!!! ACHTUNG - evtl. veraltet - ACHTUNG !!!

Diese Seite wurde zuletzt am 9. Juli 2014 um 10:35 Uhr geändert.

qmail

qmail anhalten

```
qmailctl stop
```

Debian-Pakete installieren

```
aptitude install openssl libssl-dev
```

qmail um tls und custom-error-messages erweitern

```
cd /usr/local/src/netqmail-1.06
wget
ftp://ftp.bluemetaljackets.de/qmail/tls_20110119_qmail-queue_custom_error_v1
_FOR_net-qmail-1.06_auth.patch
patch < tls_20110119_qmail-queue_custom_error_v1_FOR_net-
qmail-1.06_auth.patch
make clean
make
make setup check
make cert
```

(Sollte man bereits im Besitz eines „richtigen“ Zertifikates, z. B. von http://www.startssl.com/ sein, einfach den Key und die Certs hintereinander in eine Datei servercert.pem)

von micro$oft angestoßener inkompatibilität entgegenwirken

micro$oft soll mit hotmail der erste e-mail-provider gewesen sein, der gegen den „freien standard“ RFC 2822 Section 2.3 (http://tools.ietf.org/html/rfc2822#section-2.3) „verstoßen“ hat…

leider gibt es mittlerweile neben anderen providern auch clients, die es micro$oft nachmachen.

ABER: D. J. Bernstein wäre nicht D. J. Bernstein, wenn er nicht schon vor mehr als einem jahrzehnt ein „gegen-tool“ dafür entwickelt hätte: fixcrio!

leider bietet es in der original-fassung keine tls-unterstützung, aber hier hat Parallels (http://kb.parallels.com/en/6763) eine lösung entwickelt!

```
wget http://cr.yp.to/ucspi-tcp/ucspi-tcp-0.88.tar.gz
tar xzf ucspi-tcp-0.88.tar.gz
cd ucspi-tcp-0.88
```

```
 wget http://djbware.csi.hu/patches/ucspi-tcp-0.88.errno.patch
 patch < ucspi-tcp-0.88.errno.patch
 wget
ftp://ftp.neumannsland.de/qmail/ucspi-tcp_fixcrio_with_tls-support.patch
 patch < ucspi-tcp_fixcrio_with_tls-support.patch
 make
 cp fixcrio /usr/bin/fixcrio
 sed -i '/\/var\/qmail\/bin\/qmail-smtpd/ c\/usr/bin/fixcrio
\\\n/var/qmail/bin/qmail-smtpd \\' /var/qmail/supervise/qmail-smtpd/run
```

stündlichen cron-job erstellen

```
 cat <<EOF > /etc/cron.hourly/update_tmprsadh
 #!/bin/sh
 /var/qmail/bin/update_tmprsadh > /dev/null 2>&1
 cd /etc/qmail
 /usr/bin/wget -N http://curl.haxx.se/ca/cacert.pem > /dev/null 2>&1
 /bin/chown vpopmail:vchkpw cacert.pem > /dev/null 2>&1
 /bin/chown -h vpopmail:vchkpw clientcert.pem > /dev/null 2>&1
 /bin/chown vpopmail:vchkpw dh1024.pem > /dev/null 2>&1
 /bin/chown vpopmail:vchkpw dh512.pem > /dev/null 2>&1
 /bin/chown vpopmail:vchkpw rsa512.pem > /dev/null 2>&1
 /bin/chown vpopmail:vchkpw servercert.pem > /dev/null 2>&1
 EOF
 chmod 755 /etc/cron.hourly/update_tmprsadh
 /etc/cron.hourly/update_tmprsadh
```

fake-smtpd (bzw. Blacklists)

```
 sed '/\/var\/qmail\/bin\/qmail-smtpd/ i\\/usr\/bin\/rblsmtpd \\'
/var/qmail/supervise/qmail-smtpd/run
```

(wenn man keine clients, welche normalerweise über dynamisch vergebene ip-adressen mit dem internet verbunden sind, bedienen muss, kann man rblsmtpd mit dem schalter „-r“ auch eine oder mehrere blacklists übergeben!)

qmail neustarten

```
 qmailctl start
```

simscan

Debian-Pakete installieren

```
aptitude install clamav-daemon spamassassin p0f
```

(System-) Gruppen und Benutzer anlegen

```
addgroup --system simscan
adduser --system --ingroup simscan --home /var/qmail/simscan simscan
```

ripmime

Installation

```
cd /usr/local/src
wget http://www.pldaniels.com/ripmime/ripmime-1.4.0.9.tar.gz
wget http://qmail.tjc.fi/files/ripmime-1.4.0.9-permissions.patch
tar xzf ripmime-1.4.0.9.tar.gz
cd ripmime-1.4.0.9
patch < ../ripmime-1.4.0.9-permissions.patch
make
make install
```

Konfiguration

```
cat <<EOF > /var/qmail/control/ssattach
.bat
.bin
.cmd
.com
.exe
.scr
EOF
chmod 644 /var/qmail/control/ssattach
```

clamav-Rechte anpassen

```
usermod -a -G simscan clamav
usermod -a -G clamav simscan
chown -R simscan:clamav /var/lib/clamav/
chown -R simscan:clamav /var/run/clamav/
chown -R simscan:clamav /var/log/clamav/
sed -i s/User\ clamav/User\ simscan/g /etc/clamav/clamd.conf
sed -i s/DatabaseOwner\ clamav/DatabaseOwner\ simscan/g
/etc/clamav/freshclam.conf
```

Spamassassin

Konfiguration

```
sed -i s/ENABLED=0/ENABLED=1/ /etc/default/spamassassin
```

Dienst starten

```
/etc/init.d/spamassassin start
```

Installation

```
cd /usr/local/src
wget
http://netcologne.dl.sourceforge.net/project/simscan/simscan/simscan-1.4.0/s
imscan-1.4.0.tar.gz
wget http://qmail.jms1.net/simscan/simscan-1.4.0-clamav.3.patch
tar xvzf simscan-1.4.0.tar.gz
cd simscan-1.4.0
patch < ../simscan-1.4.0-clamav.3.patch
./configure --enable-clamav=y --enable-attach=y --enable-spam=y --enable-
received=y --enable-custom-smtp-reject
make
make install-strip
/var/qmail/bin/simscanmk -g
```

Mail-(v)Server-Integration

Zusätzlich zur Integration von ClamAV und Spamassassin in die E-Mail-Warteschlange, wird durch das „=“ vor :allow eine DNS-Abfrage durchgeführt und im Fehlerfall wird die E-Mail nicht an den smtpd (qmail) sondern an den **rblsmtpd** (ucspi-tcp) übergeben:

```
sed -i
s/:deny/=:allow,QMAILQUEUE="\/var\/qmail\/bin\/simscan"\\n:allow,RBLSMTPD="N
o Reverse DNS."/ /etc/tcp.smtp
qmailctl cdb
```

dspam

dspam-Repository hinzufügen

```
wget http://packages.kirya.net/kirya_squeeze.sources.list
wget -O -
```

```
http://packages.kirya.net/Kirya.netDebianpackagesVerificationKey.asc | apt-
key add -
 aptitude update
```

(In sid ist bereits wieder eine aktuelle Version enthalten, weshalb dieser Schritt in whezzy wieder überflüssig werden dürfte!?)

Debian-Pakete installieren

```
 aptitude install dspam procmail
```

MySQL-Datenbank und -Benutzer anlegen

```
 mysql --host=<HOST> --user=root --password -e "CREATE DATABASE `<DB>`; \
 CREATE USER '<USER>'@'<FROM_HOST>' IDENTIFIED BY '<PASSWORD>'; \
 GRANT USAGE ON * . * TO '<USER>'@'<FROM_HOST>' IDENTIFIED BY '<PASSWORD>' \
 WITH MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR
0 MAX_USER_CONNECTIONS 0; \
 GRANT SELECT , INSERT , UPDATE , DELETE , CREATE , DROP ON `<DB>` .  * TO
'<USER>'@'<FROM_HOST>';"
```

platzhalter

```
 mysql --host=<HOST> --user=<USER> --password
 [[...]]
 mysql> source /usr/share/doc/libdspam7-drv-mysql/sql/mysql_objects-4.1.sql
 [[...]]
 mysql> source /usr/share/doc/libdspam7-drv-mysql/sql/virtual_users.sql
 [[...]]
 mysql> ALTER TABLE `dspam_signature_data` ENGINE = InnoDB;
 [[...]]
 mysql> ALTER TABLE `dspam_stats` ENGINE = InnoDB;
 [[...]]
 mysql> ALTER TABLE `dspam_token_data` ENGINE = InnoDB;
 [[...]]
 mysql> ALTER TABLE `dspam_virtual_uids` ENGINE = InnoDB;
 [[...]]
 mysql> ALTER TABLE `dspam_preferences` ENGINE = InnoDB;
 [[...]]
 mysql> quit
```

platzhalter

Konfiguration

```
 sed -i s/StorageDriver\ \/usr\/lib\/dspam\/libhash_drv.so/StorageDriver\
\/usr\/lib\/dspam\/libmysql_drv.so/ /etc/dspam/dspam.conf
```

```
mv /etc/dspam.d/mysql.conf{,_debian}
cat <<EOF > /etc/dspam.d/mysql.conf
MySQLServer    <HOST>
MySQLPort      3306
MySQLUser      <USER>
MySQLPass      <PASSWORD>
MySQLDb        <DB>
MySQLCompress  true
MySQLReconnect true
EOF
chown dspam:dspam /etc/dspam.d/mysql.conf
chmod 640 /etc/dspam.d/mysql.conf
```

platzhalter

```
sed -i s/START=no/START=yes/ /etc/default/dspam
```

Training

```
mkdir -p /usr/local/src/training/{ham,spam}
cd /usr/local/src/training
wget http://spamassassin.apache.org/publiccorpus/20030228_spam.tar.bz2
tar xvjf 20030228_spam.tar.bz2 --strip=1 -C spam
wget http://spamassassin.apache.org/publiccorpus/20050311_spam_2.tar.bz2
tar xvjf 20050311_spam_2.tar.bz2 --strip=1 -C spam
rm spam/cmds
wget http://spamassassin.apache.org/publiccorpus/20030228_easy_ham.tar.bz2
tar xvjf 20030228_easy_ham.tar.bz2 --strip=1 -C ham
wget
http://spamassassin.apache.org/publiccorpus/20030228_easy_ham_2.tar.bz2
tar xvjf 20030228_easy_ham_2.tar.bz2 --strip=1 -C ham
wget http://spamassassin.apache.org/publiccorpus/20030228_hard_ham.tar.bz2
tar xvjf 20030228_hard_ham.tar.bz2 --strip=1 -C ham
rm ham/cmds
dspam_train dspam /usr/local/src/training/spam /usr/local/src/training/ham
```

(Mit libhash würde es zwar viiiel schneller gehen, dafür ist der Speicherbedarf dann aber auch viiiel höher, also: per „screen“ über Nacht laufen lassen!)

Dienst starten

```
/etc/init.d/dspam start
```

Benutzerspezifisches Training

```
cat <<EOF > /etc/cron.daily/dspam_reclass
#!/bin/sh
```

```
 DOMAINS="/home/vpopmail/domains"
 VUSERINFO="/home/vpopmail/bin/vuserinfo"
 JUNK="Maildir/.Junk/cur"
 ISJUNK="Maildir/.IsJunk/cur"
 NOJUNK="Maildir/.NoJunk/cur"
 DSPAM="/usr/bin/dspam"
 for DOMAIN in \$( ls -1 \$DOMAINS ) ; do
   for USER in \$( ls -1 \$DOMAINS/\$DOMAIN ) ; do
     if \$VUSERINFO \${USER}@\${DOMAIN} > /dev/null ; then
 # sicherstellen, dass alle Verzeichnisse vorhanden sind:
       if [[|! -d \$DOMAINS/\$DOMAIN/\$USER/Maildir/.Junk ]] ; then
 # weil die dash keine "Brace Expansion" unterstützt drei mkdir-Aufrufe:
         mkdir -p -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.Junk/cur
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.Junk/new
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.Junk/tmp
         chown -R vpopmail:vchkpw \$DOMAINS/\$DOMAIN/\$USER/Maildir/.Junk
       fi
       if [[|! -d \$DOMAINS/\$DOMAIN/\$USER/\$ISJUNK ]] ; then
         mkdir -p -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.IsJunk/cur
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.IsJunk/new
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.IsJunk/tmp
         chown -R vpopmail:vchkpw \$DOMAINS/\$DOMAIN/\$USER/Maildir/.IsJunk
         echo "IsJunk" >> $DOMAINS/$DOMAIN/$USER/Maildir/subscriptions
       fi
       if [[|! -d \$DOMAINS/\$DOMAIN/\$USER/\$NOJUNK ]] ; then
         mkdir -p -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.NoJunk/cur
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.NoJunk/new
         mkdir -m 700 \$DOMAINS/\$DOMAIN/\$USER/Maildir/.NoJunk/tmp
         chown -R vpopmail:vchkpw \$DOMAINS/\$DOMAIN/\$USER/Maildir/.NoJunk
         echo "NoJunk" >> $DOMAINS/$DOMAIN/$USER/Maildir/subscriptions
       fi
 # vier Wochen alte, gelesene Junk-Mails löschen:
       find \$DOMAINS/\$DOMAIN/\$USER/\$JUNK -type f -mtime +28 -exec rm {}
\;
 # aus den manuell als Junk "markierten" Mail lernen und löschen:
       for ISJUNK in \$( ls -1 \$DOMAINS/\$DOMAIN/\$USER/\$ISJUNK ) ; do
         cat \$ISJUNK | \$DSPAM --user \${USER}@\${DOMAIN} --mode=teft --
class=spam --source=error
         rm \$ISJUNK
       done
 # aus den manuell als NICHT-Junk "markierten" Mails lernen und verschieben:
       for NOJUNK in \$( ls -1 \$DOMAINS/\$DOMAIN/\$USER/\$NOJUNK ) ; do
         cat \$NOJUNK | \$DSPAM --user \${USER}@\${DOMAIN} --mode=teft --
class=innocent --source=error
         mv \$NOJUNK \$DOMAINS/\$DOMAIN/\$USER/Maildir/cur
       done
     fi
   done
 done
 EOF
```

```
 chmod 755 /etc/cron.daily/dspam_reclass
```

.procmailrc

```
 cat <<EOF > /var/vpopmail/domains/<DOMAIN>/.procmailrc
 MAILDIR="/home/vpopmail/domains/\$USER/\$EXT/Maildir"
 LOGFILE="/var/log/procmail.log"
 VERBOSE="on"
>0:
 * ^X-DSPAM-Result: spam
 .Junk/
>0w
 | /home/vpopmail/bin/vdelivermail // delete
 EOF
```

Mail-(v)Server-Integration

```
 echo "| /usr/bin/dspam --mode=teft --deliver=innocent --token=chain --
feature=noise --user \$EXT@\$USER --stdout \
 | /var/qmail/bin/preline /usr/bin/procmail -p -m
/home/vpopmail/domains/bluemetaljackets.de/.procmailrc" \
 > /var/vpopmail/domains/<DOMAIN>/.qmail-default
```

platzhalter

Todo

1. dspam_clean
2. mysql> purge.sql