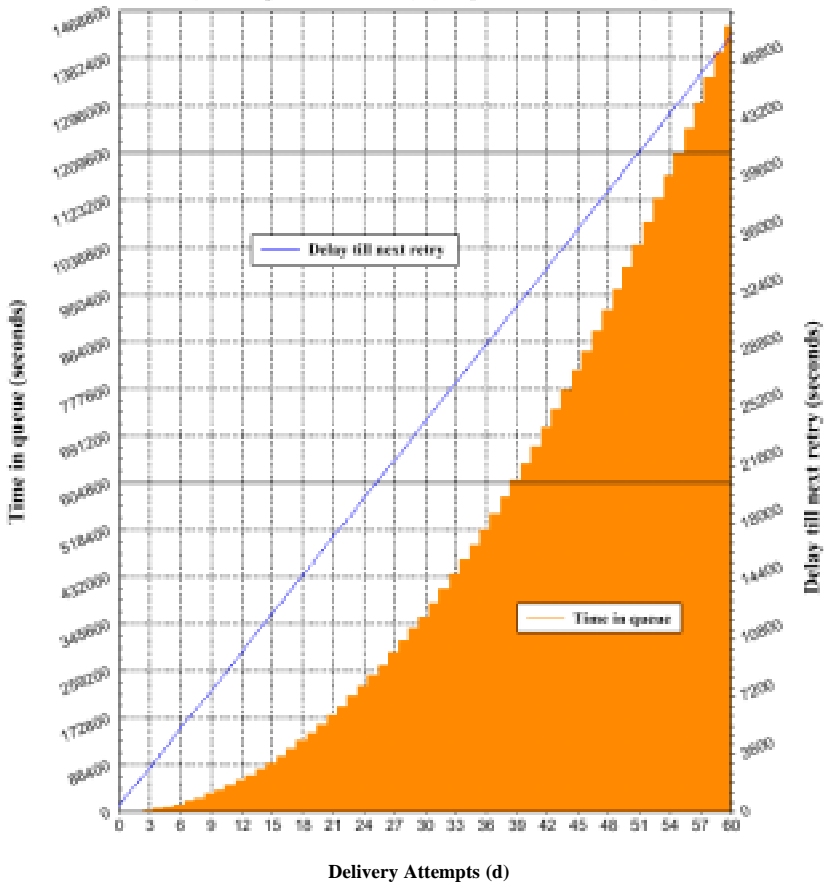
- Für jeden Sendeprozess wird eine neue Instanz von *qmail-remote* oder *qmail-local* gestartet.
 - Defaultlimit 20
 - Compilelimit 120
- Nicht auslieferbare E-Mails (deferred) wird individuell nach einem quadratischen Reschedule-Verfahren abgearbeitet.
 - Lokal auszuliefernde E-Mails:
 - $time\ in\ queue = 100 * delivery\ attempt$
 - $delay\ till\ next\ retry = 200 * delivery\ attempt + 100$
 - An andere Rechner zu versendende E-Mails:
 - $time\ in\ queue = 400 * delivery\ attempt$
 - $delay\ till\ next\ retry = 800 * delivery\ attempt + 400$
 - Erfolgt auf zwei Verbindungsversuche (mit mindestens 2 Minuten Abstand) keine Antwort des entfernter Rechner, pausiert QMAIL für eine Stunde und versucht anschliessend einen *Slow-Start*.
 - Die TCP-Verbindungsinformationen werden in der Queue gespeichert.

Philosophie von QMAIL

Sende Retry-Schedule

Quadratic Retry Schedule for qmail-send (remote)

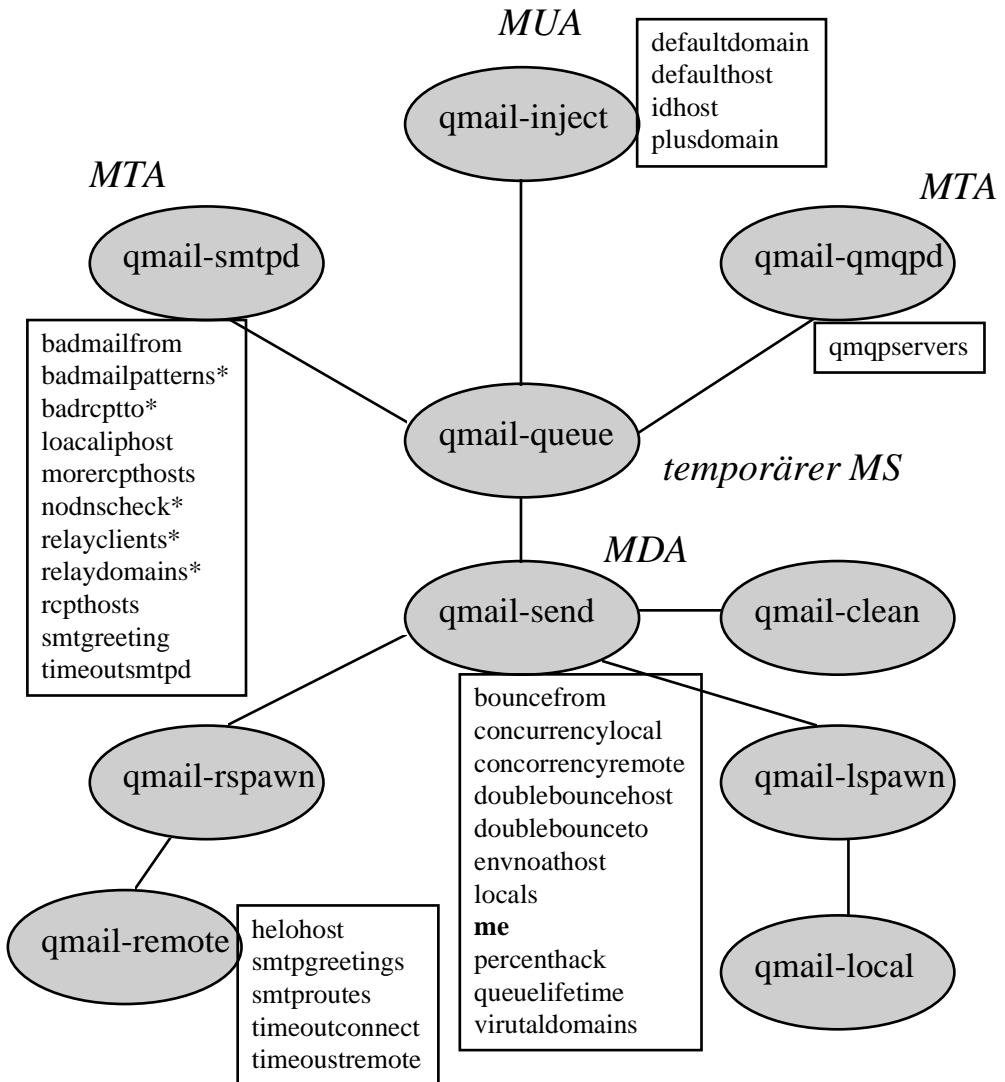
(time in queue = $400 * d^2$) (delay time = $800 * d + 400$)



(von Peter Samuel - AUUG 1998-09-15)

Arbeitsweise von QMAIL

Sende- und Empfangsprozesse



Arbeitsweise von QMAIL

Konfigurationsdateien

Die QMAIL-Konfiguration erfolgt über
Kontrolldateien im Verzeichnis
`/var/qmail/control/`.

- Die wichtigste Kontrolldatei ist *me*, in der der Hostname des MTA definiert wird.
- Zweitwichtigste Kontrolldatei ist *rcpthosts*, in der festgehalten wird, wie der FQDNs im E-Mail Umschlag (Mail From:) lauten muss, damit QMAIL die E-Mail in den Message-Store überführt
 - was nicht impliziert, dass diese auch ausgeliefert wird!
- Die Konfigurationsdateien sind modulspezifisch (qmail-send, qmail-smtpd)!

☞ Eine QMAIL Grundkonfiguration wird durch das Installationsskript `./config` vorgenommen.

☞ Defaultangaben können während QMAIL-Laufzeit über Environment-Variablen verändert werden.

☞ Maildelivery-Aktionen werden über `.qmail-` Dateien gesteuert.

Arbeitsweise von QMAIL

QMAIL Startup

QMAIL verfügt über vordefinierte Startskripts unter `/var/qmail/boot/`.

```
#!/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 ./Mailbox splogger qmail
```

Start von QMAIL über *tcpserver*:

```
tcpserver -v -u 7791 -g 2108 -c 100 \
0 smtp /var/qmail/bin/qmail-smtpd 2>&1 \
| /var/qmail/bin/splogger smtpd 3 &
```

Arbeitsweise von QMAIL

XINETD Integration

Start der SMTP- und POP3-Dienste über
xinetd.conf:

```
service smtp
{
    socket_type      = stream
    protocol        = tcp
    wait            = no
    user            = qmaild
    server          = /var/qmail/bin/tcp-env
    server_args     = /var/qmail/bin/qmail-smtpd
    env             = NODNSCHECK=""
    log_type       = FILE /var/log/mail
    log_on_success  = HOST
    log_on_failure  = HOST RECORD

service pop3
{
    socket_type      = stream
    protocol        = tcp
    wait            = no
    user            = root
    server          = /var/qmail/bin/qmail-popup
    server_args     = orion.fehcom.de \
                    /bin/checkpassword \
                    /var/qmail/bin/qmail-pop3d Maildir
    log_type       = FILE /var/log/xinetd.log
    log_on_success  = HOST
    log_on_failure  = HOST RECORD
}
```

Arbeitsweise von QMAIL

SUSE Startup Skript

Einbetten in /sbin/init.d/:

```
#!/bin/sh
#/sbin/init.d/rc.qmail
#
. /etc/rc.config
test "$SMTP" = yes || exit 0
case "$1" in
    start)
        echo "Initializing SMTP port (qmail):"
        csh -cf '/var/qmail/rc &'
        ;;
    stop)
        echo -n "Shutting down SMTP port (qmail):"
        killproc -TERM /var/qmail/bin/qmail-send
        echo
        ;;
    alarm)
        echo -n "Alarm processsing of E-Mails (qmail):"
        killproc -ALRM /var/qmail/bin/qmail-send
        echo
        ;;
    *)
        echo "Usage: $0 {start|stop|alarm}"
        exit 1
esac
exit 0
```

Arbeitsweise von QMAIL

E-Mail-Verarbeitung

QMAIL empfängt einlaufende E-Mail über drei Mechanismen:

- STMP: *qmail-smtpd*
- QMQP: *qmail-qmtpd*
Dan's *Quick Mail Queueing Protocol*
- lokal: *qmail-inject*, *mailsubj*

Diese Programme geben die E-Mail an *qmail-queue* weiter, wo sie

- in die eigentliche Nachricht (unter Hinzufügen einer "Received: " Zeile) und
- zweimal den Umschlag aufgeteilt wird.
- Bei lokalen Nachrichten wird *qmail-lspawn* und im Anschluß *qmail-local* aufgerufen und im Postfach des (existierenden !) Empfängers abgelegt.
- Bei Nachrichten für entfernte Empfänger wird *qmail-rspawn* und *qmail-remote* zum Versenden der Nachricht an den entfernten MTA bemüht.

Arbeitsweise von QMAIL

Queue-Struktur

Die QMAIL-Queue lebt unter `/var/qmail/queue/.../` und besitzt folgenden Aufbau:

- `/var/qmail/queue/pid/tempfile`
eindeutige temporäre Datei
- `/var/qmail/queue/mess/0..22/nnnnn`
Hardlink nach `/var/qmail/queue/pid/tempfile` mit inode als Namen. Beinhaltet Nachrichten-Kopf und -Mitteilung.
`/var/qmail/queue/pid/tempfile` wird gelöscht.
- `/var/qmail/queue/intd/nnnnn`
Umschlag der E-Mail in Bearbeitung
- `/var/qmail/queue/todo/nnnnn`
Senderadresse nach Bearbeitung
- `/var/qmail/queue/lock/trigger`
Named Pipe zur Kommunikation mit `qmail-send`
- `/var/qmail/queue/info`
Senderadresse im Umschlag nach Bearbeitung
- `/var/qmail/queue/local/0...22/nnnn`
lokale Empfängeradresse nach Bearbeitung
- `/var/qmail/queue/remote/0...22/nnnn`
remote Empfängeradresse nach Bearbeitung
- `/var/qmail/queue/bounce`
vorübergehend unzustellbare E-Mails

Arbeitsweise von QMAIL

Maildir vs. Mailbox

QMAIL verlangt, dass die benutzerspezifischen Postfächer nicht unter `/var/mail/usr` sondern im jeweiligen `$Home`-Verzeichnis abgelegt werden.

- QMAIL läßt zwei Arten von Postfächern zu:
 - Standard Mbox-Format - E-Mails werden in dieser Datei konkatinert.
 - Maildir - E-Mails werden in Unterverzeichnissen als getrennte Dateien aufbewahrt.
- Vor- und Nachteile von `$HOME/Maildir/`:
 - *maildirmake* erzeugt Maildir in `$HOME` und muss in Benutzer-Generierungsskripte eingebunden (statt Standard-Mbox) sowie Environment-Variable `$MAIL/$MAILDIR` angepasst werden.
 - Lokale UAs wie *mail* verstehen das Maildir-Format aber nicht (\Rightarrow *mutt*, *procmail*).
 - Maildir wird für POP-User (*qmail-pop3d*) benötigt.
 - Statt *qmail-pop3d* kann *qpopper* für Mbox eingesetzt werden
 - Mittels des Kommandos *maildir2mbox* wird eine E-Mail on-the-fly von Maildir nach Mbox transferiert.

Arbeitsweise von QMAIL VERP

QMAIL nutzt intern ein Verfahren, das Dan Bernstein als "Variable Envelope Return Path" (VERP) bezeichnet.

- Eine E-Mail Adresse kann hierbei um eine bzw. mehrere Extensions mit folgender Syntax erweitert werden:

user@qmailer.de => user-extension@qmailer.de

- "extension" wird (falls kein anderer Benutzer mit Namen "user-extension" existiert) mit einer lokalen, benutzerspezifischen Konfigurationsdatei identifiziert und kann somit als Kommando verstanden werden.
- Die Verkettung mehrere Extensions ist möglich, ebenso eine Defaultverarbeitung.
- Das VERP-Verfahren ist Aufgabe des Message Store und kann sowohl beim Senden einer E-Mail (*qmail-inject*) als auch typischerweise beim Empfang (*qmail-local*) von E-Mails genutzt werden.

Arbeitsweise von QMAIL

.qmail (dot-qmail) Files

QMAIL nutzt für den Empfangsprozess *qmail-local* Kontroll- und Steuerungsdateien, die

- systemweit unter `/var/qmail/alias/.qmail-xxxx` (Alias-User) bzw.
- benutzerspezifisch unter `$HOME/.qmail-yyyy`

abgelegt werden können.

Aufbau von .qmail

```
# Erwin's .qmail-default Datei
|preline /user/ucb/vacation erwin (Programmzeile*)
&erwin_hoffmann@compuserve.com # (Forwarding)
/home/erwin/Mailbox.sos (Mailbox Delivery*)
/home/erwin/Maildir/ (Maildir Delivery*)
```

* hier darf in .qmail kein x-Bit gesetzt sein

Falls bei .qmail `o+w` und `g+w` gesetzt ist, wird die Ausführung gestoppt.

- Normalerweise ist die Datei .qmail nicht existent bzw. leer. Dann findet eine Defaultdelivery statt.

Arbeitsweise von QMAIL

.qmail Files und VERP

Wird eine E-Mail an den lokalen Account <erwin-extension-neu@qmailer.de> geschickt, geht QMAIL folgendermassen vor:

- *\$HOME/.qmail-erwin-extension-neu* wird gesucht und ausgewertet
- *\$HOME/.qmail-erwin-extension-default* wird gesucht und ausgewertet
- *\$HOME/.qmail-default* wird gesucht und ausgewertet

E-Mails an nicht existierende Accounts werden mit der gleichen Logik über den QMAIL Alias-Benutzer abgewickelt (*/var/qmail/alias*).

- */var/qmail/alias/.qmail-default* regelt hierbei die systemweite QMAIL Defaultverarbeitung

Arbeitsweise von QMAIL

Aliasing

QMAIL bietet drei Mechanismen für Alias-User:

- `/var/qmail/alias/.qmail-aliasname`
- *qmsmac* - sendmail kompatible Alias-Liste
 - `/var/qmail/alias/.qmail-default:`

```
| /var/qmsmac/bin/qmsmac
```
 - Über die Hilfsroutine *newaliases* wird eine kompilierte Alias-Liste unter `/var/qmsmac/etc` erzeugt.
 - *qmsmac* nimmt keinen Dublettencheck vor.
- *fastforward* - erweiterter Mechanismus mit der Möglichkeit, Alias-Listen einzubetten.
 - `/var/qmail/alias/.qmail-default:`

```
| fastforward -d /etc/aliases.cdb  
&postmaster@qmailer.de
```
 - Auch hier wird per *newaliases* eine kompilierte Alias-Liste aufgebaut,
 - *fastforward* unternimmt allerdings einen Dublettencheck und erlaubt über Returncodes und Programmparameter eine gesteuerte Alias-Verarbeitung.

QMAIL Spezialitäten

Environment-Variablen

QMAIL nutzt zur Kontrolle der E-Mails ein System von statischen und temporären (d.h. per E-Mail) Environment-Variablen.

- Statische Environment-Variablen:
 - `qmail-inject`
 - `QMAILUSER`, `MAILUSER`, `USER`, `LOGNAME` - Lokaler Name des Absenders in der E-Mail Header-Zeile "From:"
 - `QMAILHOST`, `MAILHOST` - Name des sendenden MTAs
 - `QMAILNAME`, `MAILNAME` - der persönliche Name
 - `QMAILSUSER`, `QMAILSHOST` - E-Mail Umschlag "Mail From:"
 - `QMAILDEFAULTDOMAIN` - Domän-Name für unqualifizierte Absenderadresse
 - `QMAILIDHOST` - Hostname für die im Header einzufügende Message-ID.
 - `QMAILPLUSDOMAIN` - wird an Absenderadress angehängt, die mit einem "+" enden

QMAIL Spezialitäten

Environment-Variablen (2)

- qmail-smtpd
 - DATABYTES - maximale Größe einer zu akzeptierenden E-Mail
 - RELAYCLIENT - IP-Adresse(n) von Rechnern, die den QMAIL MTA als Relay benutzen dürfen
- Temporäre Environment-Variablen:
 - qmail-local:
 - SENDER- Absenderadresse im Umschlag
 - NEWSENDER - Weiterleitungsadresse im zugestellten Umschlag
 - RECIPIENT - Empfängeradresse im Umschlag in Form von local@domain
 - USER - Unix User
 - HOME - Unix User Home-Verzeichnis
 - HOST - Domain-Teil der Empfängeradresse RECIPIENT
 - HOST2... HOST4 - "domain=host4.host3.host2.suffix"
 - LOCAL - lokaler (User) Teil von RECIPIENT
 - EXT - QMAIL Extension
 - EXT2 .. EXT4 - "local=user-EXT2-EXT3-EXT4"
 - DTLINE und RPLINE - "Delivered-To:" und "Return-Path:" Information im Header
 - UFLINE - UUCP-Stil "From_" Zeile im Header

QMAIL Spezialitäten

tcpserver

Serverprozesse (z.B. SMTPD) können auf mehrere Arten gestartet werden:

- als Daemon-Prozesse (z.B. *httpd*)
- unter Kontrolle von *inetd*
- unter Kontrolle von *xinetd*
- unter Kontrolle von *tcpserver*

tcpserver (und *tcpclient*) stellt eine Implementierung von UCSPI dar, d.h. des *UNIX Client-Server Program Interface* auf Grundlage des TCP-Protokolls

- Im Gegensatz zu *inetd/xinetd*, wo die Serverprozesse über Argumentlisten aufzusetzen sind, arbeitet *tcpserver* mit Kommandoverkettung und Environment-Variablen.
- *tcpserver* kann wie *tcpwrapper* eingesetzt werden, indem in einer Datenbank IP-Adressen von berechtigten/unberechtigten Hosts (on-the-fly) gehalten werden.
- *tcpserver* erlaubt das Setzen von Concurrency-Limits für Verbindungen.

QMAIL Spezialitäten

POP3 und IMAP4

QMAIL unterstützt mittels *qmail-pop3d* das Postoffice Protokoll. Voraussetzungen sind allerdings

- die Einrichtung von Maildirs
- die Verwendung eines externen checkpassword-Programms (oder via LDAP, mysql etc.)
- APOP wird mit Patches unterstützt
- *fetchmail* und *pullmail* (NT) Unterstützung
- Weitere POP3-Server:
 - *vpopmail* (<http://www.inter7.com>)
 - QUALCOMM's *qpopper* (3.0.2) (<http://www.qpopper.org>)

IMAP4 Zugriff wird über externe IMAP4-Server ermöglicht (Maildir!):

- University of Washington *UW-IMAP*
- *courier-imap* (<http://www.inter7.com>)
- TLS und stunnel werden optional unterstützt

QMAIL Spezialitäten

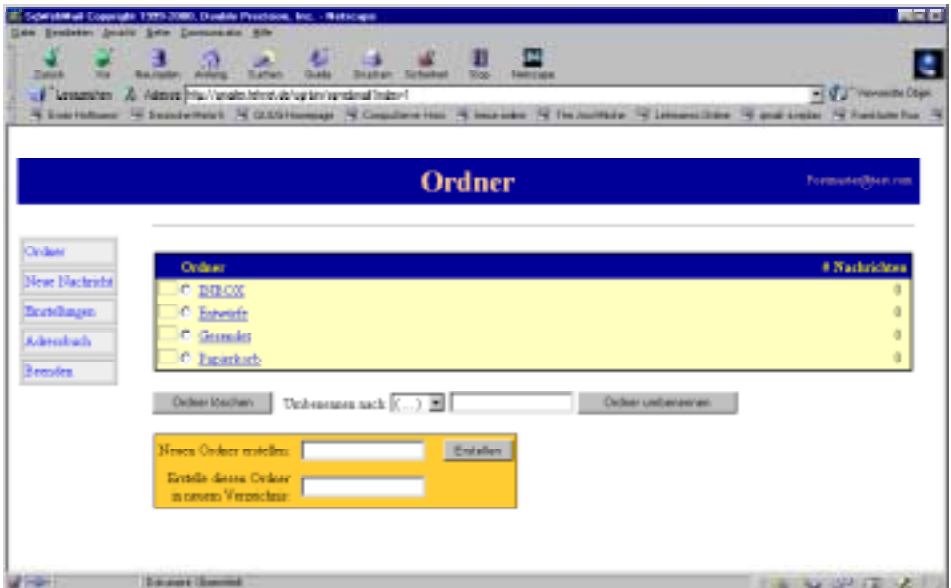
Web-Interface

Mit den Zusatzpaketen

- *vpopmail* und
- *sqwebmail*

lässt sich ein effizienter E-Mail-Server für Benutzer in "virtuellen Domänen" aufsetzen.

- Benutzerverwaltung über MySQL/PHP sowie Quota-Support für die Benutzer ist optional.
- Die Web-Oberfläche lässt sich über Konfigurationsdateien anpassen.



QMAIL Spezialitäten

Authentisierung

Es gibt eine Reihe von Patches, die Authentisierungsfunktionen bereit stellen:

- SMTP-after POP - Relaying von E-Mails wird erst nach erfolgreichem Aufbau einer POP3 (oder IMAP4) Session gewährt.
- STARTTLS - SMTP-E-Mail-Austausch über eine gesicherte SSL/TLS-Verbindung (Client- und Server)
- SMTP-Authentisierung gemäß RFC 2554 (login, plain, CRAM-MD5) für den QMAIL SMTP-Client.

Die Benutzer-Authentisierung erfolgt über das eigenständige Paket checkpassword, für das es auch eine PAM-Erweiterung gibt.

QMAIL Spezialitäten

LDAP Support

Für ISPs und POP-Toaster eignet sich besonders, die POP-Benutzer nicht als lokale UNIX-User sondern in einer LDAP-Datenbank zu halten. Hierzu gibt es für QMAIL ein umfangreiches Patch (<http://www.nrg4u.com/>) mit folgenden Eigenschaften (Auszug):

- Users and virtual domains in an LDAP database
- No local accounts needed
- Supports size quotas on user maildirs and mbox
- Automatic creation of home- and maildir's
- Handles replies with new qmail-reply
- Extensive logging in qmail-smtpd and qmail-pop3d
- Supports OpenLDAP 1.2.X and Mozilla Directory SDK
- Support for SHA, MD5, MD4, RIPE-MD160 and clear text passwords
- Support for NS-MTA-MD5 encrypted passwords used by Netscape Mailserver
- Support for TLS (SSL) encryption of SMTP mail transport

QMAIL als Internet MTA

Relaying

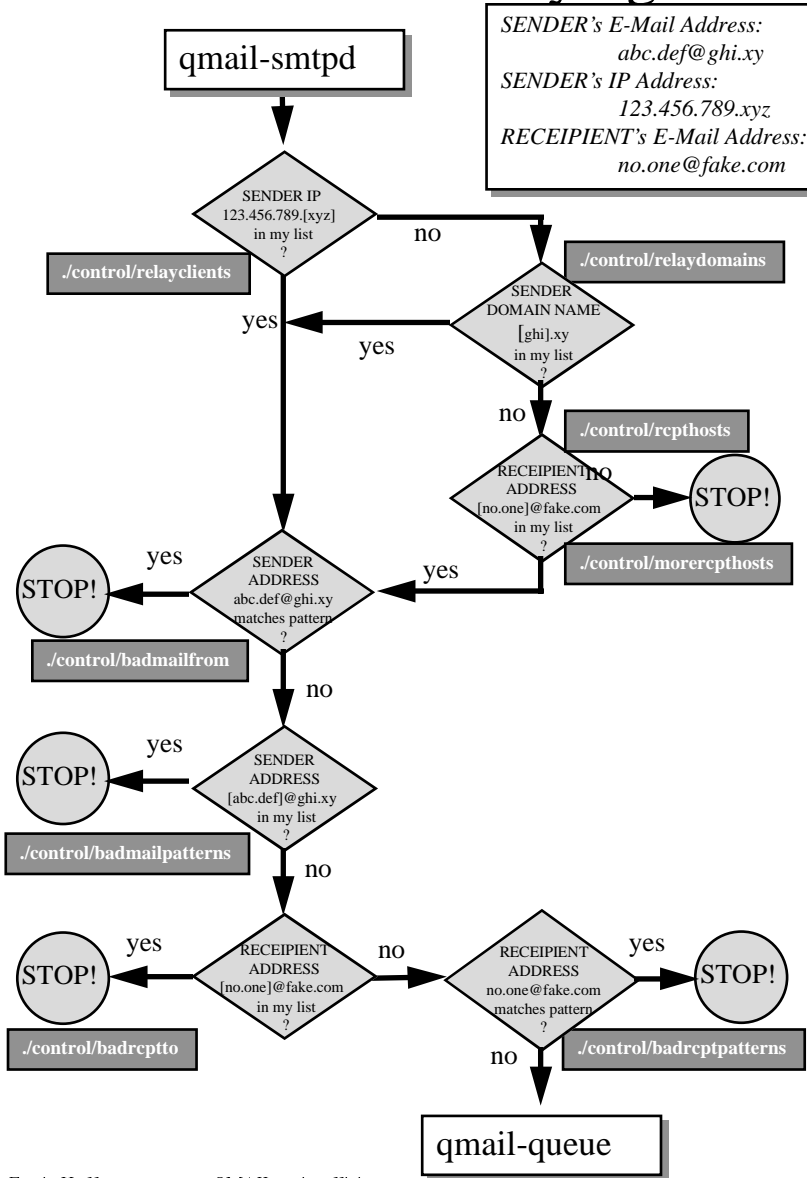
Unter Relaying wird die Eigenschaft eines MTAs bezeichnet, einlaufende E-Mails auch dann zu akzeptieren und weiterzuleiten, wenn sie nicht für die eigene Domäne bestimmt sind (=> offenes Relay).

recipient@mta.domain.com@mta-relay.de

- In der Basiskonfiguration von QMAIL ohne *rcpthosts* Kontrolldatei arbeitet QMAIL als offenes Relay.
- QMAIL kann über die Environment-Variable RELAYCLIENT und mittels *tcpserver* als selektives Relay (IP-Adresse) konfiguriert werden.
- Alternativ kann mittels meines SPAMCONTROL Patches (inkl. relaying über IP-Adresse, Domain-Name) ein zusätzliches Logging von abgewiesenen E-Mails vorgenommen werden

QMAIL als Internet MTA

Selective Relaying



QMAIL als Internet MTA

Virtual Domains

Das Einrichten von virtuelle Domänen unter QMAIL bedarf mehrerer Schritte:

- Der MX-Record der virtuellen Domäne muss auf die reale zeigen.
- QMAIL muss E-Mails für die virtuelle Domäne als eigene akzeptieren => Eintrag in `/var/qmail/control/rcpthosts`

```
qmailer.de  
virtual.com
```

- Eintrag der virtuellen Domäne in Datei `/var/qmail/control/virtualdomains`

```
virtual.com:newmta
```

- Erzeugen eines `.qmail`-Files mit forwarding-Informationen:

```
/var/qmail/alias/.qmail-newmta
```

```
|forward $LOCAL@mta.domain.com
```

- Eventuell Eintrag einer SMTPROUTE Information in `/var/qmail/control/smtproutes`

```
mat.domain.com: [12.34.56.78]
```

QMAIL als Internet MTA

Host Masquerading

Schritt 1:

- /var/qmail/control/defaultdomain

```
devel.domain.com
```

- Unqualifiziertes "From:" Absenderadresse erhalten nun "devel.domain.com" hinzugefügt.

Schritt 2:

- UNIX Users können ihren "From:" Header mit Environment-Variables setzen

```
export QMAILHOST=some.domain
export QMAILNAME="Erwin Hoffmann"
export QMAILUSER=Erwin.Hoffmann"
export QMAILINJECT=f
```

- Dies wird zu

From: Erwin Hoffman <Erwin.Hoffmannn@some.domain>

QMAIL als Internet MTA

Anti-Spam

Für QMAIL existieren eine Reihe von Anti-Spam Patches:

- Filtern von Spam E-Mail auf Adress- und Domainbasis (Wildcard!)
- DNS-Lookup für Sender-Domäne

tcpserver ermöglicht darüber hinaus die Einbeziehung von unerwünschten Sende-MTAs aufgrund der

- Relay Black Liste RBL
- ORBS
- Mail-Abuse

die simultan ausgewertet werden können.

☞ Richtig eingerichtete QMAIL MTAs finden keinen Platz auf irgendwelchen Blacklisten!

- Content-Typ Filtering ist über Standard-Mechanismen der .qmails Files möglich

QMAIL als Internet MTA

Anti-Virus

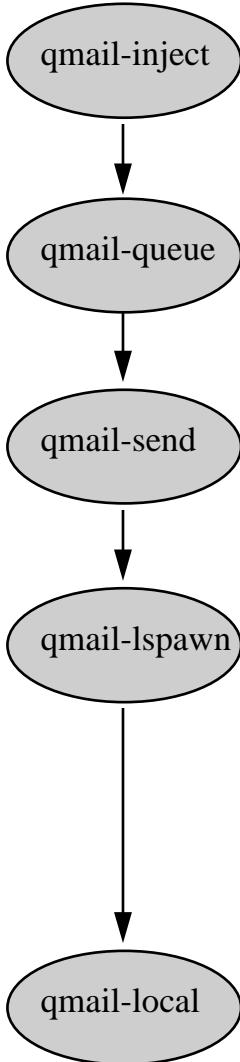
Die Erfahrung mit dem Melissa- und ILOVEYOU-Virus zeigt, dass MTAs über effektive Content-Filter-Mechanismen verfügen sollten.

QMAIL kann zwei populäre Anti-Viren-Implementierungen nutzen:

- Scan4Virus - Virus Scan Wrapper
(<http://www.geocities.com/jhaar/scan4virus/>)
- AMaViS E-Mail Wrapper
(<http://satan.oih.rwth-aachen.de/AMaViS/>)
 - Unterstützte Viren Scanner
 - Trend's Virus Scanner
 - MacAfee's (NAI's) Virus Scanner
 - Sophos's "sweep" Virus Scanner
 - H+BEDV Antivir Scanner
 - AVP AVPLinux Scanner
 - Alle Implementierungen klinken sich in die *qmail-queue* ein und scannen die E-Mail
- Weiterhin gibt es einige QMAIL spezifische Content- und Attachment-Typ Filtertools

QMAIL im UNIX Umfeld

Lokale E-Mails



Nachricht:

To: fred

Hi.

...vollständiger E-Mail-Umschlag und -Header:

From: erwin@qmailer.de

To: fred@qmailer.de

E-Mail wird sicher auf Platte geschrieben.

=> *qmail-send* wird aufgerufen.

Umschlag-Empfänger:

- fred@qmailer.de => qmailer.de lokal !

qmail-lspawn ./Mailbox

- Gibt es eine lokale mailbox fred?
- Ist fred in qmail-users? (Nein)
- Gibt es einen Account fred?
- Ist fred's UID $\neq 0$?
- Ist ~fred erreichbar für den qmail User?
- Gehört ~fred fred?

=> *qmail-local* !

qmail-local fred -fred fred " " qmailer.de \

joe@qmailer.de ./Mailbox

- Existiert ~fred/.qmail? (Nein)
- E-Mail wird nach ~/fred/Mailbox geschrieben.

QMAIL im UNIX Umfeld

QMAIL Extensions

qmail-inject

Nachricht:

To: fred

Hi.

...vollständiger E-Mail-Umschlag und -Header:

From: erwin@qmailer.de

To: fred-sos@qmailer.de

qmail-queue

E-Mail wird sicher auf Platte geschrieben.

=> *qmail-send* wird aufgerufen.

qmail-send

Umschlag-Empfänger:

- fred@qmailer.de => qmailer.de lokal !

qmail-lspawn ./Mailbox

- Gibt es eine lokale mailbox fred-sos ? (Nein)
- Ist fred-sos in qmail-users? (Nein)
- Gibt es einen Account fred-sos ? (Nein)
- Gibt es einen Account fred ? (Nein)
- Ist fred's UID \neq 0
- Ist ~fred erreichbar für den qmailp User?
- Gehört ~fred fred?

=> *qmail-local* !

qmail-lspawn

qmail-local fred -fred fred-sos - sos qmailer.de \

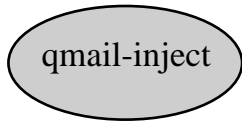
joe@qmailer.de ./Mailbox

- Existiert ~fred/.qmail- (Ja) "/.Extramail"
- E-Mail wird nach ~/fred/Extramail geschrieben.

qmail-local

QMAIL im UNIX Umfeld

Virtuelle Domänen



Nachricht:

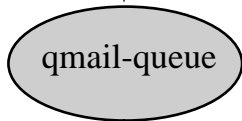
To: dummy@virtual.de

Hi.

...vollständiger E-Mail-Umschlag und -Header:

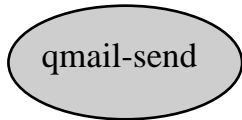
From: erwin@qmailer.de

To: dummy@virtual.de



E-Mail wird sicher auf Platte geschrieben.

=> *qmail-send* wird aufgerufen.



Umschlag-Empfänger:

- dummy@virtual.de ? Lokal ? (Nein)
- dummy@virtual.de ? virtualdomains (Ja)
=> virtualdomains: "dummy@virtual.de:fred"
=> versand an: fred-dummy@virtual.de



qmail-lspawn ./Mailbox

- Gibt es eine lokale mailbox fred-dummy ? (Nein)
- Ist fred-dummy in qmail-users? (Nein)
- Gibt es einen Account fred-sos ? (Nein)
- Ist fred's UID ¹ 0
- Ist ~fred erreichbar für den qmailp User?
- Gehört ~fred fred?

=> *qmail-local* !

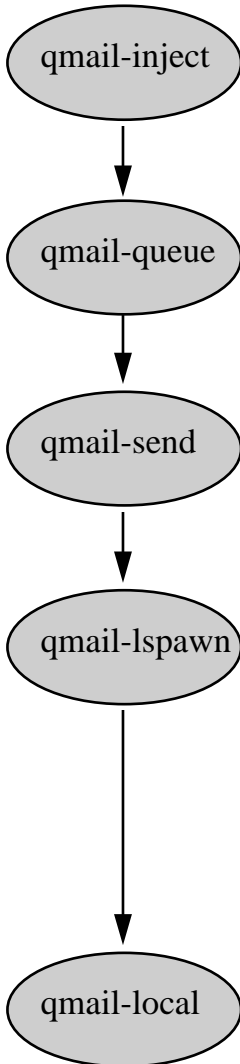


qmail-local fred -fred fred-dummy - dummy qmailer.de \
joe@qmailer.de ./Mailbox

- Existiert ~fred/.qmail-dummy? (Nein)
- Existiert ~fred/.qmail-default? (Ja) "./Dummymail"
- E-Mail wird nach ~/fred/Dummymail geschrieben.

QMAIL im UNIX Umfeld

Lokale Aliasnamen



Nachricht:

To: help

Hi.

...vollständiger E-Mail-Umschlag und -Header:

From: erwin@qmailer.de

To: help@qmailer.de

E-Mail wird sicher auf Platte geschrieben.

=> *qmail-send* wird aufgerufen.

Umschlag-Empfänger:

- fred@qmailer.de => qmailer.de lokal !

qmail-lspawn ./Mailbox

- Gibt es eine lokale mailbox fred?
- Ist fred in qmail-users? (Nein)
- Gibt es einen Account fred?
- Ist fred's UID \neq 0
- Ist ~fred erreichbar für den qmailp User?
- Gehört ~fred fred?

=> *qmail-local* !

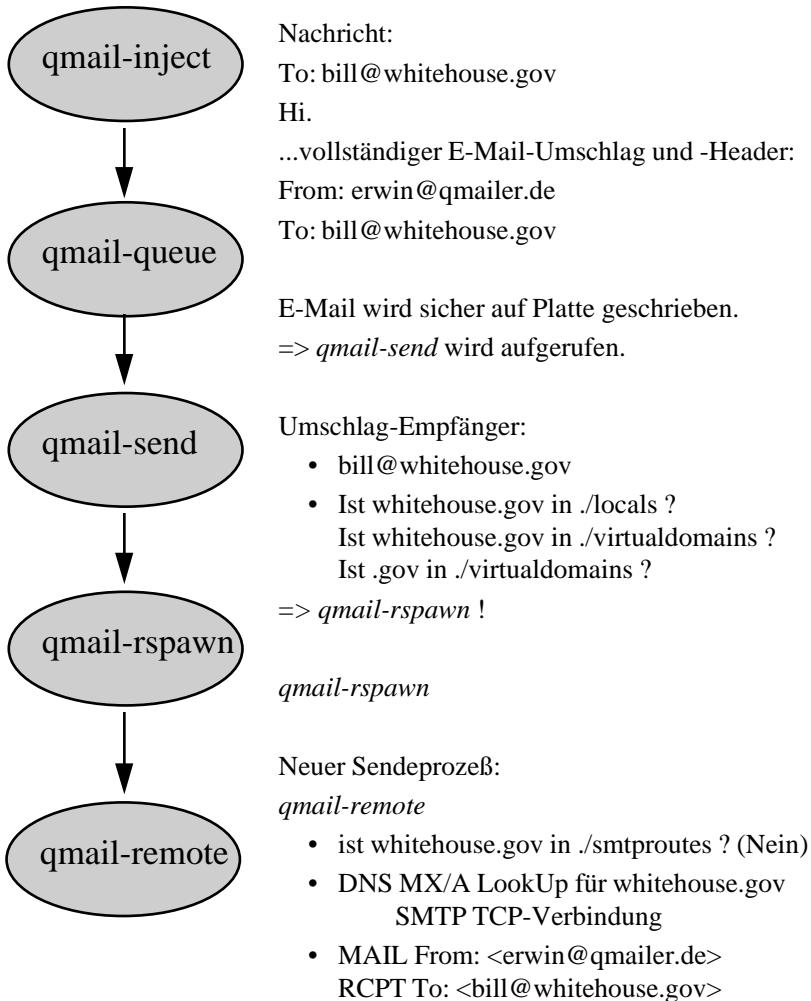
qmail-local fred -fred fred " " qmailer.de \

joe@qmailer.de ./Mailbox

- Existiert ~fred/.qmail? (Nein)
- E-Mail wird nach ~/fred/Mailbox geschrieben.

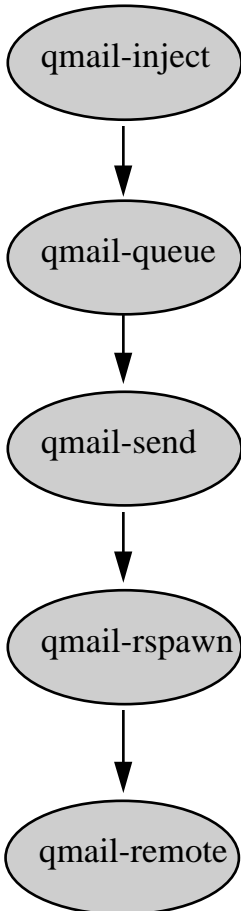
QMAIL im UNIX Umfeld

E-Mail an entfernte Hosts



QMAIL im UNIX Umfeld

Null-Client



Nachricht:

To: bill@whitehouse.gov

Hi.

...vollständiger E-Mail-Umschlag und -Header:

From: erwin@qmailer.de

To: bill@whitehouse.gov

E-Mail wird sicher auf Platte geschrieben.

=> *qmail-send* wird aufgerufen.

Umschlag-Empfänger:

- bill@whitehouse.gov
- Ist whitehouse.gov in `./locals` ?
Ist whitehouse.gov in `./virtualdomains` ?
Ist .gov in `./virtualdomains` ?

=> *qmail-rspawn* !

qmail-rspawn

Neuer Sendeprozess:

qmail-remote

- ist whitehouse.gov in `./smtproutes` ? (Ja)
whitehouse.gov:kremlin.rus
- DNS A-RR LookUp für kremlin.rus
SMTP TCP-Verbindung
- MAIL From: <erwin@qmailer.de>
RCPT To: <bill@whitehouse.gov>

EZMLM

Easy Mailing Listen Manager

QMAIL kommt mit einem rudimentären Mailinglisten-Programm, verfügt aber mit dem

- EZMLM (Version 0.53) über einen leistungsfähigen Mailinglistenmanager dessen Funktion durch das Patch
- EZMLM-IDX (Version 0.40) noch beachtlich erweitert wird.
- EZMLM erlaubt offene und moderierte Mailinglisten (Abonnenten und Beiträge) mit remoter Administration und Archivfunktion.
- EZMLM-IDX verfügt über ein
 - WEB-Interface und ein
 - WEB-Archiv.
- EZMLM setzt vollständig auf das QMAIL VERP-Verfahren auf.
 - Subscription und Unsubscription sowie Management geschehen via *listenname-kommando@host.domain.suffix*
 - EZMLM bietet eine Schnittstelle zu *mysql*
 - EZMLM ermöglicht Listen-Nesting und Berichtslisten

EZMLM

Administrations WEB-Interface

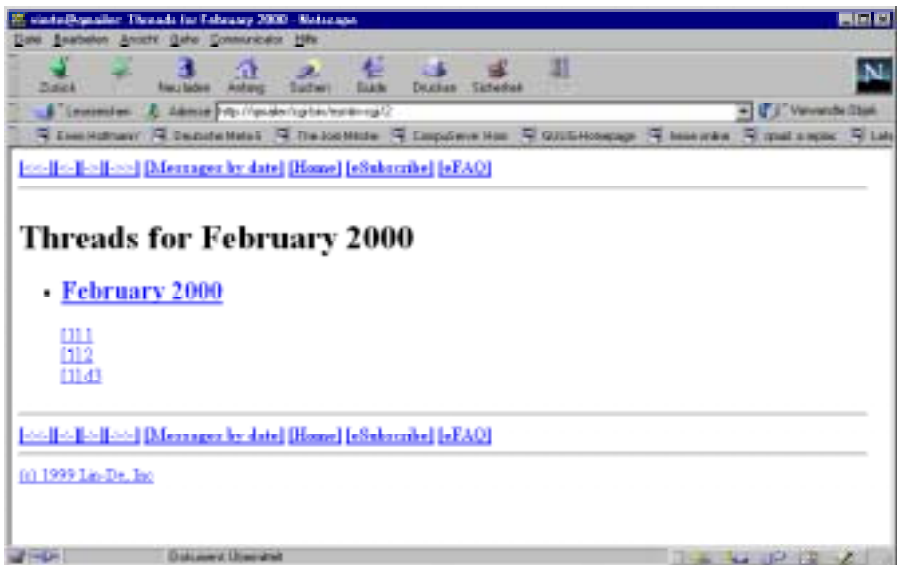
EZMLM-IDX kann über eine WEB/Cgi-Script komplett administriert werden (EZMLM-Web).

- Einrichten von Listen
- Einrichten von Benutzern
- Listenkonfiguration



EZMLM WEB Archiv

Seit der Version 0.40 bietet EZMLM-IDX eine Web-basierte Archivfunktion, in der die Beiträge nach Thema (Thread) und Datum sortiert sind.



QMAIL

URL-Auswahl

- QMAIL Info
 - <http://www.qmail.org>
 - <http://cr.yip.to/djb.html>
 - <http://x42.com/qmail/cookbook/>
 - <http://www.flounder.net/qmail/qmail-howto-v2.html>
 - <http://www.elysium.pl/members/brush/smtp-auth/index.html>
 - <http://www.fehcom.de/qmail.html>
- Anti SPAM
 - <http://maps.vix.com/rbl/>
 - <http://www.orbs.org/>
 - <http://www.obtuse.com/smtpd.html>
 - <http://spam.abuse.net/spam/>
 - <http://www.summersault.com/chris/techno/qmail/qmail-antispam.html>
- Anti Virus
 - <http://satan.oih.rwth-aachen.de/AMaViS/>
 - <http://www.geocities.com/jhaar/scan4virus/>
 - <http://em.ca/~bruceg/qmail-qfilter/>
 - <http://www.superscript.com/qtools/intro.ht>

QMAIL

So what?

Nachteile von QMAIL:

- Komplexe Struktur
- Fragmentierte Konfiguration
- IPv6 Unterstützung unklar
- Viele gute Features müssen über Patches eingespielt werden
- Für viele Fragen und Ergänzungen gibt es mehrere Lösungen
- Wann die nächste Version von QMAIL (2.0) kommt, ist unklar
- Ein Buch über QMAIL bei O'Reilly läßt (immer noch) auf sich warten....